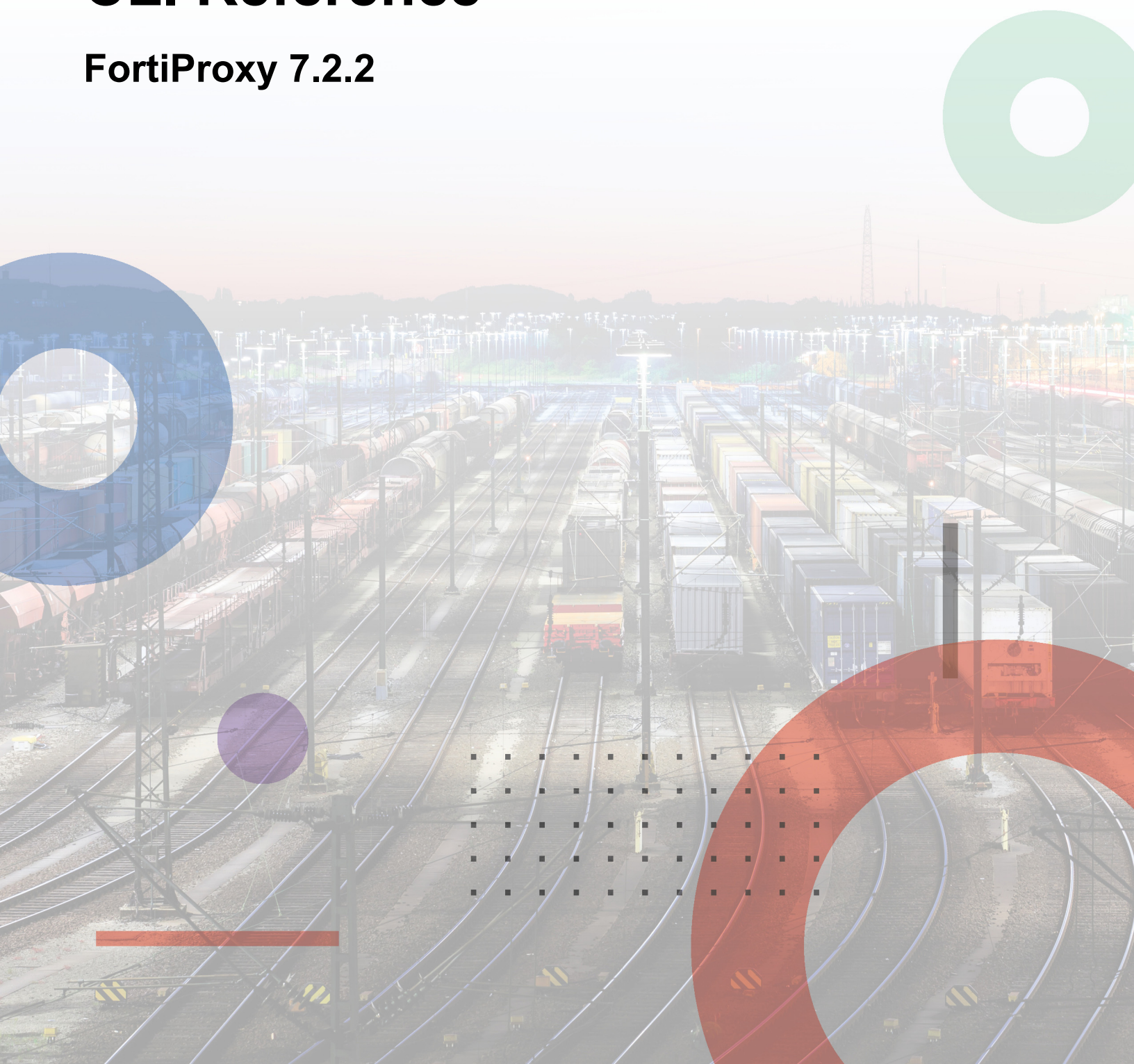
FORTINET

CLI Reference

FortiProxy 7.2.2



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

August 2, 2023
FortiProxy 7.2.2 CLI Reference
45-722-717315-20230802

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-12-20	Initial release.
2023-08-02	Deleted some commands and options that do not apply to FortiProxy.

FortiProxy CLI Interface

This document describes FortiProxy 7.2.2 CLI commands that are used to configure and manage FortiProxy from the command line interface (CLI). For information on using the CLI, see the FortiProxy Administration Guide.

alertemail

This section includes syntax for the following commands:

config alertemail setting

Configure alert email settings.

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

config alertemail setting

Parameter	Description	Type	Size	Default
username	Name that appears in the From: field of alert emails (max. 63 characters).	string	Maximum length: 63	
mailto1	Email address to send alert email to (usually a system administrator) (max. 63 characters).	string	Maximum length: 63	
mailto2	Optional second email address to send alert email to (max. 63 characters).	string	Maximum length: 63	
mailto3	Optional third email address to send alert email to (max. 63 characters).	string	Maximum length: 63	
filter-mode	How to filter log messages that are sent to alert emails.	option	-	category
	Option / **Description** *category* — Filter based on category. *threshold* — Filter based on severity.			
email-interval	Interval between sending alert emails .	integer	Minimum value: 1 Maximum value: 99999	5
IPS-logs	Enable/disable IPS logs in alert email.	option	-	disable
	Option / **Description** *enable* — Enable IPS logs in alert email. *disable* — Disable IPS logs in alert email.			
firewall-authentication-failure-logs	Enable/disable firewall authentication failure logs in alert email.	option	-	disable
	Option / **Description** *enable* — Enable firewall authentication failure logs in alert email. *disable* — Disable firewall authentication failure logs in alert email.			
HA-logs	Enable/disable HA logs in alert email.	option	-	disable
	Option / **Description** *enable* — Enable HA logs in alert email. *disable* — Disable HA logs in alert email.			

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Parameter	Description	Type	Size	Default

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

antivirus

This section includes syntax for the following commands:

config antivirus profile

Configure AntiVirus profiles.

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

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

```
        set archive-log {option1}, {option2}, ...
        set emulator [enable|disable]
    end
    config cifs
        Description: Configure CIFS AntiVirus options.
        set av-scan [disable|block|...]
        set outbreak-prevention [disable|block|...]
        set external-blocklist [disable|block|...]
        set fortindr [disable|block|...]
        set quarantine [disable|enable]
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set emulator [enable|disable]
    end
    config ssh
        Description: Configure SFTP and SCP AntiVirus options.
        set av-scan [disable|block|...]
        set outbreak-prevention [disable|block|...]
        set external-blocklist [disable|block|...]
        set fortindr [disable|block|...]
        set quarantine [disable|enable]
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set emulator [enable|disable]
    end
    config nac-quar
        Description: Configure AntiVirus quarantine settings.
        set infected [none|quar-src-ip]
        set expiry {user}
        set log [enable|disable]
    end
    config content-disarm
        Description: AV Content Disarm and Reconstruction settings.
        set original-file-destination [fortisandbox|quarantine|...]
        set error-action [block|log-only|...]
        set office-macro [disable|enable]
        set office-hylink [disable|enable]
        set office-linked [disable|enable]
        set office-embed [disable|enable]
        set office-dde [disable|enable]
        set office-action [disable|enable]
        set pdf-javacode [disable|enable]
        set pdf-embedfile [disable|enable]
        set pdf-hyperlink [disable|enable]
        set pdf-act-gotor [disable|enable]
        set pdf-act-launch [disable|enable]
        set pdf-act-sound [disable|enable]
        set pdf-act-movie [disable|enable]
        set pdf-act-java [disable|enable]
        set pdf-act-form [disable|enable]
        set cover-page [disable|enable]
        set detect-only [disable|enable]
    end
    set outbreak-prevention-archive-scan [disable|enable]
    set external-blocklist-enable-all [disable|enable]
    set external-blocklist <name1>, <name2>, ...
```

```
        set ems-threat-feed [disable|enable]
        set fortindr-error-action [log-only|block|...]
        set fortindr-timeout-action [log-only|block|...]
        set av-virus-log [enable|disable]
        set av-block-log [enable|disable]
        set extended-log [enable|disable]
        set scan-mode [default|legacy]
    next
end
```

config antivirus profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
replacemsg-group	Replacement message group customized for this profile.	string	Maximum length: 35	
ftgd-analytics	Settings to control which files are uploaded to FortiSandbox.	option	-	disable

Option	Description
disable	Do not upload files to FortiSandbox.
suspicious	Submit files supported by FortiSandbox if heuristics or other methods determine they are suspicious.
everything	Submit files supported by FortiSandbox and known infected files.

analytics-max-upload	Maximum size of files that can be uploaded to FortiSandbox.	integer	Minimum value: 1 Maximum value: 204	10
analytics-ignore-filetype	Do not submit files matching this DLP file-pattern to FortiSandbox.	integer	Minimum value: 0 Maximum value: 4294967295	0
analytics-accept-filetype	Only submit files matching this DLP file-pattern to FortiSandbox.	integer	Minimum value: 0 Maximum value: 4294967295	0
analytics-db	Enable/disable using the FortiSandbox signature database to supplement the AV signature databases.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Use only the standard AV signature databases. *enable* — Also use the FortiSandbox signature database.			
mobile-malware-db	Enable/disable using the mobile malware signature database.	option	-	enable
	Option / **Description** *disable* — Do not use the mobile malware signature database. *enable* — Also use the mobile malware signature database.			
outbreak-prevention-archive-scan	Enable/disable outbreak-prevention archive scanning.	option	-	enable
	Option / **Description** *disable* — Analyze files as sent, not the content of archives. *enable* — Analyze files including the content of archives.			
external-blocklist-enable-all	Enable/disable all external blocklists.	option	-	disable
	Option / **Description** *disable* — Use configured external blocklists. *enable* — Enable all external blocklists.			
external-blocklist `<name>`	One or more external malware block lists. External blocklist.	string	Maximum length: 79	
ems-threat-feed	Enable/disable use of EMS threat feed when performing AntiVirus scan. Analyzes files including the content of archives.	option	-	disable
	Option / **Description** *disable* — Disable use of EMS threat feed when performing AntiVirus scan. *enable* — Enable use of EMS threat feed when performing AntiVirus scan.			
fortindr-error-action	Action to take if FortiNDR encounters an error.	option	-	log-only

Parameter	Description	Type	Size	Default
	Option / **Description** *log-only* — Log FortiNDR error, but allow the file. *block* — Block the file on FortiNDR error. *ignore* — Do nothing on FortiNDR error.			
fortindr-timeout-action	Action to take if FortiNDR encounters a scan timeout.	option	-	log-only
	Option / **Description** *log-only* — Log FortiNDR scan timeout, but allow the file. *block* — Block the file on FortiNDR scan timeout. *ignore* — Do nothing on FortiNDR scan timeout.			
av-virus-log	Enable/disable AntiVirus logging.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
av-block-log	Enable/disable logging for AntiVirus file blocking.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
extended-log	Enable/disable extended logging for antivirus.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
scan-mode	Configure scan mode .	option	-	default
	Option / **Description** *default* — On the fly decompression and scanning of certain archive files. *legacy* — Scan archive files only after the entire file is received.			

config http

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

Option	Description
disable	Disable.
block	Block the virus infected files.
monitor	Log the virus infected files.

Parameter	Description	Type	Size	Default
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable

Option	Description
disable	Disable.
block	Block the matched files.
monitor	Log the matched files.

Parameter	Description	Type	Size	Default
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable

Option	Description
disable	Disable.
block	Block the matched files.
monitor	Log the matched files.

Parameter	Description	Type	Size	Default
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable

Option	Description
disable	Disable.
block	Block the FortiNDR detected infections.
monitor	Log the FortiNDR detected infections.

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

Option	Description
disable	Disable quarantine for infected files.
enable	Enable quarantine for infected files.

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

Parameter	Description	Type	Size	Default
	Option / **Description** *encrypted* — Block encrypted archives. *corrupted* — Block corrupted archives. *partiallycorrupted* — Block partially corrupted archives. *multipart* — Block multipart archives. *nested* — Block nested archives that exceed uncompressed nest limit. *mailbomb* — Block mail bomb archives. *timeout* — Block scan timeout. *unhandled* — Block archives that FortiProxy cannot open.			
archive-log	Select the archive types to log.	option	-	
	Option / **Description** *encrypted* — Log encrypted archives. *corrupted* — Log corrupted archives. *partiallycorrupted* — Log partially corrupted archives. *multipart* — Log multipart archives. *nested* — Log nested archives that exceed uncompressed nest limit. *mailbomb* — Log mail bomb archives. *timeout* — Log scan timeout. *unhandled* — Log archives that FortiProxy cannot open.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option / **Description** *enable* — Enable the virus emulator. *disable* — Disable the virus emulator.			
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable
	Option / **Description** *disable* — Disable Content Disarm and Reconstruction when performing AntiVirus scan. *enable* — Enable Content Disarm and Reconstruction when performing AntiVirus scan.			

config ftp

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

Option	Description
disable	Disable.
block	Block the virus infected files.
monitor	Log the virus infected files.

Parameter	Description	Type	Size	Default
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable

Option	Description
disable	Disable.
block	Block the matched files.
monitor	Log the matched files.

Parameter	Description	Type	Size	Default
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable

Option	Description
disable	Disable.
block	Block the matched files.
monitor	Log the matched files.

Parameter	Description	Type	Size	Default
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable

Option	Description
disable	Disable.
block	Block the FortiNDR detected infections.
monitor	Log the FortiNDR detected infections.

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

Option	Description
disable	Disable quarantine for infected files.
enable	Enable quarantine for infected files.

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

Parameter	Description	Type	Size	Default
	Option / **Description** *encrypted* — Block encrypted archives. *corrupted* — Block corrupted archives. *partiallycorrupted* — Block partially corrupted archives. *multipart* — Block multipart archives. *nested* — Block nested archives that exceed uncompressed nest limit. *mailbomb* — Block mail bomb archives. *timeout* — Block scan timeout. *unhandled* — Block archives that FortiProxy cannot open.			
archive-log	Select the archive types to log.	option	-	
	Option / **Description** *encrypted* — Log encrypted archives. *corrupted* — Log corrupted archives. *partiallycorrupted* — Log partially corrupted archives. *multipart* — Log multipart archives. *nested* — Log nested archives that exceed uncompressed nest limit. *mailbomb* — Log mail bomb archives. *timeout* — Log scan timeout. *unhandled* — Log archives that FortiProxy cannot open.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option / **Description** *enable* — Enable the virus emulator. *disable* — Disable the virus emulator.			

config imap

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

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Disable. *block* — Block the virus infected files. *monitor* — Log the virus infected files.			
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the matched files. *monitor* — Log the matched files.			
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the matched files. *monitor* — Log the matched files.			
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the FortiNDR detected infections. *monitor* — Log the FortiNDR detected infections.			
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option / **Description** *disable* — Disable quarantine for infected files. *enable* — Enable quarantine for infected files.			
archive-block	Select the archive types to block.	option	-	
	Option / **Description** *encrypted* — Block encrypted archives.			

Parameter	Description	Type	Size	Default
	Option / **Description** *corrupted* — Block corrupted archives. *partiallycorrupted* — Block partially corrupted archives. *multipart* — Block multipart archives. *nested* — Block nested archives that exceed uncompressed nest limit. *mailbomb* — Block mail bomb archives. *timeout* — Block scan timeout. *unhandled* — Block archives that FortiProxy cannot open.			
archive-log	Select the archive types to log.	option	-	
	Option / **Description** *encrypted* — Log encrypted archives. *corrupted* — Log corrupted archives. *partiallycorrupted* — Log partially corrupted archives. *multipart* — Log multipart archives. *nested* — Log nested archives that exceed uncompressed nest limit. *mailbomb* — Log mail bomb archives. *timeout* — Log scan timeout. *unhandled* — Log archives that FortiProxy cannot open.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option / **Description** *enable* — Enable the virus emulator. *disable* — Disable the virus emulator.			
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default
	Option / **Description** *default* — Perform standard AntiVirus scanning of Windows executable files. *virus* — Treat Windows executables as viruses.			
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Disable Content Disarm and Reconstruction when performing AntiVirus scan. *enable* — Enable Content Disarm and Reconstruction when performing AntiVirus scan.			

config pop3

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the virus infected files. *monitor* — Log the virus infected files.			
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the matched files. *monitor* — Log the matched files.			
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the matched files. *monitor* — Log the matched files.			
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the FortiNDR detected infections. *monitor* — Log the FortiNDR detected infections.			
quarantine	Enable/disable quarantine for infected files.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Disable quarantine for infected files. *enable* — Enable quarantine for infected files.			
archive-block	Select the archive types to block.	option	-	
	Option / **Description** *encrypted* — Block encrypted archives. *corrupted* — Block corrupted archives. *partiallycorrupted* — Block partially corrupted archives. *multipart* — Block multipart archives. *nested* — Block nested archives that exceed uncompressed nest limit. *mailbomb* — Block mail bomb archives. *timeout* — Block scan timeout. *unhandled* — Block archives that FortiProxy cannot open.			
archive-log	Select the archive types to log.	option	-	
	Option / **Description** *encrypted* — Log encrypted archives. *corrupted* — Log corrupted archives. *partiallycorrupted* — Log partially corrupted archives. *multipart* — Log multipart archives. *nested* — Log nested archives that exceed uncompressed nest limit. *mailbomb* — Log mail bomb archives. *timeout* — Log scan timeout. *unhandled* — Log archives that FortiProxy cannot open.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option / **Description** *enable* — Enable the virus emulator. *disable* — Disable the virus emulator.			
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default

Parameter	Description	Type	Size	Default
	Option / **Description** *default* — Perform standard AntiVirus scanning of Windows executable files. *virus* — Treat Windows executables as viruses.			
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable
	Option / **Description** *disable* — Disable Content Disarm and Reconstruction when performing AntiVirus scan. *enable* — Enable Content Disarm and Reconstruction when performing AntiVirus scan.			

config smtp

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the virus infected files. *monitor* — Log the virus infected files.			
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the matched files. *monitor* — Log the matched files.			
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the matched files. *monitor* — Log the matched files.			
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Disable. *block* — Block the FortiNDR detected infections. *monitor* — Log the FortiNDR detected infections.			
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option / **Description** *disable* — Disable quarantine for infected files. *enable* — Enable quarantine for infected files.			
archive-block	Select the archive types to block.	option	-	
	Option / **Description** *encrypted* — Block encrypted archives. *corrupted* — Block corrupted archives. *partiallycorrupted* — Block partially corrupted archives. *multipart* — Block multipart archives. *nested* — Block nested archives that exceed uncompressed nest limit. *mailbomb* — Block mail bomb archives. *timeout* — Block scan timeout. *unhandled* — Block archives that FortiProxy cannot open.			
archive-log	Select the archive types to log.	option	-	
	Option / **Description** *encrypted* — Log encrypted archives. *corrupted* — Log corrupted archives. *partiallycorrupted* — Log partially corrupted archives. *multipart* — Log multipart archives. *nested* — Log nested archives that exceed uncompressed nest limit. *mailbomb* — Log mail bomb archives. *timeout* — Log scan timeout. *unhandled* — Log archives that FortiProxy cannot open.			
emulator	Enable/disable the virus emulator.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable the virus emulator. *disable* — Disable the virus emulator.			
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default
	Option / **Description** *default* — Perform standard AntiVirus scanning of Windows executable files. *virus* — Treat Windows executables as viruses.			
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable
	Option / **Description** *disable* — Disable Content Disarm and Reconstruction when performing AntiVirus scan. *enable* — Enable Content Disarm and Reconstruction when performing AntiVirus scan.			

config mapi

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the virus infected files. *monitor* — Log the virus infected files.			
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the matched files. *monitor* — Log the matched files.			
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Disable. *block* — Block the matched files. *monitor* — Log the matched files.			
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the FortiNDR detected infections. *monitor* — Log the FortiNDR detected infections.			
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option / **Description** *disable* — Disable quarantine for infected files. *enable* — Enable quarantine for infected files.			
archive-block	Select the archive types to block.	option	-	
	Option / **Description** *encrypted* — Block encrypted archives. *corrupted* — Block corrupted archives. *partiallycorrupted* — Block partially corrupted archives. *multipart* — Block multipart archives. *nested* — Block nested archives that exceed uncompressed nest limit. *mailbomb* — Block mail bomb archives. *timeout* — Block scan timeout. *unhandled* — Block archives that FortiProxy cannot open.			
archive-log	Select the archive types to log.	option	-	
	Option / **Description** *encrypted* — Log encrypted archives. *corrupted* — Log corrupted archives. *partiallycorrupted* — Log partially corrupted archives.			

Parameter	Description	Type	Size	Default
	Option / **Description** *multipart* — Log multipart archives. *nested* — Log nested archives that exceed uncompressed nest limit. *mailbomb* — Log mail bomb archives. *timeout* — Log scan timeout. *unhandled* — Log archives that FortiProxy cannot open.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option / **Description** *enable* — Enable the virus emulator. *disable* — Disable the virus emulator.			
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default
	Option / **Description** *default* — Perform standard AntiVirus scanning of Windows executable files. *virus* — Treat Windows executables as viruses.			

config nntp

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the virus infected files. *monitor* — Log the virus infected files.			
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the matched files. *monitor* — Log the matched files.			

Parameter	Description	Type	Size	Default
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable

Option	Description
disable	Disable.
block	Block the matched files.
monitor	Log the matched files.

Parameter	Description	Type	Size	Default
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable

Option	Description
disable	Disable.
block	Block the FortiNDR detected infections.
monitor	Log the FortiNDR detected infections.

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

Option	Description
disable	Disable quarantine for infected files.
enable	Enable quarantine for infected files.

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

Option	Description
encrypted	Block encrypted archives.
corrupted	Block corrupted archives.
partiallycorrupted	Block partially corrupted archives.
multipart	Block multipart archives.
nested	Block nested archives that exceed uncompressed nest limit.
mailbomb	Block mail bomb archives.
timeout	Block scan timeout.
unhandled	Block archives that FortiProxy cannot open.

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

Option	Description
encrypted	Log encrypted archives.

Parameter	Description	Type	Size	Default
	Option / **Description** *corrupted* — Log corrupted archives. *partiallycorrupted* — Log partially corrupted archives. *multipart* — Log multipart archives. *nested* — Log nested archives that exceed uncompressed nest limit. *mailbomb* — Log mail bomb archives. *timeout* — Log scan timeout. *unhandled* — Log archives that FortiProxy cannot open.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option / **Description** *enable* — Enable the virus emulator. *disable* — Disable the virus emulator.			

config cifs

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the virus infected files. *monitor* — Log the virus infected files.			
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the matched files. *monitor* — Log the matched files.			
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Disable. *block* — Block the matched files. *monitor* — Log the matched files.			
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the FortiNDR detected infections. *monitor* — Log the FortiNDR detected infections.			
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option / **Description** *disable* — Disable quarantine for infected files. *enable* — Enable quarantine for infected files.			
archive-block	Select the archive types to block.	option	-	
	Option / **Description** *encrypted* — Block encrypted archives. *corrupted* — Block corrupted archives. *partiallycorrupted* — Block partially corrupted archives. *multipart* — Block multipart archives. *nested* — Block nested archives that exceed uncompressed nest limit. *mailbomb* — Block mail bomb archives. *timeout* — Block scan timeout. *unhandled* — Block archives that FortiProxy cannot open.			
archive-log	Select the archive types to log.	option	-	
	Option / **Description** *encrypted* — Log encrypted archives. *corrupted* — Log corrupted archives. *partiallycorrupted* — Log partially corrupted archives.			

Parameter	Description	Type	Size	Default
	Option / **Description** *multipart* — Log multipart archives. *nested* — Log nested archives that exceed uncompressed nest limit. *mailbomb* — Log mail bomb archives. *timeout* — Log scan timeout. *unhandled* — Log archives that FortiProxy cannot open.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option / **Description** *enable* — Enable the virus emulator. *disable* — Disable the virus emulator.			

config ssh

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the virus infected files. *monitor* — Log the virus infected files.			
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the matched files. *monitor* — Log the matched files.			
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	Option / **Description** *disable* — Disable.			

Parameter	Description	Type	Size	Default
	Option / **Description** *block* — Block the matched files. *monitor* — Log the matched files.			
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the FortiNDR detected infections. *monitor* — Log the FortiNDR detected infections.			
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option / **Description** *disable* — Disable quarantine for infected files. *enable* — Enable quarantine for infected files.			
archive-block	Select the archive types to block.	option	-	
	Option / **Description** *encrypted* — Block encrypted archives. *corrupted* — Block corrupted archives. *partiallycorrupted* — Block partially corrupted archives. *multipart* — Block multipart archives. *nested* — Block nested archives that exceed uncompressed nest limit. *mailbomb* — Block mail bomb archives. *timeout* — Block scan timeout. *unhandled* — Block archives that FortiProxy cannot open.			
archive-log	Select the archive types to log.	option	-	
	Option / **Description** *encrypted* — Log encrypted archives. *corrupted* — Log corrupted archives. *partiallycorrupted* — Log partially corrupted archives. *multipart* — Log multipart archives.			

Parameter	Description	Type	Size	Default
	Option / **Description** *nested* — Log nested archives that exceed uncompressed nest limit. *mailbomb* — Log mail bomb archives. *timeout* — Log scan timeout. *unhandled* — Log archives that FortiProxy cannot open.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option / **Description** *enable* — Enable the virus emulator. *disable* — Disable the virus emulator.			

config nac-quar

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

config content-disarm

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

Parameter	Description	Type	Size	Default
	Option / **Description** *fortisandbox* — Send original file to configured FortiSandbox. *quarantine* — Send original file to quarantine. *discard* — Original file will be discarded after content disarm.			
error-action	Action to be taken if CDR engine encounters an unrecoverable error.	option	-	log-only
	Option / **Description** *block* — Block file on CDR error. *log-only* — Log CDR error, but allow file. *ignore* — Do nothing on CDR error.			
office-macro	Enable/disable stripping of macros in Microsoft Office documents.	option	-	enable
	Option / **Description** *disable* — Disable this Content Disarm and Reconstruction feature. *enable* — Enable this Content Disarm and Reconstruction feature.			
office-hylink	Enable/disable stripping of hyperlinks in Microsoft Office documents.	option	-	enable
	Option / **Description** *disable* — Disable this Content Disarm and Reconstruction feature. *enable* — Enable this Content Disarm and Reconstruction feature.			
office-linked	Enable/disable stripping of linked objects in Microsoft Office documents.	option	-	enable
	Option / **Description** *disable* — Disable this Content Disarm and Reconstruction feature. *enable* — Enable this Content Disarm and Reconstruction feature.			
office-embed	Enable/disable stripping of embedded objects in Microsoft Office documents.	option	-	enable
	Option / **Description** *disable* — Disable this Content Disarm and Reconstruction feature. *enable* — Enable this Content Disarm and Reconstruction feature.			

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

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

Parameter	Description	Type	Size	Default
office-action	Enable/disable stripping of PowerPoint action events in Microsoft Office documents.	option	-	enable

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

Parameter	Description	Type	Size	Default
pdf-javacode	Enable/disable stripping of JavaScript code in PDF documents.	option	-	enable

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

Parameter	Description	Type	Size	Default
pdf-embedfile	Enable/disable stripping of embedded files in PDF documents.	option	-	enable

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

Parameter	Description	Type	Size	Default
pdf-hyperlink	Enable/disable stripping of hyperlinks from PDF documents.	option	-	enable

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

Parameter	Description	Type	Size	Default
pdf-act-gotor	Enable/disable stripping of PDF document actions that access other PDF documents.	option	-	enable

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

Parameter	Description	Type	Size	Default
pdf-act-launch	Enable/disable stripping of PDF document actions that launch other applications.	option	-	enable

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

Parameter	Description	Type	Size	Default
pdf-act-sound	Enable/disable stripping of PDF document actions that play a sound.	option	-	enable

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

Parameter	Description	Type	Size	Default
pdf-act-movie	Enable/disable stripping of PDF document actions that play a movie.	option	-	enable

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

Parameter	Description	Type	Size	Default
pdf-act-java	Enable/disable stripping of PDF document actions that execute JavaScript code.	option	-	enable

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

Parameter	Description	Type	Size	Default
pdf-act-form	Enable/disable stripping of PDF document actions that submit data to other targets.	option	-	enable

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

Parameter	Description	Type	Size	Default
cover-page	Enable/disable inserting a cover page into the disarmed document.	option	-	enable

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

Parameter	Description	Type	Size	Default
detect-only	Enable/disable only detect disarmable files, do not alter content.	option	-	disable

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

config antivirus quarantine

Configure quarantine options.

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

config antivirus quarantine

Parameter	Description	Type	Size	Default
agelimit	Age limit for quarantined files .	integer	Minimum value: 0 Maximum value: 479	0
maxfilesize	Maximum file size to quarantine .	integer	Minimum value: 0 Maximum value: 500	0
quarantine-quota	The amount of disk space to reserve for quarantining files .	integer	Minimum value: 0 Maximum value: 4294967295	0

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

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

Parameter	Description	Type	Size	Default
store-infected	Quarantine infected files found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nntp imaps smtps pop3s https ftps mapi cifs ssh

Option	Description
imap	IMAP.
smtp	SMTP.
pop3	POP3.
http	HTTP.
ftp	FTP.

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

Parameter	Description	Type	Size	Default
store-blocked	Quarantine blocked files found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nntp imaps smtps pop3s ftps mapi cifs ssh

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

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

Option	Description
imap	IMAP.
smtp	SMTP.
pop3	POP3.
http	HTTP.
ftp	FTP.
nntp	NNTP.

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

Parameter	Description	Type	Size	Default
lowspace	Select the method for handling additional files when running low on disk space.	option	-	ovrw-old

Option	Description
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.

Parameter	Description	Type	Size	Default
destination	Choose whether to quarantine files to the FortiProxy disk or to FortiAnalyzer or to delete them instead of quarantining them.	option	-	disk

Option	Description
NULL	Files that would be quarantined are deleted.
disk	Quarantine files to the FortiProxy hard disk.
FortiAnalyzer	FortiAnalyzer

config antivirus settings

Configure AntiVirus settings.

```
config antivirus settings
    Description: Configure AntiVirus settings.
    set machine-learning-detection [enable|monitor|...]
    set use-extreme-db [enable|disable]
    set grayware [enable|disable]
    set override-timeout {integer}
    set cache-infected-result [enable|disable]
end
```

config antivirus settings

Parameter	Description	Type	Size	Default
machine-learning-detection	Use machine learning based malware detection.	option	-	enable

Option	Description
enable	Enable machine learning based malware detection.

Parameter	Description	Type	Size	Default
	Option / **Description** *monitor* — Enable machine learning based malware detection for monitoring only. *disable* — Disable machine learning based malware detection.			
use-extreme-db	Enable/disable the use of Extreme AVDB.	option	-	disable
	Option / **Description** *enable* — Enable extreme AVDB. *disable* — Disable extreme AVDB.			
grayware	Enable/disable grayware detection when an AntiVirus profile is applied to traffic.	option	-	disable
	Option / **Description** *enable* — Enable grayware detection. *disable* — Disable grayware detection.			
override-timeout	Override the large file scan timeout value in seconds . Zero is the default value and is used to disable this command. When disabled, the daemon adjusts the large file scan timeout based on the file size.	integer	Minimum value: 30 Maximum value: 3600	0
cache-infected-result	Enable/disable cache of infected scan results .	option	-	enable
	Option / **Description** *enable* — Enable cache of infected scan results. *disable* — Disable cache of infected scan results.			

application

This section includes syntax for the following commands:

config application custom

Configure custom application signatures.

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

config application custom

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

Parameter	Description	Type	Size	Default
category	Custom application category ID (use ? to view available options).	integer	Minimum value: 0 Maximum value: 4294967295	0
protocol	Custom application signature protocol.	user	Not Specified	
technology	Custom application signature technology.	user	Not Specified	
behavior	Custom application signature behavior.	user	Not Specified	
vendor	Custom application signature vendor.	user	Not Specified	

config application group

Configure firewall application groups.

```
config application group
    Description: Configure firewall application groups.
    edit <name>
        set comment {var-string}
        set type [application|filter]
        set application <id1>, <id2>, ...
        set category <id1>, <id2>, ...
        set risk <level1>, <level2>, ...
        set protocols {user}
        set vendor {user}
        set technology {user}
        set behavior {user}
        set popularity {option1}, {option2}, ...
    next
end
```

config application group

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

Option	Description
application	Application ID.
filter	Application filter.

Parameter	Description	Type	Size	Default
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
risk <level>	Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical). Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).	integer	Minimum value: 0 Maximum value: 4294967295	
protocols	Application protocol filter.	user	Not Specified	all
vendor	Application vendor filter.	user	Not Specified	all
technology	Application technology filter.	user	Not Specified	all
behavior	Application behavior filter.	user	Not Specified	all
popularity	Application popularity filter .	option	-	1 2 3 4 5

Option	Description
1	Popularity level 1.
2	Popularity level 2.
3	Popularity level 3.
4	Popularity level 4.
5	Popularity level 5.

config application list

Configure application control lists.

```
config application list
    Description: Configure application control lists.
    edit <name>
        set comment {var-string}
        set replacemsg-group {string}
        set extended-log [enable|disable]
        set other-application-action [pass|block]
```

```
        set app-replacemsg [disable|enable]
        set other-application-log [disable|enable]
        set enforce-default-app-port [disable|enable]
        set force-inclusion-ssl-di-sigs [disable|enable]
        set unknown-application-action [pass|block]
        set unknown-application-log [disable|enable]
        set p2p-block-list {option1}, {option2}, ...
        set deep-app-inspection [disable|enable]
        set options {option1}, {option2}, ...
        config entries
            Description: Application list entries.
            edit <id>
                set risk <level1>, <level2>, ...
                set category <id1>, <id2>, ...
                set application <id1>, <id2>, ...
                set protocols {user}
                set vendor {user}
                set technology {user}
                set behavior {user}
                set popularity {option1}, {option2}, ...
                set exclusion <id1>, <id2>, ...
                config parameters
                    Description: Application parameters.
                    edit <id>
                        config members
                            Description: Parameter tuple members.
                            edit <id>
                                set name {string}
                                set value {string}
                            next
                        end
                    next
                end
                set action [pass|block|...]
                set log [disable|enable]
                set log-packet [disable|enable]
                set rate-count {integer}
                set rate-duration {integer}
                set rate-mode [periodical|continuous]
                set rate-track [none|src-ip|...]
                set session-ttl {integer}
                set shaper {string}
                set quarantine [none|attacker]
                set quarantine-expiry {user}
                set quarantine-log [disable|enable]
            next
        end
        set control-default-network-services [disable|enable]
        config default-network-services
            Description: Default network service entries.
            edit <id>
                set port {integer}
                set services {option1}, {option2}, ...
                set violation-action [pass|monitor|...]
            next
        end
```

```
    next
end
```

config application list

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

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

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

config entries

Parameter	Description	Type	Size	Default
risk `<level>`	Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical). Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).	integer	Minimum value: 0 Maximum value: 4294967295	
category `<id>`	Category ID list. Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
application <id>	ID of allowed applications. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
protocols	Application protocol filter.	user	Not Specified	all
vendor	Application vendor filter.	user	Not Specified	all
technology	Application technology filter.	user	Not Specified	all
behavior	Application behavior filter.	user	Not Specified	all
popularity	Application popularity filter .	option	-	1 2 3 4 5

Option	Description
1	Popularity level 1.
2	Popularity level 2.
3	Popularity level 3.
4	Popularity level 4.
5	Popularity level 5.

exclusion <id>	ID of excluded applications. Excluded application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
action	Pass or block traffic, or reset connection for traffic from this application.	option	-	block

Option	Description
pass	Pass or allow matching traffic.
block	Block or drop matching traffic.
reset	Reset sessions for matching traffic.

log	Enable/disable logging for this application list.	option	-	enable

Option	Description
disable	Disable logging.
enable	Enable logging.

log-packet	Enable/disable packet logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Disable packet logging. *enable* — Enable packet logging.			
rate-count	Count of the rate.	integer	Minimum value: 0 Maximum value: 65535	0
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535	60
rate-mode	Rate limit mode.	option	-	continuous
	Option / **Description** *periodical* — Allow configured number of packets every rate-duration. *continuous* — Block packets once the rate is reached.			
rate-track	Track the packet protocol field.	option	-	none
	Option / **Description** *none* — none *src-ip* — Source IP. *dest-ip* — Destination IP. *dhcp-client-mac* — DHCP client. *dns-domain* — DNS domain.			
session-ttl	Session TTL .	integer	Minimum value: 0 Maximum value: 4294967295	0
shaper	Traffic shaper.	string	Maximum length: 35	
quarantine	Quarantine method.	option	-	none
	Option / **Description** *none* — Quarantine is disabled.			

Parameter	Description	Type	Size	Default
	Option **Description** *attacker* Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.			
quarantine-expiry	Duration of quarantine. . Requires quarantine set to attacker.	user	Not Specified	5m
quarantine-log	Enable/disable quarantine logging. **Option** **Description** *disable* Disable quarantine logging. *enable* Enable quarantine logging.	option	-	enable

config members

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

config default-network-services

Parameter	Description	Type	Size	Default
port	Port number.	integer	Minimum value: 0 Maximum value: 65535	0
services	Network protocols. **Option** **Description** *http* HTTP. *ssh* SSH. *telnet* TELNET. *ftp* FTP. *dns* DNS.	option	-	

Parameter	Description	Type	Size	Default
	Option / **Description** *smtp* — SMTP. *pop3* — POP3. *imap* — IMAP. *snmp* — SNMP. *nntp* — NNTP. *https* — HTTPS.			
violation-action	Action for protocols not in the allowlist for selected port.	option	-	block
	Option / **Description** *pass* — Allow protocols not in the allowlist for selected port. *monitor* — Monitor protocols not in the allowlist for selected port. *block* — Block protocols not in the allowlist for selected port.			

config application name

Configure application signatures.

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

```
            next
        end
    next
end
```

config application name

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

config parameters

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

config metadata

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

config application rule-settings

Configure application rule settings.

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

authentication

This section includes syntax for the following commands:

config authentication rule

Configure Authentication Rules.

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

config authentication rule

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

Parameter	Description	Type	Size	Default
	Option / **Description** *http* — HTTP traffic is matched and authentication is required. *ftp* — FTP traffic is matched and authentication is required. *socks* — SOCKS traffic is matched and authentication is required. *ssh* — SSH traffic is matched and authentication is required.			
web-proxy	Web-Proxy profile.	string	Maximum length: 35	
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79	
srcaddr <name>	Authentication is required for the selected IPv4 source address. Address name.	string	Maximum length: 79	
dstaddr <name>	Select an IPv4 destination address from available options. Required for web proxy authentication. Address name.	string	Maximum length: 79	
srcaddr6 <name>	Authentication is required for the selected IPv6 source address. Address name.	string	Maximum length: 79	
dstaddr6 <name>	Select an IPv6 destination address from available options. Required for web proxy authentication. Address name.	string	Maximum length: 79	
ip-based	Enable/disable IP-based authentication. When enabled, previously authenticated users from the same IP address will be exempted.	option	-	enable
	Option / **Description** *enable* — Enable IP-based authentication. *disable* — Disable IP-based authentication.			
active-auth-method	Select an active authentication method.	string	Maximum length: 35	
sso-auth-method	Select a single-sign on (SSO) authentication method.	string	Maximum length: 35	
web-auth-cookie	Enable/disable Web authentication cookies .	option	-	disable

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

config authentication scheme

Configure Authentication Schemes.

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

config authentication scheme

Parameter	Description	Type	Size	Default
method	Authentication methods . **Option** — **Description** *ntlm* — NTLM authentication. *basic* — Basic HTTP authentication. *digest* — Digest HTTP authentication. *form* — Form-based HTTP authentication. *negotiate* — Negotiate authentication. *fsso* — Fortinet Single Sign-On (FSSO) authentication. *rsso* — RADIUS Single Sign-On (RSSO) authentication. *ssh-publickey* — Public key based SSH authentication. *cert* — Client certificate authentication. *saml* — SAML authentication. *x-auth-user* — User from HTTP x-authenticated-user header.	option	-	
negotiate-ntlm	Enable/disable negotiate authentication for NTLM . **Option** — **Description** *enable* — Enable negotiate authentication for NTLM. *disable* — Disable negotiate authentication for NTLM.	option	-	enable
kerberos-keytab	Kerberos keytab setting.	string	Maximum length: 35	
domain-controller	Domain controller setting.	string	Maximum length: 35	
saml-server	SAML configuration.	string	Maximum length: 35	
saml-timeout	SAML authentication timeout in seconds.	integer	Minimum value: 30 Maximum value: 1200	120
fsso-agent-for-ntlm	FSSO agent to use for NTLM authentication.	string	Maximum length: 35	
require-tfa	Enable/disable two-factor authentication .	option	-	disable

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

config authentication setting

Configure authentication setting.

```
config authentication setting
    Description: Configure authentication setting.
    set active-auth-scheme {string}
    set sso-auth-scheme {string}
    set captive-portal-type [fqdn|ip]
    set captive-portal-ip {ipv4-address-any}
    set captive-portal-ip6 {ipv6-address}
    set captive-portal {string}
    set captive-portal6 {string}
    set cert-auth [enable|disable]
    set cert-captive-portal {string}
    set cert-captive-portal-ip {ipv4-address-any}
    set cert-captive-portal-port {integer}
    set captive-portal-port {integer}
    set auth-https [enable|disable]
    set captive-portal-ssl-port {integer}
    set rewrite-https-port {integer}
    set user-cert-ca <name1>, <name2>, ...
```

```
    set dev-range <name1>, <name2>, ...
end
```

config authentication setting

Parameter	Description	Type	Size	Default
active-auth-scheme	Active authentication method (scheme name).	string	Maximum length: 35	
sso-auth-scheme	Single-Sign-On authentication method (scheme name).	string	Maximum length: 35	
captive-portal-type	Captive portal type.	option	-	fqdn
	Option / **Description** *fqdn* — Use FQDN for captive portal. *ip* — Use an IP address for captive portal.			
captive-portal-ip	Captive portal IP address.	ipv4-address-any	Not Specified	0.0.0.0
captive-portal-ip6	Captive portal IPv6 address.	ipv6-address	Not Specified	::
captive-portal	Captive portal host name.	string	Maximum length: 255	
captive-portal6	IPv6 captive portal host name.	string	Maximum length: 255	
cert-auth	Enable/disable redirecting certificate authentication to HTTPS portal.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
cert-captive-portal	Certificate captive portal host name.	string	Maximum length: 255	
cert-captive-portal-ip	Certificate captive portal IP address.	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
cert-captive-portal-port	Certificate captive portal port number .	integer	Minimum value: 1 Maximum value: 65535	7832
captive-portal-port	Captive portal port number .	integer	Minimum value: 1 Maximum value: 65535	7830
auth-https	Enable/disable redirecting HTTP user authentication to HTTPS.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
captive-portal-ssl-port	Captive portal SSL port number .	integer	Minimum value: 1 Maximum value: 65535	7831
rewrite-https-port	Rewrite to HTTPS port .	integer	Minimum value: 0 Maximum value: 65535	0
user-cert-ca `<name>`	CA certificate used for client certificate verification. CA certificate list.	string	Maximum length: 79	
dev-range `<name>`	Address range for the IP based device query. Address name.	string	Maximum length: 79	

certificate

This section includes syntax for the following commands:

config certificate ca

CA certificate.

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

config certificate ca

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

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

source	CA certificate source type.	option	-	user

Parameter	Description	Type	Size	Default
	Option / **Description** *factory* — Factory installed certificate. *user* — User generated certificate. *bundle* — Bundle file certificate.			
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection. **Option** / **Description** *enable* — Trusted CA for SSL inspection. *disable* — Untrusted CA for SSL inspection.	option	-	enable
scep-url	URL of the SCEP server.	string	Maximum length: 255	
auto-update-days	Number of days to wait before requesting an updated CA certificate .	integer	Minimum value: 0 Maximum value: 4294967295	0
auto-update-days-warning	Number of days before an expiry-warning message is generated .	integer	Minimum value: 0 Maximum value: 4294967295	0
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0
ca-identifier	CA identifier of the SCEP server.	string	Maximum length: 255	

config certificate crl

Certificate Revocation List as a PEM file.

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

```
        set ldap-username {string}
        set ldap-password {password}
        set http-url {string}
        set scep-url {string}
        set scep-cert {string}
        set update-interval {integer}
        set source-ip {ipv4-address}
    next
end
```

config certificate crl

Parameter	Description	Type	Size	Default
crl	Certificate Revocation List as a PEM file.	user	Not Specified	
range	Either global or VDOM IP address range for the certificate.	option	-	global
	Option / **Description** *global* — Global range. *vdom* — VDOM IP address range.			
source	Certificate source type.	option	-	user
	Option / **Description** *factory* — Factory installed certificate. *user* — User generated certificate. *bundle* — Bundle file certificate.			
update-vdom	VDOM for CRL update.	string	Maximum length: 31	root
ldap-server	LDAP server name for CRL auto-update.	string	Maximum length: 35	
ldap-username	LDAP server user name.	string	Maximum length: 63	
ldap-password	LDAP server user password.	password	Not Specified	
http-url	HTTP server URL for CRL auto-update.	string	Maximum length: 255	
scep-url	SCEP server URL for CRL auto-update.	string	Maximum length: 255	
scep-cert	Local certificate for SCEP communication for CRL auto-update.	string	Maximum length: 35	Fortinet_CA_SSL

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

config certificate local

Local keys and certificates.

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

config certificate local

Parameter	Description	Type	Size	Default
type	Type.	option	-	normal
	Option / **Description** *normal* — Normal *hsm* — HSM			
nethsm-slot	Network HSM slot name.	string	Maximum length: 35	
password	Password as a PEM file.	password	Not Specified	
comments	Comment.	string	Maximum length: 511	
private-key	PEM format key encrypted with a password.	user	Not Specified	
certificate	PEM format certificate.	user	Not Specified	
csr	Certificate Signing Request.	user	Not Specified	
state	Certificate Signing Request State.	user	Not Specified	
scep-url	SCEP server URL.	string	Maximum length: 255	
range	Either a global or VDOM IP address range for the certificate.	option	-	global
	Option / **Description** *global* — Global range. *vdom* — VDOM IP address range.			
source	Certificate source type.	option	-	user
	Option / **Description** *factory* — Factory installed certificate. *user* — User generated certificate. *bundle* — Bundle file certificate.			

Parameter	Description	Type	Size	Default
auto-regenerate-days	Number of days to wait before expiry of an updated local certificate is requested (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0
auto-regenerate-days-warning	Number of days to wait before an expiry warning message is generated (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0
scep-password	SCEP server challenge password for auto-regeneration.	password	Not Specified	
ca-identifier	CA identifier of the CA server for signing via SCEP.	string	Maximum length: 255	
name-encoding	Name encoding method for auto-regeneration.	option	-	printable

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

Parameter	Description	Type	Size	Default
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0
ike-localid	Local ID the FortiProxy uses for authentication as a VPN client.	string	Maximum length: 63	
ike-localid-type	IKE local ID type.	option	-	asn1dn

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

Parameter	Description	Type	Size	Default
enroll-protocol	Certificate enrollment protocol.	option	-	none

Option	Description
none	None (default).
scep	Simple Certificate Enrollment Protocol.

Parameter	Description	Type	Size	Default
	Option / **Description** *cmpv2* / Certificate Management Protocol Version 2. *acme2* / Automated Certificate Management Environment Version 2.			
cmp-server	Address and port for CMP server (format = address:port).	string	Maximum length: 63	
cmp-path	Path location inside CMP server.	string	Maximum length: 255	
cmp-server-cert	CMP server certificate.	string	Maximum length: 79	
cmp-regeneration-method	CMP auto-regeneration method.	option	-	keyupate
	Option / **Description** *keyupate* / Key Update. *renewal* / Renewal.			
acme-ca-url	The URL for the ACME CA server .	string	Maximum length: 255	https://acme-v02.api.letsencrypt.org/directory
acme-domain	A valid domain that resolves to this FortiProxy unit.	string	Maximum length: 255	
acme-email	Contact email address that is required by some CAs like LetsEncrypt.	string	Maximum length: 255	
acme-rsa-key-size	Length of the RSA private key of the generated cert (Minimum 2048 bits).	integer	Minimum value: 2048 Maximum value: 4096	2048
acme-renew-window	Beginning of the renewal window .	integer	Minimum value: 1 Maximum value: 60	30

config certificate remote

Remote certificate as a PEM file.

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

config certificate remote

Parameter	Description	Type	Size	Default
remote	Remote certificate.	user	Not Specified	
range	Either the global or VDOM IP address range for the remote certificate.	option	-	global

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

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

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

dlp

This section includes syntax for the following commands:

config dlp filepattern

Configure file patterns used by DLP blocking.

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

config dlp filepattern

Parameter	Description	Type	Size	Default
name	Name of table containing the file pattern list.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default
filter-type	Filter by file name pattern or by file type.	option	-	pattern

Parameter	Description	Type	Size	Default
	Option / **Description** *pattern* — Filter by file name pattern. *type* — Filter by file type.			
file-type	Select a file type.	option	-	unknown
	Option / **Description** *7z* — Match 7-zip files. *arj* — Match arj compressed files. *cab* — Match Windows cab files. *lzh* — Match lzh compressed files. *rar* — Match rar archives. *tar* — Match tar files. *zip* — Match zip files. *bzip* — Match bzip files. *gzip* — Match gzip files. *bzip2* — Match bzip2 files. *xz* — Match xz files. *bat* — Match Windows batch files. *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.			

Parameter	Description	Type	Size	Default

Option	Description
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.
sis	Match sis files.
hlp	Match Windows help files.
activemime	Match activemime files.
jpeg	Match jpeg files.
gif	Match gif files.
tiff	Match tiff files.
png	Match png files.
bmp	Match bmp files.
unknown	Match unknown files.
mpeg	Match mpeg files.
mov	Match mov files.
mp3	Match mp3 files.
wma	Match wma files.
wav	Match wav files.
pdf	Match Acrobat PDF files.
avi	Match avi files.
rm	Match rm files.
torrent	Match torrent files.
hibun	Match special-file-23-support files.
msi	Match Windows Installer msi files.
mach-o	Match Mach object files.
dmg	Match Apple disk image files.
.net	Match .NET files.

Parameter	Description	Type	Size	Default

Option	Description
xar	Match xar archive files.
chm	Match Windows compiled HTML help files.
iso	Match ISO archive files.
crx	Match Chrome extension files.
flac	Match flac files.

config dlp fp-doc-source

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

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

config dlp fp-doc-source

Parameter	Description	Type	Size	Default
server-type	Protocol used to communicate with the file server. Currently only Samba (SMB) servers are supported.	option	-	samba

Parameter	Description	Type	Size	Default
	Option / **Description** *samba* / SAMBA server.			
server	IPv4 or IPv6 address of the server.	string	Maximum length: 35	
period	Frequency for which the FortiProxy checks the server for new or changed files.	option	-	none
	Option / **Description** *none* / Check the server when the FortiProxy starts up. *daily* / Check the server once a day. *weekly* / Check the server once a week. *monthly* / Check the server once a month.			
vdom	Select the VDOM that can communicate with the file server.	option	-	mgmt
	Option / **Description** *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.			
scan-subdirectories	Enable/disable scanning subdirectories to find files to create fingerprints from.	option	-	enable
	Option / **Description** *enable* / Scan subdirectories. *disable* / Do not scan subdirectories.			
scan-on-creation	Enable to keep the fingerprint database up to date when a file is added or changed on the server.	option	-	enable
	Option / **Description** *enable* / Keep the fingerprint database up to date when a file is added or changed on the server. *disable* / Do not check for added or changed files on the server. Saves system resources.			
remove-deleted	Enable to keep the fingerprint database up to date when a file is deleted from the server.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Keep the fingerprint database up to date when a file is deleted from the server. *disable* — Do not check for deleted files on the server. Saves system resources.			
keep-modified	Enable so that when a file is changed on the server the FortiProxy keeps the old fingerprint and adds a new fingerprint to the database.	option	-	enable
	Option / **Description** *enable* — Keep the old fingerprint and add a new fingerprint when a file is changed on the server. *disable* — Replace the old fingerprint with the new fingerprint when a file is changed on the server.			
username	User name required to log into the file server.	string	Maximum length: 35	
password	Password required to log into the file server.	password	Not Specified	
file-path	Path on the server to the fingerprint files (max 119 characters).	string	Maximum length: 119	
file-pattern	Files matching this pattern on the server are fingerprinted. Optionally use the * and ? wildcards.	string	Maximum length: 35	*
sensitivity	Select a sensitivity or threat level for matches with this fingerprint database. Add sensitivities using sensitivity.	string	Maximum length: 35	
tod-hour	Hour of the day on which to scan the server .	integer	Minimum value: 0 Maximum value: 23	1
tod-min	Minute of the hour on which to scan the server .	integer	Minimum value: 0 Maximum value: 59	0
weekday	Day of the week on which to scan the server.	option	-	sunday
	Option / **Description** *sunday* — Sunday *monday* — Monday			

Parameter	Description	Type	Size	Default
	Option / **Description** *tuesday* / Tuesday *wednesday* / Wednesday *thursday* / Thursday *friday* / Friday *saturday* / Saturday			
date	Day of the month on which to scan the server .	integer	Minimum value: 1 Maximum value: 31	1

config dlp sensitivity

Create self-explanatory DLP sensitivity levels to be used when setting sensitivity under config fp-doc-source.

```
config dlp sensitivity
    Description: Create self-explanatory DLP sensitivity levels to be used when setting
sensitivity under config fp-doc-source.
    edit <name>
    next
end
```

config dlp sensor

Configure DLP sensors.

```
config dlp sensor
    Description: Configure DLP sensors.
    edit <name>
        set comment {var-string}
        set replacemsg-group {string}
        config filter
            Description: Set up DLP filters for this sensor.
            edit <id>
                set name {string}
                set severity [info|low|...]
                set type [file|message]
                set proto {option1}, {option2}, ...
                set filter-by [credit-card|ssn|...]
                set file-size {integer}
                set company-identifier {string}
                set sensitivity <name1>, <name2>, ...
```

```
                set match-percentage {integer}
                set file-type {integer}
                set regexp {string}
                set archive [disable|enable]
                set action [allow|log-only|...]
                set expiry {user}
            next
        end
        set dlp-log [enable|disable]
        set extended-log [enable|disable]
        set nac-quar-log [enable|disable]
        set full-archive-proto {option1}, {option2}, ...
        set summary-proto {option1}, {option2}, ...
    next
end
```

config dlp sensor

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
replacemsg-group	Replacement message group used by this DLP sensor.	string	Maximum length: 35	
dlp-log	Enable/disable DLP logging.	option	-	enable
	Option / **Description** *enable* — Enable DLP logging. *disable* — Disable DLP logging.			
extended-log	Enable/disable extended logging for data leak prevention.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
nac-quar-log	Enable/disable NAC quarantine logging.	option	-	disable
	Option / **Description** *enable* — Enable NAC quarantine logging. *disable* — Disable NAC quarantine logging.			
full-archive-proto	Protocols to always content archive.	option	-	

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

config filter

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

Parameter	Description	Type	Size	Default
severity	Select the severity or threat level that matches this filter.	option	-	medium

Option	Description
info	Informational.
low	Low.
medium	Medium.
high	High.
critical	Critical.

Parameter	Description	Type	Size	Default
type	Select whether to check the content of messages (an email message) or files (downloaded files or email attachments).	option	-	file

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

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

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

Parameter	Description	Type	Size	Default
filter-by	Select the type of content to match.	option	-	credit-card

Option	Description
credit-card	Match credit cards.

Parameter	Description	Type	Size	Default
	Option / **Description** *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. *file-type-and-size* — Match DLP file pattern list for any file with size over the thresold.			
file-size	Match files this size or larger .	integer	Minimum value: 0 Maximum value: 4294967295	10
company-identifier	Enter a company identifier watermark to match. Only watermarks that your company has placed on the files are matched.	string	Maximum length: 35	
sensitivity <name>	Select a DLP file pattern sensitivity to match. Select a DLP sensitivity.	string	Maximum length: 35	
match-percentage	Percentage of fingerprints in the fingerprint databases designated with the selected sensitivity to match.	integer	Minimum value: 1 Maximum value: 100	10
file-type	Select the number of a DLP file pattern table to match.	integer	Minimum value: 0 Maximum value: 4294967295	0
regexp	Enter a regular expression to match (max. 255 characters).	string	Maximum length: 255	
archive	Enable/disable DLP archiving.	option	-	disable
	Option / **Description** *disable* — No DLP archiving. *enable* — Enable full DLP archiving.			

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

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

expiry	Quarantine duration in days, hours, minutes (format = dddhhmm).	user	Not Specified	5m

config dlp settings

Designate logical storage for DLP fingerprint database.

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

config dlp settings

Parameter	Description	Type	Size	Default
storage-device	Storage device name.	string	Maximum length: 35	
size	Maximum total size of files within the storage (MB).	integer	Minimum value: 16 Maximum value: 4294967295	16
db-mode	Behavior when the maximum size is reached.	option	-	stop-adding

Parameter	Description	Type	Size	Default
	Option / **Description** *stop-adding* — Stop adding entries. *remove-modified-then-oldest* — Remove modified chunks first, then oldest file entries. *remove-oldest* — Remove the oldest files first.			
cache-mem-percent	Maximum percentage of available memory allocated to caching .	integer	Minimum value: 1 Maximum value: 15	2
chunk-size	Maximum fingerprint chunk size. Caution, changing this setting will flush the entire database.	integer	Minimum value: 100 Maximum value: 100000	2800

dnsfilter

This section includes syntax for the following commands:

config dnsfilter domain-filter

Configure DNS domain filters.

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

config dnsfilter domain-filter

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

config entries

Parameter	Description	Type	Size	Default
domain	Domain entries to be filtered.	string	Maximum length: 511	

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

config dnsfilter profile

Configure DNS domain filter profile.

```
config dnsfilter profile
    Description: Configure DNS domain filter profile.
    edit <name>
        set comment {var-string}
        config domain-filter
            Description: Domain filter settings.
            set domain-filter-table {integer}
        end
        config ftgd-dns
            Description: FortiGuard DNS Filter settings.
            set options {option1}, {option2}, ...
            config filters
                Description: FortiGuard DNS domain filters.
                edit <id>
                    set category {integer}
                    set action [block|monitor]
                    set log [enable|disable]
                next
            end
        end
```

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

config dnsfilter profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
log-all-domain	Enable/disable logging of all domains visited (detailed DNS logging).	option	-	disable

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

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

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

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

Parameter	Description	Type	Size	Default
	Option — **Description** *enable* — Enable domain filtering and botnet domain logging. *disable* — Disable domain filtering and botnet domain logging.			
block-action	Action to take for blocked domains.	option	-	redirect
	Option — **Description** *block* — Return NXDOMAIN for blocked domains. *redirect* — Redirect blocked domains to SDNS portal. *block-sevrfail* — Return SERVFAIL for blocked domains.			
redirect-portal	IPv4 address of the SDNS redirect portal.	ipv4-address	Not Specified	0.0.0.0
redirect-portal6	IPv6 address of the SDNS redirect portal.	ipv6-address	Not Specified	::
block-botnet	Enable/disable blocking botnet C&C DNS lookups.	option	-	disable
	Option — **Description** *disable* — Disable blocking botnet C&C DNS lookups. *enable* — Enable blocking botnet C&C DNS lookups.			
safe-search	Enable/disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.	option	-	disable
	Option — **Description** *disable* — Disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search. *enable* — Enable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.			
youtube-restrict	Set safe search for YouTube restriction level.	option	-	strict
	Option — **Description** *strict* — Enable strict safe seach for YouTube. *moderate* — Enable moderate safe search for YouTube.			
external-ip-blocklist `<name>`	One or more external IP block lists. External domain block list name.	string	Maximum length: 79	

config domain-filter

Parameter	Description	Type	Size	Default
domain-filter-table	DNS domain filter table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config ftgd-dns

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

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

config filters

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

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

Parameter	Description	Type	Size	Default
log	Enable/disable DNS filter logging for this DNS profile.	option	-	enable

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

config dns-translation

Parameter	Description	Type	Size	Default
addr-type	DNS translation type (IPv4 or IPv6). **Option** — **Description** *ipv4* — IPv4 address type. *ipv6* — IPv6 address type.	option	-	ipv4
src	IPv4 address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with dst.	ipv4-address	Not Specified	0.0.0.0
dst	IPv4 address or subnet on the external network to substitute for the resolved address in DNS query replies. Can be single IP address or subnet on the external network, but number of addresses must equal number of mapped IP addresses in src.	ipv4-address	Not Specified	0.0.0.0
netmask	If src and dst are subnets rather than single IP addresses, enter the netmask for both src and dst.	ipv4-netmask	Not Specified	255.255.255.255
status	Enable/disable this DNS translation entry. **Option** — **Description** *enable* — Enable this DNS translation. *disable* — Disable this DNS translation.	option	-	enable
src6	IPv6 address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with dst6.	ipv6-address	Not Specified	::
dst6	IPv6 address or subnet on the external network to substitute for the resolved address in DNS query replies. Can be single IP address or subnet on the external network, but number of addresses must equal number of mapped IP addresses in src6.	ipv6-address	Not Specified	::
prefix	If src6 and dst6 are subnets rather than single IP addresses, enter the prefix for both src6 and dst6 .	integer	Minimum value: 1 Maximum value: 128	128

emailfilter

This section includes syntax for the following commands:

config emailfilter block-allow-list

Configure anti-spam block/allow list.

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

config emailfilter block-allow-list

Parameter	Description	Type	Size	Default
name	Name of table.	string	Maximum length: 63	

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

config entries

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

Option	Description
enable	Enable status.
disable	Disable status.

Parameter	Description	Type	Size	Default
type	Entry type.	option	-	ip

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

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

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

Parameter	Description	Type	Size	Default
addr-type	IP address type.	option	-	ipv4

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

Parameter	Description	Type	Size	Default
ip4-subnet	IPv4 network address/subnet mask bits.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
ip6-subnet	IPv6 network address/subnet mask bits.	ipv6-network	Not Specified	::/128
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard

Option	Description
wildcard	Wildcard pattern.

Parameter	Description	Type	Size	Default
	Option — **Description** *regexp* — Perl regular expression.			
email-pattern	Email address pattern.	string	Maximum length: 127	

config emailfilter bword

Configure AntiSpam banned word list.

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

config emailfilter bword

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

config entries

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

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable status. *disable* — Disable status.			
pattern	Pattern for the banned word.	string	Maximum length: 127	
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard
	Option / **Description** *wildcard* — Wildcard pattern. *regexp* — Perl regular expression.			
action	Mark spam or good.	option	-	spam
	Option / **Description** *spam* — Mark as spam email. *clear* — Mark as good email.			
where	Component of the email to be scanned.	option	-	all
	Option / **Description** *subject* — Banned word in email subject. *body* — Banned word in email body. *all* — Banned word in both subject and body.			
language	Language for the banned word.	option	-	western
	Option / **Description** *western* — Western. *simch* — Simplified Chinese. *trach* — Traditional Chinese. *japanese* — Japanese. *korean* — Korean. *french* — French. *thai* — Thai. *spanish* — Spanish.			

Parameter	Description	Type	Size	Default
score	Score value.	integer	Minimum value: 1 Maximum value: 99999	10

config emailfilter dnsbl

Configure AntiSpam DNSBL/ORBL.

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

config emailfilter dnsbl

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

config entries

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

Option	Description
enable	Enable status.

Parameter	Description	Type	Size	Default
	Option **Description** *disable* Disable status.			
server	DNSBL or ORBL server name.	string	Maximum length: 127	
action	Reject connection or mark as spam email.	option	-	spam
	Option **Description** *reject* Reject the connection. *spam* Mark as spam email.			

config emailfilter fortishield

Configure FortiGuard - AntiSpam.

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

config emailfilter fortishield

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

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

config emailfilter iptrust

Configure AntiSpam IP trust.

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

config emailfilter iptrust

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

config entries

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

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable status. *disable* / Disable status.			
addr-type	Type of address.	option	-	ipv4
	Option / **Description** *ipv4* / IPv4 Address type. *ipv6* / IPv6 Address type.			
ip4-subnet	IPv4 network address or network address/subnet mask bits.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
ip6-subnet	IPv6 network address/subnet mask bits.	ipv6-network	Not Specified	::/128

config emailfilter mheader

Configure AntiSpam MIME header.

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

config emailfilter mheader

Parameter	Description	Type	Size	Default
name	Name of table.	string	Maximum length: 63	

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

config entries

Parameter	Description	Type	Size	Default
status	Enable/disable status.	option	-	enable
	Option / **Description**: *enable* — Enable status.; *disable* — Disable status.			
fieldname	Pattern for header field name.	string	Maximum length: 63	
fieldbody	Pattern for the header field body.	string	Maximum length: 127	
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard
	Option / **Description**: *wildcard* — Wildcard pattern.; *regexp* — Perl regular expression.			
action	Mark spam or good.	option	-	spam
	Option / **Description**: *spam* — Mark as spam email.; *clear* — Mark as good email.			

config emailfilter options

Configure AntiSpam options.

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

config emailfilter options

Parameter	Description	Type	Size	Default
dns-timeout	DNS query time out .	integer	Minimum value: 1 Maximum value: 30	7

config emailfilter profile

Configure Email Filter profiles.

```
config emailfilter profile
    Description: Configure Email Filter profiles.
    edit <name>
        set comment {var-string}
        set replacemsg-group {string}
        set spam-log [disable|enable]
        set spam-log-fortiguard-response [disable|enable]
        set spam-filtering [enable|disable]
        set external [enable|disable]
        set options {option1}, {option2}, ...
        config imap
            Description: IMAP.
            set log-all [disable|enable]
            set action [pass|tag]
            set tag-type {option1}, {option2}, ...
            set tag-msg {string}
        end
        config pop3
            Description: POP3.
            set log-all [disable|enable]
            set action [pass|tag]
            set tag-type {option1}, {option2}, ...
            set tag-msg {string}
        end
        config smtp
            Description: SMTP.
            set log-all [disable|enable]
            set action [pass|tag|...]
            set tag-type {option1}, {option2}, ...
            set tag-msg {string}
            set hdrip [disable|enable]
            set local-override [disable|enable]
        end
        config mapi
            Description: MAPI.
            set log-all [disable|enable]
            set action [pass|discard]
        end
        config msn-hotmail
```

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

config emailfilter profile

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

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

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

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

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

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
external	Enable/disable external Email inspection.	option	-	disable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
options	Options.	option	-	
	Option / **Description** *bannedword* / Content block. *spambal* / Block/allow list. *spamfsip* / Email IP address FortiGuard AntiSpam block list check. *spamfssubmit* / Add FortiGuard AntiSpam spam submission text. *spamfschksum* / Email checksum FortiGuard AntiSpam check. *spamfsurl* / Email content URL FortiGuard AntiSpam check. *spamhelodns* / Email helo/ehlo domain DNS check. *spamraddrdns* / Email return address DNS check. *spamrbl* / Email DNSBL & ORBL check. *spamhdrcheck* / Email mime header check. *spamfsphish* / Email content phishing URL FortiGuard AntiSpam check.			
spam-bword-threshold	Spam banned word threshold.	integer	Minimum value: 0 Maximum value: 2147483647	10
spam-bword-table	Anti-spam banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

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

config imap

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	Option / **Description** *disable* — Disable logging of all email traffic. *enable* — Enable logging of all email traffic.			
action	Action for spam email.	option	-	tag
	Option / **Description** *pass* — Allow spam email to pass through. *tag* — Tag spam email with configured text in subject or header.			
tag-type	Tag subject or header for spam email.	option	-	subject spaminfo

Parameter	Description	Type	Size	Default
	Option — **Description** *subject* — Prepend text to spam email subject. *header* — Append a user defined mime header to spam email. *spaminfo* — Append spam info to spam email header.			
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63	Spam

config pop3

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

config smtp

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable

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

config mapi

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable

Option	Description
disable	Disable logging of all email traffic.
enable	Enable logging of all email traffic.

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

Option	Description
pass	Allow spam email to pass through.
discard	Discard (block) spam email.

config msn-hotmail

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable

Option	Description
disable	Disable logging of all email traffic.
enable	Enable logging of all email traffic.

config yahoo-mail

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable

Option	Description
disable	Disable logging of all email traffic.
enable	Enable logging of all email traffic.

config gmail

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Disable logging of all email traffic. *enable* — Enable logging of all email traffic.			

config other-webmails

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	Option / **Description** *disable* — Disable logging of all email traffic. *enable* — Enable logging of all email traffic.			

endpoint-control

This section includes syntax for the following commands:

config endpoint-control fctems

Configure FortiClient Enterprise Management Server (EMS) entries.

```
config endpoint-control fctems
    Description: Configure FortiClient Enterprise Management Server (EMS) entries.
    edit <name>
        set fortinetone-cloud-authentication [enable|disable]
        set server {string}
        set https-port {integer}
        set source-ip {ipv4-address-any}
        set pull-sysinfo [enable|disable]
        set pull-vulnerabilities [enable|disable]
        set pull-avatars [enable|disable]
        set pull-tags [enable|disable]
        set pull-malware-hash [enable|disable]
        set cloud-server-type [production|alpha|...]
        set capabilities {option1}, {option2}, ...
        set call-timeout {integer}
        set websocket-override [disable|enable]
        set preserve-ssl-session [enable|disable]
        set interface-select-method [auto|sdwan|...]
        set interface {string}
    next
end
```

config endpoint-control fctems

Parameter	Description	Type	Size	Default
fortinetone-cloud-authentication	Enable/disable authentication of FortiClient EMS Cloud through FortiCloud account.	option	-	disable

Option	Description
enable	Enable authentication of FortiClient EMS Cloud through the use of FortiCloud account.
disable	Disable authentication of FortiClient EMS Cloud through the use of FortiCloud account.

Parameter	Description	Type	Size	Default
server	FortiClient EMS FQDN or IPv4 address.	string	Maximum length: 255	
https-port	FortiClient EMS HTTPS access port number. .	integer	Minimum value: 1 Maximum value: 65535	443
source-ip	REST API call source IP.	ipv4-address-any	Not Specified	0.0.0.0
pull-sysinfo	Enable/disable pulling SysInfo from EMS.	option	-	enable
	Option / **Description** *enable* — Enable pulling FortiClient user SysInfo from EMS. *disable* — Disable pulling FortiClient user SysInfo from EMS.			
pull-vulnerabilities	Enable/disable pulling vulnerabilities from EMS.	option	-	enable
	Option / **Description** *enable* — Enable pulling client vulnerabilities from EMS. *disable* — Disable pulling client vulnerabilities from EMS.			
pull-avatars	Enable/disable pulling avatars from EMS.	option	-	enable
	Option / **Description** *enable* — Enable pulling FortiClient user avatars from EMS. *disable* — Disable pulling FortiClient user avatars from EMS.			
pull-tags	Enable/disable pulling FortiClient user tags from EMS.	option	-	enable
	Option / **Description** *enable* — Enable pulling FortiClient user tags from EMS. *disable* — Disable pulling FortiClient user tags from EMS.			
pull-malware-hash	Enable/disable pulling FortiClient malware hash from EMS.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable pulling FortiClient malware hash from EMS. *disable* — Disable pulling FortiClient malware hash from EMS.			
cloud-server-type	Cloud server type.	option	-	production
	Option / **Description** *production* — Production FortiClient EMS Cloud Controller. *alpha* — Alpha FortiClient EMS Cloud Controller. *beta* — Beta FortiClient EMS Cloud Controller.			
capabilities	List of EMS capabilities.	option	-	
	Option / **Description** *fabric-auth* — Allow this FortiProxy unit to load the authentication page provided by EMS to authenticate itself with EMS. *silent-approval* — Allow silent approval of non-root or FortiProxy HA clusters on EMS in the Security Fabric. *websocket* — Enable/disable websockets for this FortiProxy unit. Override behavior using websocket-override. *websocket-malware* — Allow this FortiGate unit to request malware hash notifications over websocket. *push-ca-certs* — Enable/disable syncing deep inspection certificates with EMS. *common-tags-api* — Can recieve tag information from New Common Tags API from EMS.			
call-timeout	FortiClient EMS call timeout in seconds .	integer	Minimum value: 1 Maximum value: 180	30
websocket-override	Enable/disable override behavior for how this FortiProxy unit connects to EMS using a WebSocket connection.	option	-	disable
	Option / **Description** *disable* — Do not override the WebSocket connection. Connect to WebSocket of this EMS server if it is capable (default).			

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Override the WebSocket connection. Do not connect to WebSocket even if EMS is capable of a WebSocket connection.			
preserve-ssl-session	Enable/disable preservation of EMS SSL session connection. Warning, most users should not touch this setting.	option	-	disable
	Option / **Description** *enable* / Allow preservation of EMS SSL session connection. *disable* / Don't allow preservation of EMS SSL session connection.			
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* / Set outgoing interface automatically. *sdwan* / Set outgoing interface by SD-WAN or policy routing rules. *specify* / Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

file-filter

This section includes syntax for the following commands:

config file-filter profile

Configure file-filter profiles.

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

config file-filter profile

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

Option	Description
disable	Disable logging.

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

config rules

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
protocol	Protocols to apply rule to.	option	-	http ftp smtp imap pop3 mapi cifs ssh
	Option **Description** *http* Filter on HTTP. *ftp* Filter on FTP. *smtp* Filter on SMTP. *imap* Filter on IMAP. *pop3* Filter on POP3. *mapi* Filter on MAPI. (Proxy mode only.) *cifs* Filter on CIFS. *ssh* Filter on SFTP and SCP. (Proxy mode only.)			
action	Action taken for matched file.	option	-	log-only

Parameter	Description	Type	Size	Default
	Option / **Description** *log-only* — Allow the content and write a log message. *block* — Block the content and write a log message.			
direction	Traffic direction (HTTP, FTP, SSH, CIFS only).	option	-	any
	Option / **Description** *incoming* — Match files transmitted in the session's reply direction. *outgoing* — Match files transmitted in the session's originating direction. *any* — Match files transmitted in the session's originating and reply directions.			
password-protected	Match password-protected files.	option	-	any
	Option / **Description** *yes* — Match only password-protected files. *any* — Match any file.			
file-type `<name>`	Select file type. File type name.	string	Maximum length: 39	

firewall

This section includes syntax for the following commands:

config firewall access-proxy-ssh-client-cert

Configure Access Proxy SSH client certificate.

```
config firewall access-proxy-ssh-client-cert
    Description: Configure Access Proxy SSH client certificate.
    edit <name>
        set source-address [enable|disable]
        set permit-x11-forwarding [enable|disable]
        set permit-agent-forwarding [enable|disable]
        set permit-port-forwarding [enable|disable]
        set permit-pty [enable|disable]
        set permit-user-rc [enable|disable]
        config cert-extension
            Description: Configure certificate extension for user certificate.
            edit <name>
                set critical [no|yes]
                set type [fixed|user]
                set data {string}
            next
```

```
        end
        set auth-ca {string}
    next
end
```

config firewall access-proxy-ssh-client-cert

Parameter	Description	Type	Size	Default
source-address	Enable/disable appending source-address certificate critical option. This option ensure certificate only accepted from FortiGate source address.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
permit-x11-forwarding	Enable/disable appending permit-x11-forwarding certificate extension.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
permit-agent-forwarding	Enable/disable appending permit-agent-forwarding certificate extension.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
permit-port-forwarding	Enable/disable appending permit-port-forwarding certificate extension.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
permit-pty	Enable/disable appending permit-pty certificate extension.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
permit-user-rc	Enable/disable appending permit-user-rc certificate extension.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
auth-ca	Name of the SSH server public key authentication CA.	string	Maximum length: 79	

config cert-extension

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

config firewall access-proxy-virtual-host

Configure Access Proxy virtual hosts.

```
config firewall access-proxy-virtual-host
    Description: Configure Access Proxy virtual hosts.
    edit <name>
        set ssl-certificate {string}
        set host {string}
        set host-type [sub-string|wildcard]
        set replacemsg-group {string}
    next
end
```

config firewall access-proxy-virtual-host

Parameter	Description	Type	Size	Default
ssl-certificate	SSL certificate for this host.	string	Maximum length: 35	
host	The host name.	string	Maximum length: 79	
host-type	Type of host pattern.	option	-	sub-string
	Option / **Description** *sub-string* — Match the pattern if a string contains the sub-string. *wildcard* — Match the pattern with wildcards.			
replacemsg-group	Access-proxy-virtual-host replacement message override group.	string	Maximum length: 35	

config firewall access-proxy

Configure IPv4 access proxy.

```
config firewall access-proxy
    Description: Configure IPv4 access proxy.
    edit <name>
        set vip {string}
        set client-cert [disable|enable]
        set auth-portal [disable|enable]
        set auth-virtual-host {string}
        set empty-cert-action [accept|block]
        set log-blocked-traffic [enable|disable]
        set decrypted-traffic-mirror {string}
        config api-gateway
            Description: Set IPv4 API Gateway.
            edit <id>
                set url-map {string}
                set service [http|https|...]
                set ldb-method [static|round-robin|...]
                set virtual-host {string}
                set url-map-type [sub-string|wildcard|...]
                config realservers
                    Description: Select the real servers that this Access Proxy will
distribute traffic to.
                    edit <id>
                        set addr-type [ip|fqdn]
                        set address {string}
                        set ip {ipv4-address-any}
                        set domain {string}
                        set port {integer}
                        set mappedport {user}
```

```
                        set status [active|standby|...]
                        set type [tcp-forwarding|ssh]
                        set weight {integer}
                        set http-host {string}
                        set health-check [disable|enable]
                        set health-check-proto [ping|http|...]
                        set holddown-interval [enable|disable]
                        set ssh-client-cert {string}
                        set ssh-host-key-validation [disable|enable]
                        set ssh-host-key <name1>, <name2>, ...
                    next
                end
                set persistence [none|http-cookie]
                set http-cookie-domain-from-host [disable|enable]
                set http-cookie-domain {string}
                set http-cookie-path {string}
                set http-cookie-generation {integer}
                set http-cookie-age {integer}
                set http-cookie-share [disable|same-ip]
                set https-cookie-secure [disable|enable]
                set saml-server {string}
                set saml-redirect [disable|enable]
                set ssl-dh-bits [768|1024|...]
                set ssl-algorithm [high|medium|...]
                config ssl-cipher-suites
                    Description: SSL/TLS cipher suites to offer to a server, ordered by
priority.
                    edit <priority>
                        set cipher [TLS-RSA-WITH-3DES-EDE-CBC-SHA|TLS-DHE-RSA-WITH-DES-CBC-
SHA|...]
                        set versions {option1}, {option2}, ...
                    next
                end
                set ssl-min-version [tls-1.0|tls-1.1|...]
                set ssl-max-version [tls-1.0|tls-1.1|...]
                set ssl-vpn-web-portal {string}
            next
        end
        config api-gateway6
            Description: Set IPv6 API Gateway.
            edit <id>
                set url-map {string}
                set service [http|https|...]
                set ldb-method [static|round-robin|...]
                set virtual-host {string}
                set url-map-type [sub-string|wildcard|...]
                config realservers
                    Description: Select the real servers that this Access Proxy will
distribute traffic to.
                    edit <id>
                        set addr-type [ip|fqdn]
                        set address {string}
                        set ip {ipv6-address}
                        set domain {string}
                        set port {integer}
                        set mappedport {user}
```

```
                        set status [active|standby|...]
                        set type [tcp-forwarding|ssh]
                        set weight {integer}
                        set http-host {string}
                        set health-check [disable|enable]
                        set health-check-proto [ping|http|...]
                        set holddown-interval [enable|disable]
                        set ssh-client-cert {string}
                        set ssh-host-key-validation [disable|enable]
                        set ssh-host-key <name1>, <name2>, ...
                    next
                end
                set persistence [none|http-cookie]
                set http-cookie-domain-from-host [disable|enable]
                set http-cookie-domain {string}
                set http-cookie-path {string}
                set http-cookie-generation {integer}
                set http-cookie-age {integer}
                set http-cookie-share [disable|same-ip]
                set https-cookie-secure [disable|enable]
                set saml-server {string}
                set saml-redirect [disable|enable]
                set ssl-dh-bits [768|1024|...]
                set ssl-algorithm [high|medium|...]
                config ssl-cipher-suites
                    Description: SSL/TLS cipher suites to offer to a server, ordered by
priority.
                    edit <priority>
                        set cipher [TLS-RSA-WITH-3DES-EDE-CBC-SHA|TLS-DHE-RSA-WITH-DES-CBC-
SHA|...]
                        set versions {option1}, {option2}, ...
                    next
                end
                set ssl-min-version [tls-1.0|tls-1.1|...]
                set ssl-max-version [tls-1.0|tls-1.1|...]
                set ssl-vpn-web-portal {string}
            next
        end
    next
end
```

config firewall access-proxy

Parameter	Description	Type	Size	Default
vip	Virtual IP name.	string	Maximum length: 79	
client-cert	Enable/disable to request client certificate.	option	-	disable

Option	Description
disable	Disable client certificate request.

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable client certificate request.			
auth-portal	Enable/disable authentication portal.	option	-	disable
	Option **Description** *disable* Disable authentication portal. *enable* Enable authentication portal.			
auth-virtual-host	Virtual host for authentication portal.	string	Maximum length: 79	
empty-cert-action	Action of an empty client certificate.	option	-	block
	Option **Description** *accept* Accept the SSL handshake if the client certificate is empty. *block* Block the SSL handshake if the client certificate is empty.			
log-blocked-traffic	Enable/disable logging of blocked traffic.	option	-	disable
	Option **Description** *enable* Log all traffic denied by this access proxy. *disable* Do not log all traffic denied by this access proxy.			
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35	

config api-gateway

Parameter	Description	Type	Size	Default
url-map	URL pattern to match.	string	Maximum length: 511	/
service	Service.	option	-	https
	Option **Description** *http* HTTP *https* HTTPS			

Parameter	Description	Type	Size	Default
	Option / **Description** *tcp-forwarding* — TCP-FORWARDING *samlsp* — SAML-SP *web-portal* — VPN-SSL-WEB-PORTAL			
ldb-method	Method used to distribute sessions to real servers. **Option** / **Description** *static* — Distribute to server based on source IP. *round-robin* — Distribute to server based round robin order. *weighted* — Distribute to server based on weight. *first-alive* — Distribute to the first server that is alive. *http-host* — Distribute to server based on host field in HTTP header.	option	-	static
virtual-host	Virtual host.	string	Maximum length: 79	
url-map-type	Type of url-map. **Option** / **Description** *sub-string* — Match the pattern if a string contains the sub-string. *wildcard* — Match the pattern with wildcards. *regex* — Match the pattern with a regular expression.	option	-	sub-string
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session. **Option** / **Description** *none* — None. *http-cookie* — HTTP cookie.	option	-	none
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP. **Option** / **Description** *disable* — Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting). *enable* — Enable use of HTTP cookie domain from host field in HTTP.	option	-	disable

Parameter	Description	Type	Size	Default
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35	
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35	
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60
http-cookie-share	Control sharing of cookies across API Gateway. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip

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

Parameter	Description	Type	Size	Default
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable

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

Parameter	Description	Type	Size	Default
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35	
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	disable

Option	Description
disable	Do not support redirection after successful SAML authentication.
enable	Support redirection after successful SAML authentication.

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

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

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

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

ssl-min-version	Lowest SSL/TLS version acceptable from a server.	option	-	tls-1.0

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

ssl-max-version	Highest SSL/TLS version acceptable from a server.	option	-	tls-1.2

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

ssl-vpn-web-portal	SSL-VPN web portal.	string	Maximum length: 35	

config realservers

Parameter	Description	Type	Size	Default
addr-type	Type of address.	option	-	ip
	Option / **Description** *ip* — Standard IPv4 address. *fqdn* — Non-wildcard FQDN address object.			
address	Address or address group of the real server.	string	Maximum length: 79	
ip	IPv6 address of the real server.	ipv6-address	Not Specified	::
domain	Wildcard domain name of the real server.	string	Maximum length: 255	
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443
mappedport	Port for communicating with the real server.	user	Not Specified	
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active
	Option / **Description** *active* — Server status active. *standby* — Server status standby. *disable* — Server status disable.			
type	TCP forwarding server type.	option	-	tcp-forwarding
	Option / **Description** *tcp-forwarding* — TCP forwarding. *ssh* — SSH.			
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1

Parameter	Description	Type	Size	Default
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63	
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable
	Option / **Description** *disable* — Disable per server health check. *enable* — Enable per server health check.			
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping
	Option / **Description** *ping* — Use PING to test the link with the server. *http* — Use HTTP-GET to test the link with the server. *tcp-connect* — Use a full TCP connection to test the link with the server.			
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable
	Option / **Description** *enable* — Enable per server holddown. *disable* — Disable per server holddown.			
ssh-client-cert	Set access-proxy SSH client certificate profile.	string	Maximum length: 79	
ssh-host-key-validation	Enable/disable SSH real server host key validation.	option	-	disable
	Option / **Description** *disable* — Disable SSH real server host key validation. *enable* — Enable SSH real server host key validation.			
ssh-host-key `<name>`	One or more server host key. Server host key name.	string	Maximum length: 79	

config ssl-cipher-suites

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

Parameter	Description	Type	Size	Default
	Option / **Description** *TLS-RSA-WITH-3DES-EDE-CBC-SHA* — Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-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.			
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	tls-1.0 tls-1.1 tls-1.2
	Option / **Description** *tls-1.0* — TLS 1.0. *tls-1.1* — TLS 1.1. *tls-1.2* — TLS 1.2.			

config api-gateway6

Parameter	Description	Type	Size	Default
url-map	URL pattern to match.	string	Maximum length: 511	/
service	Service.	option	-	https
	Option / **Description** *http* — HTTP *https* — HTTPS *tcp-forwarding* — TCP-FORWARDING *samlsp* — SAML-SP *web-portal* — VPN-SSL-WEB-PORTAL			
ldb-method	Method used to distribute sessions to real servers.	option	-	static
	Option / **Description** *static* — Distribute to server based on source IP.			

Parameter	Description	Type	Size	Default
	Option / **Description** *round-robin* — Distribute to server based round robin order. *weighted* — Distribute to server based on weight. *first-alive* — Distribute to the first server that is alive. *http-host* — Distribute to server based on host field in HTTP header.			
virtual-host	Virtual host.	string	Maximum length: 79	
url-map-type	Type of url-map.	option	-	sub-string
	Option / **Description** *sub-string* — Match the pattern if a string contains the sub-string. *wildcard* — Match the pattern with wildcards. *regex* — Match the pattern with a regular expression.			
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none
	Option / **Description** *none* — None. *http-cookie* — HTTP cookie.			
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable
	Option / **Description** *disable* — Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting). *enable* — Enable use of HTTP cookie domain from host field in HTTP.			
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35	
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60
http-cookie-share	Control sharing of cookies across API Gateway. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip

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

Parameter	Description	Type	Size	Default
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable

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

Parameter	Description	Type	Size	Default
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35	
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	disable

Option	Description
disable	Do not support redirection after successful SAML authentication.
enable	Support redirection after successful SAML authentication.

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

Option	Description
768	768-bit Diffie-Hellman prime.

Parameter	Description	Type	Size	Default
	Option / **Description** *1024* — 1024-bit Diffie-Hellman prime. *1536* — 1536-bit Diffie-Hellman prime. *2048* — 2048-bit Diffie-Hellman prime. *3072* — 3072-bit Diffie-Hellman prime. *4096* — 4096-bit Diffie-Hellman prime.			
ssl-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength. **Option** / **Description** *high* — High encryption. Allow only AES and ChaCha. *medium* — Medium encryption. Allow AES, ChaCha, 3DES, and RC4. *low* — Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.	option	-	high
ssl-min-version	Lowest SSL/TLS version acceptable from a server. **Option** / **Description** *tls-1.0* — TLS 1.0. *tls-1.1* — TLS 1.1. *tls-1.2* — TLS 1.2.	option	-	tls-1.0
ssl-max-version	Highest SSL/TLS version acceptable from a server. **Option** / **Description** *tls-1.0* — TLS 1.0. *tls-1.1* — TLS 1.1. *tls-1.2* — TLS 1.2.	option	-	tls-1.2
ssl-vpn-web-portal	SSL-VPN web portal.	string	Maximum length: 35	

config realservers

Parameter	Description	Type	Size	Default
addr-type	Type of address.	option	-	ip

Parameter	Description	Type	Size	Default
address	Address or address group of the real server.	string	Maximum length: 79	
ip	IPv6 address of the real server.	ipv6-address	Not Specified	::
domain	Wildcard domain name of the real server.	string	Maximum length: 255	
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443
mappedport	Port for communicating with the real server.	user	Not Specified	
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active
type	TCP forwarding server type.	option	-	tcp-forwarding
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63	
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable
ssh-client-cert	Set access-proxy SSH client certificate profile.	string	Maximum length: 79	
ssh-host-key-validation	Enable/disable SSH real server host key validation.	option	-	disable
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79	

config ssl-cipher-suites

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

config firewall access-proxy6

Configure IPv6 access proxy.

```
config firewall access-proxy6
    Description: Configure IPv6 access proxy.
    edit <name>
        set vip {string}
    next
end
```

config firewall access-proxy6

Parameter	Description	Type	Size	Default
vip	Virtual IP name.	string	Maximum length: 79	

config firewall address

Configure IPv4 addresses.

```
config firewall address
    Description: Configure IPv4 addresses.
    edit <name>
        set uuid {uuid}
        set subnet {ipv4-classnet-any}
        set type [ipmask|iprange|...]
        set sub-type [sdn|clearpass-spt|...]
        set clearpass-spt [unknown|healthy|...]
        set start-ip {ipv4-address-any}
        set end-ip {ipv4-address-any}
        set fqdn {string}
        set country {string}
        set wildcard-fqdn {string}
        set pattern-start {integer}
        set pattern-end {integer}
        set cache-ttl {integer}
```

```
            set wildcard {ipv4-classnet-any}
            set sdn {string}
            set fsso-group <name1>, <name2>, ...
            set interface {string}
            set tenant {string}
            set organization {string}
            set epg-name {string}
            set subnet-name {string}
            set sdn-tag {string}
            set policy-group {string}
            set obj-tag {string}
            set obj-type [ip|mac]
            set tag-detection-level {string}
            set tag-type {string}
            set comment {var-string}
            set associated-interface {string}
            set color {integer}
            set filter {var-string}
            set sdn-addr-type [private|public|...]
            set node-ip-only [enable|disable]
            set obj-id {var-string}
            config list
                Description: IP address list.
                edit <ip>
                next
            end
            config tagging
                Description: Config object tagging.
                edit <name>
                    set category {string}
                    set tags <name1>, <name2>, ...
                next
            end
            set allow-routing [enable|disable]
            set fabric-object [enable|disable]
        next
    end
```

config firewall address

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
subnet	IP address and subnet mask of address.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
type	Type of address.	option	-	ipmask

Parameter	Description	Type	Size	Default
	Option / **Description** *ipmask* — Standard IPv4 address with subnet mask. *iprange* — Range of IPv4 addresses between two specified addresses (inclusive). *fqdn* — Fully Qualified Domain Name address. *fqdn-group* — Fully Qualified Domain Name Group address. *geography* — IP addresses from a specified country. *wildcard* — Standard IPv4 using a wildcard subnet mask. *dynamic* — Dynamic address object. *interface-subnet* — IP and subnet of interface.			
sub-type	Sub-type of address.	option	-	sdn
	Option / **Description** *sdn* — SDN address. *clearpass-spt* — ClearPass SPT (System Posture Token) address. *fsso* — FSSO address. *ems-tag* — FortiClient EMS tag. *fortivoice-tag* — FortiVoice tag. *fortinac-tag* — FortiNAC tag. *swc-tag* — Switch Controller NAC policy tag.			
clearpass-spt	SPT (System Posture Token) value.	option	-	unknown
	Option / **Description** *unknown* — UNKNOWN. *healthy* — HEALTHY. *quarantine* — QUARANTINE. *checkup* — CHECKUP. *transient* — TRANSIENT. *infected* — INFECTED.			
start-ip	First IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
end-ip	Final IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0
fqdn	Fully Qualified Domain Name address.	string	Maximum length: 255	
country	IP addresses associated to a specific country.	string	Maximum length: 2	
wildcard-fqdn	Fully Qualified Domain Name with wildcard characters.	string	Maximum length: 255	
pattern-start	Starting number of pattern for fqdn-group.	integer	Minimum value: 0 Maximum value: 65535	0
pattern-end	Ending number of pattern for fqdn-group.	integer	Minimum value: 0 Maximum value: 65535	0
cache-ttl	Defines the minimal TTL of individual IP addresses in FQDN cache measured in seconds.	integer	Minimum value: 0 Maximum value: 86400	0
wildcard	IP address and wildcard netmask.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
sdn	SDN.	string	Maximum length: 35	
fsso-group <name>	FSSO group(s). FSSO group name.	string	Maximum length: 511	
interface	Name of interface whose IP address is to be used.	string	Maximum length: 35	
tenant	Tenant.	string	Maximum length: 35	
organization	Organization domain name (Syntax: organization/domain).	string	Maximum length: 35	
epg-name	Endpoint group name.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default
subnet-name	Subnet name.	string	Maximum length: 255	
sdn-tag	SDN Tag.	string	Maximum length: 15	
policy-group	Policy group name.	string	Maximum length: 15	
obj-tag	Tag of dynamic address object.	string	Maximum length: 255	
obj-type	Object type.	option	-	ip
	Option / **Description** *ip* — IP address. *mac* — MAC address			
tag-detection-level	Tag detection level of dynamic address object.	string	Maximum length: 15	
tag-type	Tag type of dynamic address object.	string	Maximum length: 63	
comment	Comment.	var-string	Maximum length: 255	
associated-interface	Network interface associated with address.	string	Maximum length: 35	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
filter	Match criteria filter.	var-string	Maximum length: 2047	
sdn-addr-type	Type of addresses to collect.	option	-	private
	Option / **Description** *private* — Collect private addresses only. *public* — Collect public addresses only. *all* — Collect both public and private addresses.			
node-ip-only	Enable/disable collection of node addresses only in Kubernetes.	option	-	disable

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

config tagging

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

config firewall address6-template

Configure IPv6 address templates.

```
config firewall address6-template
    Description: Configure IPv6 address templates.
    edit <name>
        set ip6 {ipv6-network}
        set subnet-segment-count {integer}
        config subnet-segment
            Description: IPv6 subnet segments.
            edit <id>
                set name {string}
```

```
                set bits {integer}
                set exclusive [enable|disable]
                config values
                    Description: Subnet segment values.
                    edit <name>
                        set value {string}
                    next
                end
            next
        end
        set fabric-object [enable|disable]
    next
end
```

config firewall address6-template

Parameter	Description	Type	Size	Default
ip6	IPv6 address prefix.	ipv6-network	Not Specified	::/0
subnet-segment-count	Number of IPv6 subnet segments.	integer	Minimum value: 1 Maximum value: 6	0
fabric-object	Security Fabric global object setting.	option	-	disable

Option	Description
enable	Object is set as a security fabric-wide global object.
disable	Object is local to this security fabric member.

config subnet-segment

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

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

config values

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

config firewall address6

Configure IPv6 firewall addresses.

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

config firewall address6

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
type	Type of IPv6 address object .	option	-	ipprefix
	Option / **Description** *ipprefix* — Uses the IP prefix to define a range of IPv6 addresses. *iprange* — Range of IPv6 addresses between two specified addresses (inclusive). *fqdn* — Fully qualified domain name. *geography* — IPv6 addresses from a specified country. *dynamic* — Dynamic address object for SDN. *template* — Template.			
sdn	SDN.	string	Maximum length: 35	
ip6	IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx).	ipv6-network	Not Specified	::/0
start-ip	First IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::
end-ip	Final IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::
fqdn	Fully qualified domain name.	string	Maximum length: 255	
country	IPv6 addresses associated to a specific country.	string	Maximum length: 2	
cache-ttl	Minimal TTL of individual IPv6 addresses in FQDN cache.	integer	Minimum value: 0 Maximum value: 86400	0
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0

Parameter	Description	Type	Size	Default
obj-id	Object ID for NSX.	var-string	Maximum length: 255	
comment	Comment.	var-string	Maximum length: 255	
template	IPv6 address template.	string	Maximum length: 63	
host-type	Host type.	option	-	any
	Option / **Description** *any* — Wildcard. *specific* — Specific host address.			
host	Host Address.	ipv6-address	Not Specified	::
fabric-object	Security Fabric global object setting.	option	-	disable
	Option / **Description** *enable* — Object is set as a security fabric-wide global object. *disable* — Object is local to this security fabric member.			

config tagging

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

config subnet-segment

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

config firewall addrgrp

Configure IPv4 address groups.

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

config firewall addrgrp

Parameter	Description	Type	Size	Default
type	Address group type.	option	-	default
	Option / **Description** *default* — Default address group type (address may belong to multiple groups). *folder* — Address folder group (members may not belong to any other group).			
category	Address group category.	option	-	default
	Option / **Description** *default* — Default address group category (cannot be used as ztna-ems-tag in policy). *ztna-ems-tag* — Members must be ztna-ems-tag group or ems-tag address, can be used as ztna-ems-tag in policy.			
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

Parameter	Description	Type	Size	Default
member <name>	Address objects contained within the group. Address name.	string	Maximum length: 79	
comment	Comment.	var-string	Maximum length: 255	
exclude	Enable/disable address exclusion.	option	-	disable
	Option / **Description** *enable* — Enable address exclusion. *disable* — Disable address exclusion.			
exclude-member <name>	Address exclusion member. Address name.	string	Maximum length: 79	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
allow-routing	Enable/disable use of this group in the static route configuration.	option	-	disable
	Option / **Description** *enable* — Enable use of this group in the static route configuration. *disable* — Disable use of this group in the static route configuration.			
fabric-object	Security Fabric global object setting.	option	-	disable
	Option / **Description** *enable* — Object is set as a security fabric-wide global object. *disable* — Object is local to this security fabric member.			

config tagging

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

config firewall addrgrp6

Configure IPv6 address groups.

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

config firewall addrgrp6

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	
member <name>	Address objects contained within the group. Address6/addrgrp6 name.	string	Maximum length: 79	
fabric-object	Security Fabric global object setting.	option	-	disable

Option	Description
enable	Object is set as a security fabric-wide global object.
disable	Object is local to this security fabric member.

config tagging

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

config firewall auth-portal

Configure firewall authentication portals.

```
config firewall auth-portal
    Description: Configure firewall authentication portals.
    set groups <name1>, <name2>, ...
    set portal-addr {string}
    set portal-addr6 {string}
    set identity-based-route {string}
end
```

config firewall auth-portal

Parameter	Description	Type	Size	Default
groups <name>	Firewall user groups permitted to authenticate through this portal. Separate group names with spaces. Group name.	string	Maximum length: 79	
portal-addr	Address (or FQDN) of the authentication portal.	string	Maximum length: 63	
portal-addr6	IPv6 address (or FQDN) of authentication portal.	string	Maximum length: 63	
identity-based-route	Name of the identity-based route that applies to this portal.	string	Maximum length: 35	

config firewall central-snat-map

Configure central SNAT policies.

```
config firewall central-snat-map
    Description: Configure central SNAT policies.
    edit <policyid>
        set status [enable|disable]
```

```
        set action [bypass|masquerade|...]
        set ipv6 [enable|disable]
        set srcintf {string}
        set dstintf {string}
        set src-addr <name1>, <name2>, ...
        set src-addr6 <name1>, <name2>, ...
        set dst-addr <name1>, <name2>, ...
        set dst-addr6 <name1>, <name2>, ...
        set nat-ippool <name1>, <name2>, ...
        set nat-ippool6 <name1>, <name2>, ...
    next
end
```

config firewall central-snat-map

Parameter	Description	Type	Size	Default
status	Enable/disable the active status of this policy.	option	-	enable
	Option / **Description** *enable* — Enable this policy. *disable* — Disable this policy.			
action	central SNAT action.	option	-	masquerade
	Option / **Description** *bypass* — Bypass and do not perform NAT. *masquerade* — NAT using the primary IP of destination interface. *ippool* — NAT using ip pool.			
ipv6	Enable/disable IPv6.	option	-	disable
	Option / **Description** *enable* — Enable ipv6. *disable* — Disable ipv6.			
srcintf	Source interface name from available interfaces.	string	Maximum length: 35	
dstintf	Destination interface name from available interfaces.	string	Maximum length: 35	
src-addr <name>	IPv4 Original address. Address name.	string	Maximum length: 79	
src-addr6 <name>	IPv6 Original address. Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
dst-addr <name>	IPv4 Destination address. Address name.	string	Maximum length: 79	
dst-addr6 <name>	IPv6 Destination address. Address name.	string	Maximum length: 79	
nat-ippool <name>	Name of the IP pools to be used to translate addresses from available IP Pools. IP pool name.	string	Maximum length: 79	
nat-ippool6 <name>	IPv6 pools to be used for source NAT. IP pool name.	string	Maximum length: 79	

config firewall city

Define city table.

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

config firewall city

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

config firewall country

Define country table.

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

config firewall country

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

config firewall decrypted-traffic-mirror

Configure decrypted traffic mirror.

```
config firewall decrypted-traffic-mirror
    Description: Configure decrypted traffic mirror.
    edit <name>
        set dstmac {mac-address}
        set traffic-type {option1}, {option2}, ...
        set traffic-source [client|server|...]
        set interface <name1>, <name2>, ...
    next
end
```

config firewall decrypted-traffic-mirror

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

Option	Description
ssl	Mirror decrypted SSL traffic.
ssh	Mirror decrypted SSH traffic.

Parameter	Description	Type	Size	Default
traffic-source	Source of decrypted traffic to be mirrored.	option	-	client

Option	Description
client	Mirror client side decrypted traffic.
server	Mirror server side decrypted traffic.

Parameter	Description	Type	Size	Default
	Option **Description** *both* Mirror both client and server side decrypted traffic.			
interface <name>	Decrypted traffic mirror interface. Decrypted traffic mirror interface.	string	Maximum length: 79	

config firewall identity-based-route

Configure identity based routing.

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

config firewall identity-based-route

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

config rule

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

Parameter	Description	Type	Size	Default
	Group name.			

config firewall internet-service-addition

Configure Internet Services Addition.

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

config firewall internet-service-addition

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

config entry

Parameter	Description	Type	Size	Default
protocol	Integer value for the protocol type as defined by IANA (only TCP is supported).	integer	Minimum value: 6 Maximum value: 6	6

config port-range

Parameter	Description	Type	Size	Default
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

config firewall internet-service-append

Configure additional port mappings for Internet Services.

```
config firewall internet-service-append
    Description: Configure additional port mappings for Internet Services.
    set match-port {integer}
    set append-port {integer}
end
```

config firewall internet-service-append

Parameter	Description	Type	Size	Default
match-port	Matching TCP/UDP/SCTP destination port (0 to 65535, 0 means any port).	integer	Minimum value: 0 Maximum value: 65535	0
append-port	Appending TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	0

config firewall internet-service-botnet

Show Internet Service botnet.

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

config firewall internet-service-botnet

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

config firewall internet-service-custom-group

Configure custom Internet Service group.

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

config firewall internet-service-custom-group

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

config firewall internet-service-custom

Configure custom Internet Services.

```
config firewall internet-service-custom
    Description: Configure custom Internet Services.
    edit <name>
        set reputation {integer}
        set comment {var-string}
        config entry
```

```
            Description: Entries added to the Internet Service database and custom database.
            edit <id>
                set protocol {integer}
                config port-range
                    Description: Port ranges in the custom entry.
                    edit <id>
                        set start-port {integer}
                        set end-port {integer}
                    next
                end
                set dst <name1>, <name2>, ...
            next
        end
    next
end
```

config firewall internet-service-custom

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

config entry

Parameter	Description	Type	Size	Default
protocol	Integer value for the protocol type as defined by IANA (only TCP is supported).	integer	Minimum value: 6 Maximum value: 6	6
dst <name>	Destination address or address group name. Select the destination address or address group object from available options.	string	Maximum length: 79	

config port-range

Parameter	Description	Type	Size	Default
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

config firewall internet-service-definition

Configure Internet Service definition.

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

config entry

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

config port-range

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

config firewall internet-service-extension

Configure Internet Services Extension.

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

```
                    set end-port {integer}
                next
            end
            set dst <name1>, <name2>, ...
        next
    end
    config disable-entry
        Description: Disable entries in the Internet Service database.
        edit <id>
            set protocol {integer}
            config port-range
                Description: Port ranges in the disable entry.
                edit <id>
                    set start-port {integer}
                    set end-port {integer}
                next
            end
            config ip-range
                Description: IP ranges in the disable entry.
                edit <id>
                    set start-ip {ipv4-address-any}
                    set end-ip {ipv4-address-any}
                next
            end
        next
    end
next
end
```

config firewall internet-service-extension

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

config entry

Parameter	Description	Type	Size	Default
protocol	Integer value for the protocol type as defined by IANA (only TCP is supported).	integer	Minimum value: 6 Maximum value: 6	6
dst <name>	Destination address or address group name. Select the destination address or address group object from available options.	string	Maximum length: 79	

config port-range

Parameter	Description	Type	Size	Default
start-port	Starting TCP/UDP/SCTP destination port (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1
end-port	Ending TCP/UDP/SCTP destination port (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

config disable-entry

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

config port-range

Parameter	Description	Type	Size	Default
start-port	Starting TCP/UDP/SCTP destination port (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1
end-port	Ending TCP/UDP/SCTP destination port (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

config ip-range

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

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

config firewall internet-service-group

Configure group of Internet Service.

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

config firewall internet-service-group

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
direction	How this service may be used (source, destination or both).	option	-	both
	Option / **Description** *source* — As source when applied. *destination* — As destination when applied. *both* — Both directions when applied.			
member <name>	Internet Service group member. Internet Service name.	string	Maximum length: 79	

config firewall internet-service-ipbl-reason

IP block list reason.

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

```
    next
end
```

config firewall internet-service-ipbl-reason

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

config firewall internet-service-ipbl-vendor

IP block list vendor.

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

config firewall internet-service-ipbl-vendor

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

config firewall internet-service-list

Internet Service list.

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

config firewall internet-service-list

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

config firewall internet-service-name

Define internet service names.

```
config firewall internet-service-name
    Description: Define internet service names.
    edit <name>
        set type [default|location]
        set internet-service-id {integer}
        set country-id {integer}
        set region-id {integer}
        set city-id {integer}
    next
end
```

config firewall internet-service-name

Parameter	Description	Type	Size	Default
type	Internet Service name type.	option	-	default
	Option / **Description** *default* — Automatically generated Internet Service. *location* — Geography location based Internet Service.			
internet-service-id	Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
country-id	Country or Area ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
region-id	Region ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
city-id	City ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config firewall internet-service-owner

Internet Service owner.

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

config firewall internet-service-owner

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

config firewall internet-service-reputation

Show Internet Service reputation.

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

config firewall internet-service-reputation

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	

config firewall internet-service-sld

Internet Service Second Level Domain.

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

config firewall internet-service-sld

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

config firewall internet-service

Show Internet Service application.

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

config firewall internet-service

Parameter	Description	Type	Size	Default
name	Internet Service name.	string	Maximum length: 63	
icon-id	Icon ID of Internet Service.	integer	Minimum value: 0 Maximum value: 4294967295	0
direction	How this service may be used in a firewall policy (source, destination or both).	option	-	both

Option	Description
src	As source in the firewall policy.
dst	As destination in the firewall policy.
both	Both directions in the firewall policy.

Parameter	Description	Type	Size	Default
database	Database name this Internet Service belongs to.	option	-	isdb

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

Parameter	Description	Type	Size	Default
ip-range-number	Number of IP ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0
extra-ip-range-number	Extra number of IP ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip-number	Total number of IP addresses.	integer	Minimum value: 0 Maximum value: 4294967295	0
singularity	Singular level of the Internet Service.	integer	Minimum value: 0 Maximum value: 65535	0

Parameter	Description	Type	Size	Default
obsolete	Indicates whether the Internet Service can be used.	integer	Minimum value: 0 Maximum value: 255	0

config firewall ippool

Configure IPv4 IP pools.

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

config firewall ippool

Parameter	Description	Type	Size	Default
startip	First IPv4 address (inclusive) in the range for the address pool (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0
endip	Final IPv4 address (inclusive) in the range for the address pool (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0
comments	Comment.	var-string	Maximum length: 255	

config firewall ippool6

Configure IPv6 IP pools.

```
config firewall ippool6
    Description: Configure IPv6 IP pools.
    edit <name>
        set startip {ipv6-address}
        set endip {ipv6-address}
        set comments {var-string}
        set nat46 [disable|enable]
        set add-nat46-route [disable|enable]
```

```
    next
end
```

config firewall ippool6

Parameter	Description	Type	Size	Default
startip	First IPv6 address .	ipv6-address	Not Specified	::
endip	Final IPv6 address .	ipv6-address	Not Specified	::
comments	Comment.	var-string	Maximum length: 255	
nat46	Enable/disable NAT46.	option	-	disable
	Option / **Description** *disable* — Disable NAT46. *enable* — Enable NAT46.			
add-nat46-route	Enable/disable adding NAT46 route.	option	-	enable
	Option / **Description** *disable* — Disable adding NAT46 route. *enable* — Enable adding NAT46 route.			

config firewall policy

Configure firewall policies.

```
config firewall policy
    Description: Configure firewall policies.
    edit <policyid>
        set type [explicit-web|transparent|...]
        set status [enable|disable]
        set name {string}
        set uuid {uuid}
        set force-proxy [enable|disable]
        set dynamic-bypass [enable|disable]
        set srcintf <name1>, <name2>, ...
        set dstintf <name1>, <name2>, ...
        set srcaddr <name1>, <name2>, ...
        set dstaddr <name1>, <name2>, ...
        set srcaddr6 <name1>, <name2>, ...
        set dstaddr6 <name1>, <name2>, ...
```

```
set action [accept|deny|...]
set schedule {string}
set service <name1>, <name2>, ...
set explicit-web-proxy {string}
set transparent [enable|disable]
set access-proxy <name1>, <name2>, ...
set ztna-ems-tag <name1>, <name2>, ...
set ztna-tags-match-logic [or|and]
set device-ownership [enable|disable]
set internet-service [enable|disable]
set pass-through [enable|disable]
set internet-service-name <name1>, <name2>, ...
set internet-service-custom <name1>, <name2>, ...
set utm-status [enable|disable]
set webproxy-profile {string}
set logtraffic [all|utm|...]
set logtraffic-start [enable|disable]
set log-http-transaction [enable|disable]
set wanopt [enable|disable]
set wanopt-detection [active|passive|...]
set wanopt-passive-opt [default|transparent|...]
set wanopt-profile {string}
set wanopt-peer {string}
set webcache [enable|disable]
set webcache-https [disable|enable]
set reverse-cache [disable|enable]
set http-tunnel-auth [enable|disable]
set ssh-policy-check [enable|disable]
set webproxy-forward-server {string}
set isolator-server {string}
set poolname <name1>, <name2>, ...
set groups <name1>, <name2>, ...
set users <name1>, <name2>, ...
set disclaimer [disable|domain|...]
set comments {var-string}
set redirect-url {var-string}
set custom-log-fields <field-id1>, <field-id2>, ...
set replacemsg-override-group {string}
set srcaddr-negate [enable|disable]
set dstaddr-negate [enable|disable]
set service-negate [enable|disable]
set internet-service-negate [enable|disable]
set decrypted-traffic-mirror {string}
set max-session-per-user {integer}
set profile-type [single|group]
set profile-group {string}
set profile-protocol-options {string}
set ssl-ssh-profile {string}
set av-profile {string}
set ia-profile {string}
set webfilter-profile {string}
set dnsfilter-profile {string}
set emailfilter-profile {string}
set dlp-sensor {string}
set file-filter-profile {string}
set ips-sensor {string}
```

```
        set application-list {string}
        set icap-profile {string}
        set cifs-profile {string}
        set videofilter-profile {string}
        set isolator-profile {string}
        set ssh-filter-profile {string}
    next
end
```

config firewall policy

Parameter	Description	Type	Size	Default
type	Type of policy.	option	-	transparent
	Option / **Description** *explicit-web* — Explicit Web Proxy policy *transparent* — Transparent firewall policy *explicit-ftp* — Explicit FTP Proxy policy *ssh-tunnel* — SSH Tunnel policy *ssh* — SSH policy *access-proxy* — Access Proxy *wanopt* — WANopt Tunnel			
status	Enable or disable this policy.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
name	Policy name.	string	Maximum length: 35	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
force-proxy	Force proxy.	option	-	disable
	Option / **Description** *enable* — Force all TCP transparent traffic to proxy. *disable* — Do not force TCP transparent traffic to proxy.			
dynamic-bypass	Dynamic bypass.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable dynamic bypass to all HTTP traffic in this policy. *disable* — Disable dynamic bypass to all HTTP traffic in this policy.			
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79	
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79	
srcaddr <name>	Source address and address group names. Address name.	string	Maximum length: 79	
dstaddr <name>	Destination address and address group names. Address name.	string	Maximum length: 79	
srcaddr6 <name>	IPv6 source address (web proxy only). Address name.	string	Maximum length: 79	
dstaddr6 <name>	IPv6 destination address (web proxy only). Address name.	string	Maximum length: 79	
action	Policy action (allow/deny).	option	-	deny
	Option / **Description** *accept* — Allows session that match the firewall policy. *deny* — Blocks sessions that match the firewall policy. *redirect* — Redirect sessions that match the firewall policy to a url. *isolate* — Isolate sessions that match the firewall policy with isolator.			
schedule	Schedule name.	string	Maximum length: 35	
service <name>	Service and service group names. Service and service group names.	string	Maximum length: 79	
explicit-web-proxy	Explicit web proxy.	string	Maximum length: 35	
transparent	set webproxy to use original client address.	option	-	disable
	Option / **Description** *enable* — Enable using original client address for webproxy. *disable* — Disable using original client address for webproxy.			

Parameter	Description	Type	Size	Default
access-proxy <name>	Access Proxy. Access Proxy name.	string	Maximum length: 79	
ztna-ems-tag <name>	Source ztna-ems-tag names. Address name.	string	Maximum length: 79	
ztna-tags-match-logic	ZTNA tag matching logic.	option	-	or
	Option / **Description** *or* — Match ZTNA tags using a logical OR operator. *and* — Match ZTNA tags using a logical AND operator.			
device-ownership	When enabled, the ownership enforcement will be done at policy level.	option	-	disable
	Option / **Description** *enable* — Enable device ownership. *disable* — Disable device ownership.			
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable
	Option / **Description** *enable* — Enable use of Internet Services in policy. *disable* — Disable use of Internet Services in policy.			
pass-through	Enable/disable policy matching pass through	option	-	disable
	Option / **Description** *enable* — Enable policy matching pass through. *disable* — Disable policy matching pass through.			
internet-service-name <name>	Internet Service name. Internet Service name.	string	Maximum length: 79	
internet-service-custom <name>	Custom Internet Service Name. Custom Internet Service name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
utm-status	Enable to add one or more security profiles (AV, IPS, etc.) to the firewall policy.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
webproxy-profile	Web proxy profile using when none matched policy.	string	Maximum length: 63	
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm
	Option / **Description** *all* — Log all sessions accepted or denied by this policy. *utm* — Log traffic that has a security profile applied to it. *disable* — Disable all logging for this policy.			
logtraffic-start	Record logs when a session starts and ends.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
log-http-transaction	Enable/disable http transaction log.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
wanopt	Enable/disable WAN optimization.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
wanopt-detection	WAN optimization auto-detection mode.	option	-	active

Parameter	Description	Type	Size	Default
	Option / **Description** *active* — Active WAN optimization peer auto-detection. *passive* — Passive WAN optimization peer auto-detection. *off* — Turn off WAN optimization peer auto-detection.			
wanopt-passive-opt	WAN optimization passive mode options. This option decides what IP address will be used to connect server.	option	-	default
	Option / **Description** *default* — Allow client side WAN opt peer to decide. *transparent* — Use address of client to connect to server. *non-transparent* — Use local FortiProxy address to connect to server.			
wanopt-profile	WAN optimization profile.	string	Maximum length: 35	
wanopt-peer	WAN optimization peer.	string	Maximum length: 35	
webcache	Enable/disable web cache.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
webcache-https	Enable/disable web cache for HTTPS.	option	-	disable
	Option / **Description** *disable* — Disable web cache for HTTPS. *enable* — Enable web cache for HTTPS.			
reverse-cache	Enable/disable reverse cache servers.	option	-	disable
	Option / **Description** *disable* — Disable reverse cache. *enable* — Enable reverse cache servers.			
http-tunnel-auth	Enable/disable HTTP tunnel authentication.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
ssh-policy-check	Enable/disable SSH policy check.	option	-	disable
	Option / **Description** *enable* — Enable SSH policy check. *disable* — Disable SSH policy check.			
webproxy-forward-server	Webproxy forward server name.	string	Maximum length: 63	
isolator-server	isolator server name.	string	Maximum length: 63	
poolname <name>	Name of IP pool object. IP pool name.	string	Maximum length: 79	
groups <name>	Names of user groups that can authenticate with this policy. Group name.	string	Maximum length: 79	
users <name>	Names of individual users that can authenticate with this policy. Names of individual users that can authenticate with this policy.	string	Maximum length: 79	
disclaimer	Web proxy disclaimer setting: by domain, policy, or user.	option	-	disable
	Option / **Description** *disable* — Disable disclaimer. *domain* — Display disclaimer for domain *policy* — Display disclaimer for policy *user* — Display disclaimer for current user			
comments	Comment.	var-string	Maximum length: 1023	
redirect-url	Redirect URL for further web proxy processing.	var-string	Maximum length: 1023	

Parameter	Description	Type	Size	Default
custom-log-fields <field-id>	Custom fields to append to log messages for this policy. Custom log field.	string	Maximum length: 35	
replacemsg-override-group	Override the default replacement message group for this policy.	string	Maximum length: 35	
srcaddr-negate	When enabled srcaddr specifies what the source address must NOT be.	option	-	disable
	Option / **Description** *enable* — Enable source address negate. *disable* — Disable source address negate.			
dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-	disable
	Option / **Description** *enable* — Enable destination address negate. *disable* — Disable destination address negate.			
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable
	Option / **Description** *enable* — Enable negated service match. *disable* — Disable negated service match.			
internet-service-negate	When enabled internet-service specifies what the service must NOT be.	option	-	disable
	Option / **Description** *enable* — Enable negated Internet Service match. *disable* — Disable negated Internet Service match.			
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35	
max-session-per-user	Max UTM sessions per user.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single
	Option / **Description** *single* — Do not allow security profile groups. *group* — Allow security profile groups.			
profile-group	Name of profile group.	string	Maximum length: 35	
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	no-inspection
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35	
ia-profile	Image analyzer profile.	string	Maximum length: 35	
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35	
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35	
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35	
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35	
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35	
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35	
application-list	Name of an existing Application list.	string	Maximum length: 35	
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35	
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35	
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
isolator-profile	Name of an existing isolator profile.	string	Maximum length: 35	
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35	

config firewall profile-group

Configure profile groups.

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

config firewall profile-group

Parameter	Description	Type	Size	Default
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	certificate-inspection
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35	
ia-profile	Image analyzer profile.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35	
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35	
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35	
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35	
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35	
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35	
application-list	Name of an existing Application list.	string	Maximum length: 35	
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35	
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35	
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 35	
isolator-profile	Name of an existing isolator profile.	string	Maximum length: 35	
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35	

config firewall profile-protocol-options

Configure protocol options.

```
config firewall profile-protocol-options
    Description: Configure protocol options.
    edit <name>
        set comment {var-string}
        set replacemsg-group {string}
        set oversize-log [disable|enable]
        set switching-protocols-log [disable|enable]
        config http
            Description: Configure HTTP protocol options.
            set ports {integer}
            set status [enable|disable]
            set options {option1}, {option2}, ...
```

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

```
        end
        config mapi
            Description: Configure MAPI protocol options.
            set ports {integer}
            set status [enable|disable]
            set options {option1}, {option2}, ...
            set oversize-limit {integer}
            set uncompressed-oversize-limit {integer}
            set uncompressed-nest-limit {integer}
            set scan-bzip2 [enable|disable]
        end
        config pop3
            Description: Configure POP3 protocol options.
            set ports {integer}
            set status [enable|disable]
            set options {option1}, {option2}, ...
            set oversize-limit {integer}
            set uncompressed-oversize-limit {integer}
            set uncompressed-nest-limit {integer}
            set scan-bzip2 [enable|disable]
            set ssl-offloaded [no|yes]
        end
        config smtp
            Description: Configure SMTP protocol options.
            set ports {integer}
            set status [enable|disable]
            set options {option1}, {option2}, ...
            set oversize-limit {integer}
            set uncompressed-oversize-limit {integer}
            set uncompressed-nest-limit {integer}
            set scan-bzip2 [enable|disable]
            set server-busy [enable|disable]
            set ssl-offloaded [no|yes]
        end
        config nntp
            Description: Configure NNTP protocol options.
            set ports {integer}
            set status [enable|disable]
            set options {option1}, {option2}, ...
            set oversize-limit {integer}
            set uncompressed-oversize-limit {integer}
            set uncompressed-nest-limit {integer}
            set scan-bzip2 [enable|disable]
        end
        config ssh
            Description: Configure SFTP and SCP protocol options.
            set options {option1}, {option2}, ...
            set comfort-interval {integer}
            set comfort-amount {integer}
            set oversize-limit {integer}
            set uncompressed-oversize-limit {integer}
            set uncompressed-nest-limit {integer}
            set stream-based-uncompressed-limit {integer}
            set scan-bzip2 [enable|disable]
            set tcp-window-type [auto-tuning|system|...]
            set tcp-window-minimum {integer}
```

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

config firewall profile-protocol-options

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
replacemsg-group	Name of the replacement message group to be used.	string	Maximum length: 35	
oversize-log	Enable/disable logging for antivirus oversize file blocking.	option	-	disable

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

config http

Parameter	Description	Type	Size	Default
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
options	One or more options that can be applied to the session.	option	-	
	Option / **Description** *clientcomfort* — Prevent client timeout. *servercomfort* — Prevent server timeout. *oversize* — Block oversized file.			

Parameter	Description	Type	Size	Default
	Option / **Description** *chunkedbypass* / Bypass chunked transfer encoded sites.			
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data .	integer	Minimum value: 1 Maximum value: 900	10
comfort-amount	Amount of data to send in a transmission for client comforting .	integer	Minimum value: 1 Maximum value: 65535	1
range-block	Enable/disable blocking of partial downloads.	option	-	disable
	Option / **Description** *disable* / Disable range header blocking (allow partial file downloads) *enable* / Enable range header blocking (treat all partial file downloads as full file download)			
strip-x-forwarded-for	Enable/disable stripping of HTTP X-Forwarded-For header.	option	-	disable
	Option / **Description** *disable* / Disable changing of HTTP X-Forwarded-For header. *enable* / Enable replacement of X-Forwarded-For value with 1.1.1.1.			
post-lang	ID codes for character sets to be used to convert to UTF-8 for banned words and DLP on HTTP posts (maximum of 5 character sets).	option	-	
	Option / **Description** *jisx0201* / Japanese Industrial Standard 0201. *jisx0208* / Japanese Industrial Standard 0208. *jisx0212* / Japanese Industrial Standard 0212. *gb2312* / Guojia Biaozhun 2312 (simplified Chinese). *ksc5601-ex* / Wansung Korean standard 5601. *euc-jp* / Extended Unicode Japanese. *sjis* / Shift Japanese Industrial Standard. *iso2022-jp* / ISO 2022 Japanese.			

Parameter	Description	Type	Size	Default
	Option / **Description** *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).			
streaming-content-bypass	Enable/disable bypassing of streaming content from buffering.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
dns-protection	Enable/disable DNS protection for HTTP/HTTPS traffic.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
switching-protocols	Bypass from scanning, or block a connection that attempts to switch protocol.	option	-	bypass
	Option / **Description** *bypass* — Bypass connections when switching protocols. *block* — Block connections when switching protocols.			

Parameter	Description	Type	Size	Default
unknown-http-version	How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.	option	-	reject
	Option / **Description** *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.			
tunnel-non-http	Configure how to process non-HTTP traffic when a profile configured for HTTP traffic accepts a non-HTTP session. Can occur if an application sends non-HTTP traffic using an HTTP destination port.	option	-	enable
	Option / **Description** *enable* — Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied. *disable* — Drop or tear down non-HTTP sessions accepted by the profile.			
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned in megabytes. Stream-based uncompression used only under certain conditions .	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
verify-dns-for-policy-matching	Enable/disable verify DNS for policy matching.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
block-page-status-code	Code number returned for blocked HTTP pages .	integer	Minimum value: 100 Maximum value: 599	403
retry-count	Number of attempts to retry HTTP connection .	integer	Minimum value: 0 Maximum value: 100	0
domain-fronting	Enable/disable HTTP domain fronting blocking.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning
	Option / **Description** *auto-tuning* — Allow system to auto-tune TCP window size (default). *system* — Use system default TCP window size for this protocol. *static* — Manually specify TCP window size. *dynamic* — Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			

Parameter	Description	Type	Size	Default
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no
	Option / **Description** *no* — SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled. *yes* — SSL decryption and encryption performed by an external device.			
address-ip-rating	Enable/disable IP based URL rating.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			

config ftp

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

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
options	One or more options that can be applied to the session.	option	-	
	Option / **Description** *clientcomfort* / Prevent client timeout. *oversize* / Block oversized file. *splice* / Enable splice mode. *bypass-rest-command* / Bypass REST command. *bypass-mode-command* / Bypass MODE command.			
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data .	integer	Minimum value: 1 Maximum value: 900	10
comfort-amount	Amount of data to send in a transmission for client comforting .	integer	Minimum value: 1 Maximum value: 65535	1
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12

Parameter	Description	Type	Size	Default
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned in megabytes. Stream-based uncompression used only under certain conditions .	integer	Minimum value: 0 Maximum value: 4294967295	0
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning
	Option / **Description** *auto-tuning* — Allow system to auto-tune TCP window size (default). *system* — Use system default TCP window size for this protocol. *static* — Manually specify TCP window size. *dynamic* — Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no

Parameter	Description	Type	Size	Default
	Option / **Description** *no* — SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled. *yes* — SSL decryption and encryption performed by an external device.			
explicit-ftp-tls	Enable/disable FTP redirection for explicit FTPS. **Option** / **Description** *enable* — Enable setting. *disable* — Disable setting.	option	-	disable

config imap

Parameter	Description	Type	Size	Default
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol. **Option** / **Description** *enable* — Enable setting. *disable* — Disable setting.	option	-	enable
options	One or more options that can be applied to the session. **Option** / **Description** *fragmail* — Pass fragmented email. *oversize* — Block oversized email.	option	-	
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10

Parameter	Description	Type	Size	Default
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no
	Option / **Description** *no* — SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled. *yes* — SSL decryption and encryption performed by an external device.			
address-ip-rating	Enable/disable IP based URL rating.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			

config mapi

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

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
options	One or more options that can be applied to the session.	option	-	
	Option / **Description** *fragmail* / Pass fragmented email. *oversize* / Block oversized email.			
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			

config pop3

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

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
options	One or more options that can be applied to the session.	option	-	
	Option / **Description** *fragmail* / Pass fragmented email. *oversize* / Block oversized email.			
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no
	Option / **Description** *no* / SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled. *yes* / SSL decryption and encryption performed by an external device.			

config smtp

Parameter	Description	Type	Size	Default
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
options	One or more options that can be applied to the session.	option	-	
	Option / **Description** *fragmail* — Pass fragmented email. *oversize* — Block oversized email. *splice* — Enable splice mode.			
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			

Parameter	Description	Type	Size	Default
server-busy	Enable/disable SMTP server busy when server not available.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no

Option	Description
no	SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.
yes	SSL decryption and encryption performed by an external device.

config nntp

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

Option	Description
enable	Enable setting.
disable	Disable setting.

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

Option	Description
oversize	Block oversized file.
splice	Enable splice mode.

Parameter	Description	Type	Size	Default
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10

Parameter	Description	Type	Size	Default
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

config ssh

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

Option	Description
oversize	Block oversized file.
clientcomfort	Prevent client timeout.
servercomfort	Prevent server timeout.

comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data .	integer	Minimum value: 1 Maximum value: 900	10
comfort-amount	Amount of data to send in a transmission for client comforting .	integer	Minimum value: 1 Maximum value: 65535	1
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10

Parameter	Description	Type	Size	Default
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned in megabytes. Stream-based uncompression used only under certain conditions .	integer	Minimum value: 0 Maximum value: 4294967295	0
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning
	Option / **Description** *auto-tuning* — Allow system to auto-tune TCP window size (default). *system* — Use system default TCP window size for this protocol. *static* — Manually specify TCP window size. *dynamic* — Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608

Parameter	Description	Type	Size	Default
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no

Option	Description
no	SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.
yes	SSL decryption and encryption performed by an external device.

config dns

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

Option	Description
enable	Enable setting.
disable	Disable setting.

config cifs

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

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
options	One or more options that can be applied to the session.	option	-	
	Option / **Description** *oversize* — Block oversized file.			
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 1 Maximum value: 204	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning
	Option / **Description** *auto-tuning* — Allow system to auto-tune TCP window size (default). *system* — Use system default TCP window size for this protocol. *static* — Manually specify TCP window size. *dynamic* — Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			

Parameter	Description	Type	Size	Default
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144
server-credential-type	CIFS server credential type.	option	-	none

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

domain-controller	Domain for which to decrypt CIFS traffic.	string	Maximum length: 63	

config server-keytab

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

config mail-signature

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

config firewall proxy-address

Configure web proxy address.

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

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

config firewall proxy-address

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
type	Proxy address type.	option	-	url

Option	Description
host-regex	Host regular expression.
url	HTTP URL.
category	FortiGuard URL catgegory.
url-list	HTTP URL list from external resource.
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.

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

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
post-arg	Enable/disable use of body in the HTTP POST to match the query.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
category <id>	FortiGuard category ID. FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 4294967295	
url-list	External URL list.	string	Maximum length: 35	
method	HTTP request methods to be used.	option	-	
	Option / **Description** *get* — GET method. *post* — POST method. *put* — PUT method. *head* — HEAD method. *connect* — CONNECT method. *trace* — TRACE method. *options* — OPTIONS method. *delete* — DELETE method.			
ua	Names of browsers to be used as user agent.	option	-	
	Option / **Description** *chrome* — Google Chrome. *ms* — Microsoft Internet Explorer or EDGE. *firefox* — Mozilla Firefox. *safari* — Apple Safari. *other* — Other browsers.			
header-name	Name of HTTP header.	string	Maximum length: 79	

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

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

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

config header-group

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

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

config tagging

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

config firewall proxy-addrgrp

Configure web proxy address group.

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

config firewall proxy-addrgrp

Parameter	Description	Type	Size	Default
type	Source or destination address group type. **Option** — **Description** *src* — Source group. *dst* — Destination group.	option	-	src
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
member <name>	Members of address group. Address name.	string	Maximum length: 79	
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0
comment	Optional comments.	var-string	Maximum length: 255	

config tagging

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

config firewall region

Define region table.

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

config firewall region

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

config firewall schedule group

Schedule group configuration.

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

```
    next
end
```

config firewall schedule group

Parameter	Description	Type	Size	Default
member <name>	Schedules added to the schedule group. Schedule name.	string	Maximum length: 79	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
fabric-object	Security Fabric global object setting.	option	-	disable

Option	Description
enable	Object is set as a security fabric-wide global object.
disable	Object is local to this security fabric member.

config firewall schedule onetime

Onetime schedule configuration.

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

config firewall schedule onetime

Parameter	Description	Type	Size	Default
start	Schedule start date and time, format hh:mm yyyy/mm/dd.	user	Not Specified	
end	Schedule end date and time, format hh:mm yyyy/mm/dd.	user	Not Specified	

Parameter	Description	Type	Size	Default
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
expiration-days	Write an event log message this many days before the schedule expires.	integer	Minimum value: 0 Maximum value: 100	3
fabric-object	Security Fabric global object setting.	option	-	disable

Option	Description
enable	Object is set as a security fabric-wide global object.
disable	Object is local to this security fabric member.

config firewall schedule recurring

Recurring schedule configuration.

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

config firewall schedule recurring

Parameter	Description	Type	Size	Default
start	Time of day to start the schedule, format hh:mm.	user	Not Specified	
end	Time of day to end the schedule, format hh:mm.	user	Not Specified	
day	One or more days of the week on which the schedule is valid. Separate the names of the days with a space.	option	-	none

Parameter	Description	Type	Size	Default
	Option / **Description** *sunday* / Sunday. *monday* / Monday. *tuesday* / Tuesday. *wednesday* / Wednesday. *thursday* / Thursday. *friday* / Friday. *saturday* / Saturday. *none* / None.			
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
fabric-object	Security Fabric global object setting.	option	-	disable
	Option / **Description** *enable* / Object is set as a security fabric-wide global object. *disable* / Object is local to this security fabric member.			

config firewall service category

Configure service categories.

```
config firewall service category
    Description: Configure service categories.
    edit <name>
        set comment {var-string}
        set fabric-object [enable|disable]
    next
end
```

config firewall service category

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

Parameter	Description	Type	Size	Default
fabric-object	Security Fabric global object setting.	option	-	disable

Option	Description
enable	Object is set as a security fabric-wide global object.
disable	Object is local to this security fabric member.

config firewall service custom

Configure custom services.

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

config firewall service custom

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

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
category	Service category.	string	Maximum length: 63	
protocol	Protocol type based on IANA numbers.	option	-	TCP/UDP/SCTP
	Option / **Description** *TCP/UDP/SCTP* / TCP, UDP and SCTP. *ICMP* / ICMP. *ICMP6* / ICMP6. *IP* / IP. *HTTP* / HTTP - for web proxy. *FTP* / FTP - for web proxy. *CONNECT* / Connect - for web proxy. *SOCKS-TCP* / Socks TCP - for web proxy. *SOCKS-UDP* / Socks UDP - for web proxy. *ALL* / All - for web proxy.			
iprange	Start and end of the IP range associated with service.	user	Not Specified	
fqdn	Fully qualified domain name.	string	Maximum length: 255	
protocol-number	IP protocol number.	integer	Minimum value: 0 Maximum value: 254	0
icmptype	ICMP type.	integer	Minimum value: 0 Maximum value: 4294967295	
icmpcode	ICMP code.	integer	Minimum value: 0 Maximum value: 255	

Parameter	Description	Type	Size	Default
tcp-portrange	Multiple TCP port ranges.	user	Not Specified	
udp-portrange	Multiple UDP port ranges.	user	Not Specified	
sctp-portrange	Multiple SCTP port ranges.	user	Not Specified	
tcp-halfclose-timer	Wait time to close a TCP session waiting for an unanswered FIN packet .	integer	Minimum value: 0 Maximum value: 86400	0
tcp-halfopen-timer	Wait time to close a TCP session waiting for an unanswered open session packet .	integer	Minimum value: 0 Maximum value: 86400	0
tcp-timewait-timer	Set the length of the TCP TIME-WAIT state in seconds .	integer	Minimum value: 0 Maximum value: 300	0
tcp-rst-timer	Set the length of the TCP CLOSE state in seconds .	integer	Minimum value: 5 Maximum value: 300	0
udp-idle-timer	UDP half close timeout .	integer	Minimum value: 0 Maximum value: 86400	0
session-ttl	Session TTL .	user	Not Specified	
check-reset-range	Configure the type of ICMP error message verification.	option	-	default

Option	Description
disable	Disable RST range check.
strict	Check RST range strictly.
default	Using system default setting.

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

Parameter	Description	Type	Size	Default
visibility	Enable/disable the visibility of the service on the GUI.	option	-	enable
	Option / **Description** *enable* — Show in service selection. *disable* — Hide from service selection.			
app-service-type	Application service type.	option	-	disable
	Option / **Description** *disable* — Disable application type. *app-id* — Application ID. *app-category* — Applicatin category.			
app-category <id>	Application category ID. Application category id.	integer	Minimum value: 0 Maximum value: 4294967295	
application <id>	Application ID. Application id.	integer	Minimum value: 0 Maximum value: 4294967295	
fabric-object	Security Fabric global object setting.	option	-	disable
	Option / **Description** *enable* — Object is set as a security fabric-wide global object. *disable* — Object is local to this security fabric member.			

config firewall service group

Configure service groups.

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

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

config firewall service group

Parameter	Description	Type	Size	Default
proxy	Enable/disable web proxy service group.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
member <name>	Service objects contained within the group. Address name.	string	Maximum length: 79	
comment	Comment.	var-string	Maximum length: 255	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
fabric-object	Security Fabric global object setting.	option	-	disable
	Option / **Description** *enable* — Object is set as a security fabric-wide global object. *disable* — Object is local to this security fabric member.			

config firewall shaping-policy

Configure shaping policies.

```
config firewall shaping-policy
    Description: Configure shaping policies.
    edit <id>
        set comment {var-string}
        set status [enable|disable]
        set ip-version [4|6]
        set service-type [service|internet-service]
        set srcaddr <name1>, <name2>, ...
        set dstaddr <name1>, <name2>, ...
        set srcaddr6 <name1>, <name2>, ...
        set dstaddr6 <name1>, <name2>, ...
        set service <name1>, <name2>, ...
```

```
        set internet-service-name <name1>, <name2>, ...
        set internet-service-group <name1>, <name2>, ...
        set internet-service-custom <name1>, <name2>, ...
        set internet-service-custom-group <name1>, <name2>, ...
        set users <name1>, <name2>, ...
        set groups <name1>, <name2>, ...
        set dstintf <name1>, <name2>, ...
        set class-id {integer}
        set class-id-reverse {integer}
        set diffserv-forward [enable|disable]
        set diffservcode-forward {user}
        set diffserv-reverse [enable|disable]
        set diffservcode-rev {user}
    next
end
```

config firewall shaping-policy

Parameter	Description	Type	Size	Default
comment	Comments.	var-string	Maximum length: 255	
status	Enable/disable traffic shaping policy.	option	-	enable
	Option / **Description** *enable* — Enable traffic shaping policy. *disable* — Disable traffic shaping policy.			
ip-version	IP version.	option	-	4
	Option / **Description** *4* — Use IPv4 addressing for Configuration Method. *6* — Use IPv6 addressing for Configuration Method.			
service-type	Select service-type: service / internet-service.	option	-	service
	Option / **Description** *service* — Firewall services. *internet-service* — Internet-services.			
srcaddr <name>	Source address. Address name.	string	Maximum length: 79	
dstaddr <name>	Destination address. Address name.	string	Maximum length: 79	
srcaddr6 <name>	IPv6 source address. Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
dstaddr6 <name>	IPv6 destination address. Address name.	string	Maximum length: 79	
service <name>	Service name. Service name.	string	Maximum length: 79	
internet-service-name <name>	Internet Service ID. Internet Service name.	string	Maximum length: 79	
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79	
internet-service-custom <name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79	
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79	
users <name>	User name. User name.	string	Maximum length: 79	
groups <name>	User authentication groups. Group name.	string	Maximum length: 79	
dstintf <name>	Destination interface list. Interface name.	string	Maximum length: 79	
class-id	Forward class id.	integer	Minimum value: 2 Maximum value: 31	0
class-id-reverse	Reverse class id.	integer	Minimum value: 2 Maximum value: 31	0
diffserv-forward	Enable/disable forward (original) traffic DiffServ.	option	-	enable disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
diffservcode-forward	Forward (original) traffic DiffServ code point value.	user	Not Specified	
diffserv-reverse	Enable/disable reverse (reply) traffic DiffServ.	option	-	enable disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
diffservcode-rev	Reverse (reply) traffic DiffServ code point value.	user	Not Specified	

config firewall shaping-profile

Configure shaping profiles.

```
config firewall shaping-profile
    Description: Configure shaping profiles.
    edit <profile-name>
        set comment {var-string}
        set default-class {integer}
        config classes
            Description: Define shaping classes of this shaping profile
            edit <name>
                set class-id {integer}
                set priority [top|critical|...]
                set guaranteed-bandwidth {integer}
                set maximum-bandwidth {integer}
            next
        end
    next
end
```

config firewall shaping-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 1023	
default-class	Default class ID to handle unclassified packets.	integer	Minimum value: 2 Maximum value: 32	2

config classes

Parameter	Description	Type	Size	Default
class-id	Class ID.	integer	Minimum value: 2 Maximum value: 32	0
priority	Priority.	option	-	top

Option	Description
top	Top priority.
critical	Critical priority.
high	High priority.
medium	Medium priority.
low	Low priority.

guaranteed-bandwidth	Guaranteed bandwidth in percentage.	integer	Minimum value: 0 Maximum value: 100	0
maximum-bandwidth	Maximum bandwidth in percentage.	integer	Minimum value: 1 Maximum value: 100	1

config firewall sniffer

Configure sniffer.

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

config firewall sniffer

Parameter	Description	Type	Size	Default
status	Enable/disable the active status of the sniffer.	option	-	enable
	Option / **Description** *enable* — Enable sniffer status. *disable* — Disable sniffer status.			
logtraffic	Either log all sessions, only sessions that have a security profile applied, or disable all logging for this policy.	option	-	utm
	Option / **Description** *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.			
non-ip	Enable/disable sniffing non-IP packets.	option	-	disable
	Option / **Description** *enable* — Enable sniffer for non-IP packets. *disable* — Disable sniffer for non-IP packets.			
interface	Interface name that traffic sniffing will take place on.	string	Maximum length: 35	
host	Hosts to filter for in sniffer traffic .	string	Maximum length: 63	
port	Ports to sniff .	string	Maximum length: 63	
protocol	Integer value for the protocol type as defined by IANA .	string	Maximum length: 63	
vlan	List of VLANs to sniff.	string	Maximum length: 63	
max-packet-count	Maximum packet count .	integer	Minimum value: 1 Maximum value: 1000000	4000

config firewall ssh host-key

SSH proxy host public keys.

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

config firewall ssh host-key

Parameter	Description	Type	Size	Default
status	Set the trust status of the public key.	option	-	trusted
	Option / **Description** *trusted* — The public key is trusted. *revoked* — The public key is revoked.			
type	Set the type of the public key.	option	-	RSA
	Option / **Description** *RSA* — The type of the public key is RSA. *DSA* — The type of the public key is DSA. *ECDSA* — The type of the public key is ECDSA. *ED25519* — The type of the public key is ED25519. *RSA-CA* — The type of the public key is from RSA CA. *DSA-CA* — The type of the public key is from DSA CA. *ECDSA-CA* — The type of the public key is from ECDSA CA. *ED25519-CA* — The type of the public key is from ED25519 CA.			
nid	Set the nid of the ECDSA key.	option	-	256

Parameter	Description	Type	Size	Default
	Option / **Description** *256* — The NID is ecdsa-sha2-nistp256. *384* — The NID is ecdsa-sha2-nistp384. *521* — The NID is ecdsa-sha2-nistp521.			
usage	Usage for this public key.	option	-	transparent-proxy
	Option / **Description** *transparent-proxy* — Transparent proxy uses this public key to validate server. *access-proxy* — Access proxy uses this public key to validate server.			
ip	IP address of the SSH server.	ipv4-address-any	Not Specified	0.0.0.0
port	Port of the SSH server.	integer	Minimum value: 0 Maximum value: 4294967295	22
hostname	Hostname of the SSH server to match SSH certificate principals.	string	Maximum length: 255	
public-key	SSH public key.	var-string	Maximum length: 32768	

config firewall ssh local-ca

SSH proxy local CA.

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

config firewall ssh local-ca

Parameter	Description	Type	Size	Default
password	Password for SSH private key.	password	Not Specified	
private-key	SSH proxy private key, encrypted with a password.	user	Not Specified	
public-key	SSH proxy public key.	user	Not Specified	
source	SSH proxy local CA source type.	option	-	user

Option	Description
built-in	Built-in SSH proxy local keys.
user	User imported SSH proxy local keys.

config firewall ssh local-key

SSH proxy local keys.

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

config firewall ssh local-key

Parameter	Description	Type	Size	Default
password	Password for SSH private key.	password	Not Specified	
private-key	SSH proxy private key, encrypted with a password.	user	Not Specified	
public-key	SSH proxy public key.	user	Not Specified	
source	SSH proxy local key source type.	option	-	user

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

config firewall ssh setting

SSH proxy settings.

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

config firewall ssh setting

Parameter	Description	Type	Size	Default
caname	CA certificate used by SSH Inspection.	string	Maximum length: 35	
untrusted-caname	Untrusted CA certificate used by SSH Inspection.	string	Maximum length: 35	
hostkey-rsa2048	RSA certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-dsa1024	DSA certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-ecdsa256	ECDSA nid256 certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-ecdsa384	ECDSA nid384 certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-ecdsa521	ECDSA nid384 certificate used by SSH proxy.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
hostkey-ed25519	ED25519 hostkey used by SSH proxy.	string	Maximum length: 35	
host-trusted-checking	Enable/disable host trusted checking.	option	-	enable

Option	Description
enable	Enable host key trusted checking.
disable	Disable host key trusted checking.

config firewall ssl-server

Configure SSL servers.

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

config firewall ssl-server

Parameter	Description	Type	Size	Default
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
port	Server service port .	integer	Minimum value: 1 Maximum value: 65535	443
ssl-mode	SSL/TLS mode for encryption and decryption of traffic.	option	-	full
	Option / **Description** *half* — Client to FortiProxy SSL. *full* — Client to FortiProxy and FortiProxy to Server SSL.			
add-header-x-forwarded-proto	Enable/disable adding an X-Forwarded-Proto header to forwarded requests.	option	-	enable
	Option / **Description** *enable* — Add X-Forwarded-Proto header. *disable* — Do not add X-Forwarded-Proto header.			
mapped-port	Mapped server service port .	integer	Minimum value: 1 Maximum value: 65535	80
ssl-cert	Name of certificate for SSL connections to this server .	string	Maximum length: 35	Fortinet_CA_SSL
ssl-dh-bits	Bit-size of Diffie-Hellman .	option	-	2048
	Option / **Description** *768* — 768-bit Diffie-Hellman prime. *1024* — 1024-bit Diffie-Hellman prime. *1536* — 1536-bit Diffie-Hellman prime. *2048* — 2048-bit Diffie-Hellman prime.			
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-	high
	Option / **Description** *high* — High encryption. Allow only AES and ChaCha			

Parameter	Description	Type	Size	Default
	Option / **Description** *medium* — Medium encryption. Allow AES, ChaCha, 3DES, and RC4. *low* — Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.			
ssl-client-renegotiation	Allow or block client renegotiation by server.	option	-	allow
	Option / **Description** *allow* — Allow a SSL client to renegotiate. *deny* — Abort any SSL connection that attempts to renegotiate. *secure* — Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.			
ssl-min-version	Lowest SSL/TLS version to negotiate.	option	-	tls-1.1
	Option / **Description** *tls-1.0* — TLS 1.0. *tls-1.1* — TLS 1.1. *tls-1.2* — TLS 1.2. *tls-1.3* — TLS 1.3.			
ssl-max-version	Highest SSL/TLS version to negotiate.	option	-	tls-1.3
	Option / **Description** *tls-1.0* — TLS 1.0. *tls-1.1* — TLS 1.1. *tls-1.2* — TLS 1.2. *tls-1.3* — TLS 1.3.			
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid attack on CBC IV.	option	-	enable
	Option / **Description** *enable* — Send empty fragments. *disable* — Do not send empty fragments.			
url-rewrite	Enable/disable rewriting the URL.	option	-	disable

Parameter	Description	Type	Size	Default

Option	Description
enable	Enable setting.
disable	Disable setting.

config firewall ssl-ssh-profile

Configure SSL/SSH protocol options.

```
config firewall ssl-ssh-profile
    Description: Configure SSL/SSH protocol options.
    edit <name>
        set comment {var-string}
        config ssl
            Description: Configure SSL options.
            set client-certificate [bypass|inspect|...]
            set unsupported-ssl-version [allow|block]
            set unsupported-ssl-cipher [allow|block]
            set unsupported-ssl-negotiation [allow|block]
            set expired-server-cert [allow|block|...]
            set revoked-server-cert [allow|block|...]
            set untrusted-server-cert [allow|block|...]
            set cert-validation-timeout [allow|block|...]
            set cert-validation-failure [allow|block|...]
            set sni-server-cert-check [enable|strict|...]
            set cert-probe-failure [allow|block]
            set min-allowed-ssl-version [ssl-3.0|tls-1.0|...]
        end
        config https
            Description: Configure HTTPS options.
            set ports {integer}
            set status [disable|certificate-inspection|...]
            set proxy-after-tcp-handshake [enable|disable]
            set client-certificate [bypass|inspect|...]
            set unsupported-ssl-version [allow|block]
            set unsupported-ssl-cipher [allow|block]
            set unsupported-ssl-negotiation [allow|block]
            set expired-server-cert [allow|block|...]
            set revoked-server-cert [allow|block|...]
            set untrusted-server-cert [allow|block|...]
            set cert-validation-timeout [allow|block|...]
            set cert-validation-failure [allow|block|...]
            set sni-server-cert-check [enable|strict|...]
            set cert-probe-failure [allow|block]
            set min-allowed-ssl-version [ssl-3.0|tls-1.0|...]
        end
        config ftps
            Description: Configure FTPS options.
            set ports {integer}
            set status [disable|deep-inspection]
```

```
        set client-certificate [bypass|inspect|...]
        set unsupported-ssl-version [allow|block]
        set unsupported-ssl-cipher [allow|block]
        set unsupported-ssl-negotiation [allow|block]
        set expired-server-cert [allow|block|...]
        set revoked-server-cert [allow|block|...]
        set untrusted-server-cert [allow|block|...]
        set cert-validation-timeout [allow|block|...]
        set cert-validation-failure [allow|block|...]
        set sni-server-cert-check [enable|strict|...]
        set min-allowed-ssl-version [ssl-3.0|tls-1.0|...]
    end
    config imaps
        Description: Configure IMAPS options.
        set ports {integer}
        set status [disable|deep-inspection]
        set proxy-after-tcp-handshake [enable|disable]
        set client-certificate [bypass|inspect|...]
        set unsupported-ssl-version [allow|block]
        set unsupported-ssl-cipher [allow|block]
        set unsupported-ssl-negotiation [allow|block]
        set expired-server-cert [allow|block|...]
        set revoked-server-cert [allow|block|...]
        set untrusted-server-cert [allow|block|...]
        set cert-validation-timeout [allow|block|...]
        set cert-validation-failure [allow|block|...]
        set sni-server-cert-check [enable|strict|...]
    end
    config pop3s
        Description: Configure POP3S options.
        set ports {integer}
        set status [disable|deep-inspection]
        set proxy-after-tcp-handshake [enable|disable]
        set client-certificate [bypass|inspect|...]
        set unsupported-ssl-version [allow|block]
        set unsupported-ssl-cipher [allow|block]
        set unsupported-ssl-negotiation [allow|block]
        set expired-server-cert [allow|block|...]
        set revoked-server-cert [allow|block|...]
        set untrusted-server-cert [allow|block|...]
        set cert-validation-timeout [allow|block|...]
        set cert-validation-failure [allow|block|...]
        set sni-server-cert-check [enable|strict|...]
    end
    config smtps
        Description: Configure SMTPS options.
        set ports {integer}
        set status [disable|deep-inspection]
        set proxy-after-tcp-handshake [enable|disable]
        set client-certificate [bypass|inspect|...]
        set unsupported-ssl-version [allow|block]
        set unsupported-ssl-cipher [allow|block]
        set unsupported-ssl-negotiation [allow|block]
        set expired-server-cert [allow|block|...]
        set revoked-server-cert [allow|block|...]
        set untrusted-server-cert [allow|block|...]
```

```
        set cert-validation-timeout [allow|block|...]
        set cert-validation-failure [allow|block|...]
        set sni-server-cert-check [enable|strict|...]
    end
    config ssh
        Description: Configure SSH options.
        set ports {integer}
        set status [disable|deep-inspection]
        set proxy-after-tcp-handshake [enable|disable]
        set unsupported-version [bypass|block]
        set ssh-tun-policy-check [disable|enable]
        set ssh-algorithm [compatible|high-encryption]
    end
    config dot
        Description: Configure DNS over TLS options.
        set status [disable|deep-inspection]
        set proxy-after-tcp-handshake [enable|disable]
        set client-certificate [bypass|inspect|...]
        set unsupported-ssl-version [allow|block]
        set unsupported-ssl-cipher [allow|block]
        set unsupported-ssl-negotiation [allow|block]
        set expired-server-cert [allow|block|...]
        set revoked-server-cert [allow|block|...]
        set untrusted-server-cert [allow|block|...]
        set cert-validation-timeout [allow|block|...]
        set cert-validation-failure [allow|block|...]
        set sni-server-cert-check [enable|strict|...]
    end
    config ssl-client-certificate
        Description: Configure SSL client certificate setting.
        set status [do-not-offer|keyring-list|...]
        set keyring-list {string}
        set caname {string}
    end
    config ssl-exempt
        Description: Servers to exempt from SSL inspection.
        edit <id>
            set type [fortiguard-category|address|...]
            set fortiguard-category {integer}
            set address {string}
            set address6 {string}
            set wildcard-fqdn {string}
            set regex {string}
            set finger-print-category [unknown|firefox|...]
        next
    end
    set allowlist [enable|disable]
    set block-blocklisted-certificates [disable|enable]
    set server-cert-mode [re-sign|replace]
    set use-ssl-server [disable|enable]
    set caname {string}
    set untrusted-caname {string}
    set server-cert <name1>, <name2>, ...
    config ssl-server
        Description: SSL server settings used for client certificate request.
        edit <id>
```

```
                set ip {ipv4-address-any}
                set https-client-certificate [bypass|inspect|...]
                set smtps-client-certificate [bypass|inspect|...]
                set pop3s-client-certificate [bypass|inspect|...]
                set imaps-client-certificate [bypass|inspect|...]
                set ftps-client-certificate [bypass|inspect|...]
                set ssl-other-client-certificate [bypass|inspect|...]
            next
        end
        set ssl-exemption-ip-rating [enable|disable]
        set ssl-exemption-log [disable|enable]
        set ssl-anomaly-log [disable|enable]
        set ssl-negotiation-log [disable|enable]
        set ssl-server-cert-log [disable|enable]
        set ssl-handshake-log [disable|enable]
        set rpc-over-https [enable|disable]
        set mapi-over-https [enable|disable]
        set supported-alpn [http1-1|http2|...]
    next
end
```

config firewall ssl-ssh-profile

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

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
block-blocklisted-certificates	Enable/disable blocking SSL-based botnet communication by FortiGuard certificate blocklist.	option	-	enable

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

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

Option	Description
re-sign	Multiple clients connecting to multiple servers.

Parameter	Description	Type	Size	Default
	Option / **Description** *replace* / Protect an SSL server.			
use-ssl-server	Enable/disable the use of SSL server table for SSL offloading.	option	-	disable
	Option / **Description** *disable* / Don't use SSL server configuration. *enable* / Use SSL server configuration.			
caname	CA certificate used by SSL Inspection.	string	Maximum length: 35	default-ca
untrusted-caname	Untrusted CA certificate used by SSL Inspection.	string	Maximum length: 35	default-untrusted-ca
server-cert <name>	Certificate used by SSL Inspection to replace server certificate. Certificate list.	string	Maximum length: 35	
ssl-exemption-ip-rating	Enable/disable IP based URL rating.	option	-	enable
	Option / **Description** *enable* / Enable IP based URL rating. *disable* / Disable IP based URL rating.			
ssl-exemption-log	Enable/disable logging SSL exemptions.	option	-	disable
	Option / **Description** *disable* / Disable logging SSL exemptions. *enable* / Enable logging SSL exemptions.			
ssl-anomaly-log	Enable/disable logging of SSL anomalies.	option	-	enable
	Option / **Description** *disable* / Disable logging of SSL anomalies. *enable* / Enable logging of SSL anomalies.			

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

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

Parameter	Description	Type	Size	Default
ssl-server-cert-log	Enable/disable logging of server certificate information.	option	-	disable

Option	Description
disable	Disable logging server certificate.
enable	Enable logging server certificate.

Parameter	Description	Type	Size	Default
ssl-handshake-log	Enable/disable logging of TLS handshakes.	option	-	disable

Option	Description
disable	Disable logging TLS handshakes.
enable	Enable logging TLS handshakes.

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

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

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

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

Parameter	Description	Type	Size	Default
supported-alpn	Configure ALPN option.	option	-	all

Option	Description
http1-1	Enable all ALPN including HTTP1.1 except HTTP2 and SPDY.

Parameter	Description	Type	Size	Default
	Option / **Description** *http2* — Enable all ALPN including HTTP2 except HTTP1.1 and SPDY. *all* — Allow all ALPN extensions except SPDY. *none* — Do not use ALPN.			

config ssl

Parameter	Description	Type	Size	Default
client-certificate	Action based on received client certificate. **Option** / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.	option	-	bypass
unsupported-ssl-version	Action based on the SSL version used being unsupported. **Option** / **Description** *allow* — Bypass the session when the version is not supported. *block* — Block the session when the version is not supported.	option	-	block
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported. **Option** / **Description** *allow* — Bypass the session when the cipher is not supported. *block* — Block the session when the cipher is not supported.	option	-	allow
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported. **Option** / **Description** *allow* — Bypass the session when the negotiation is not supported. *block* — Block the session when the negotiation is not supported.	option	-	allow
expired-server-cert	Action based on server certificate is expired.	option	-	block

Parameter	Description	Type	Size	Default
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
revoked-server-cert	Action based on server certificate is revoked.	option	-	block
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
cert-validation-failure	Action based on certificate validation failure.	option	-	block
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering. *strict* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection. *disable* — Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
cert-probe-failure	Action based on certificate probe failure.	option	-	block
	Option / **Description** *allow* — Bypass the session when unable to retrieve server's certificate for inspection. *block* — Block the session when unable to retrieve server's certificate for inspection.			
min-allowed-ssl-version	Minimum SSL version to be allowed.	option	-	tls-1.1
	Option / **Description** *ssl-3.0* — SSL 3.0. *tls-1.0* — TLS 1.0. *tls-1.1* — TLS 1.1. *tls-1.2* — TLS 1.2. *tls-1.3* — TLS 1.3.			

config https

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

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Disable. *certificate-inspection* — Inspect SSL handshake only. *deep-inspection* — Full SSL inspection.			
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before). **Option** / **Description** *enable* — Enable setting. *disable* — Disable setting.	option	-	disable
client-certificate	Action based on received client certificate. **Option** / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.	option	-	bypass
unsupported-ssl-version	Action based on the SSL version used being unsupported. **Option** / **Description** *allow* — Bypass the session when the version is not supported. *block* — Block the session when the version is not supported.	option	-	block
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported. **Option** / **Description** *allow* — Bypass the session when the cipher is not supported. *block* — Block the session when the cipher is not supported.	option	-	allow
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported. **Option** / **Description** *allow* — Bypass the session when the negotiation is not supported. *block* — Block the session when the negotiation is not supported.	option	-	allow

Parameter	Description	Type	Size	Default
expired-server-cert	Action based on server certificate is expired.	option	-	block

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

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

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
cert-validation-failure	Action based on certificate validation failure.	option	-	block

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

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

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

Parameter	Description	Type	Size	Default
cert-probe-failure	Action based on certificate probe failure.	option	-	block

Option	Description
allow	Bypass the session when unable to retrieve server's certificate for inspection.
block	Block the session when unable to retrieve server's certificate for inspection.

Parameter	Description	Type	Size	Default
min-allowed-ssl-version	Minimum SSL version to be allowed.	option	-	tls-1.1

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

config ftps

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

Parameter	Description	Type	Size	Default
status	Configure protocol inspection status.	option	-	deep-inspection

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

Parameter	Description	Type	Size	Default
client-certificate	Action based on received client certificate.	option	-	bypass

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

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

Option	Description
allow	Bypass the session when the version is not supported.
block	Block the session when the version is not supported.

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

Option	Description
allow	Bypass the session when the cipher is not supported.
block	Block the session when the cipher is not supported.

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

Option	Description
allow	Bypass the session when the negotiation is not supported.
block	Block the session when the negotiation is not supported.

Parameter	Description	Type	Size	Default
expired-server-cert	Action based on server certificate is expired.	option	-	block

Option	Description
allow	Allow the server certificate.

Parameter	Description	Type	Size	Default
	Option / **Description** *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
revoked-server-cert	Action based on server certificate is revoked.	option	-	block
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
cert-validation-failure	Action based on certificate validation failure.	option	-	block
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering. *strict* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection. *disable* — Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
min-allowed-ssl-version	Minimum SSL version to be allowed. **Option** / **Description** *ssl-3.0* — SSL 3.0. *tls-1.0* — TLS 1.0. *tls-1.1* — TLS 1.1. *tls-1.2* — TLS 1.2. *tls-1.3* — TLS 1.3.	option	-	tls-1.1

config imaps

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535	
status	Configure protocol inspection status. **Option** / **Description** *disable* — Disable. *deep-inspection* — Full SSL inspection.	option	-	deep-inspection
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
client-certificate	Action based on received client certificate.	option	-	inspect
	Option / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.			
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block
	Option / **Description** *allow* — Bypass the session when the version is not supported. *block* — Block the session when the version is not supported.			
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	Option / **Description** *allow* — Bypass the session when the cipher is not supported. *block* — Block the session when the cipher is not supported.			
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow
	Option / **Description** *allow* — Bypass the session when the negotiation is not supported. *block* — Block the session when the negotiation is not supported.			
expired-server-cert	Action based on server certificate is expired.	option	-	block
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			

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

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
cert-validation-failure	Action based on certificate validation failure.	option	-	block

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

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

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

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

config pop3s

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535	
status	Configure protocol inspection status.	option	-	deep-inspection
	Option **Description** *disable* Disable. *deep-inspection* Full SSL inspection.			
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
client-certificate	Action based on received client certificate.	option	-	inspect
	Option **Description** *bypass* Bypass the session. *inspect* Inspect the session. *block* Block the session.			
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block

Parameter	Description	Type	Size	Default
	Option / **Description** *allow* — Bypass the session when the version is not supported. *block* — Block the session when the version is not supported.			
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	Option / **Description** *allow* — Bypass the session when the cipher is not supported. *block* — Block the session when the cipher is not supported.			
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow
	Option / **Description** *allow* — Bypass the session when the negotiation is not supported. *block* — Block the session when the negotiation is not supported.			
expired-server-cert	Action based on server certificate is expired.	option	-	block
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
revoked-server-cert	Action based on server certificate is revoked.	option	-	block
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	Option / **Description** *allow* — Allow the server certificate.			

Parameter	Description	Type	Size	Default
	Option / **Description** *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
cert-validation-failure	Action based on certificate validation failure.	option	-	block
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable
	Option / **Description** *enable* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering. *strict* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection. *disable* — Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			

config smtps

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535	
status	Configure protocol inspection status.	option	-	deep-inspection
	Option / **Description** *disable* — Disable. *deep-inspection* — Full SSL inspection.			
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
client-certificate	Action based on received client certificate.	option	-	inspect
	Option / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.			
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block
	Option / **Description** *allow* — Bypass the session when the version is not supported. *block* — Block the session when the version is not supported.			
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	Option / **Description** *allow* — Bypass the session when the cipher is not supported. *block* — Block the session when the cipher is not supported.			

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

Option	Description
allow	Bypass the session when the negotiation is not supported.
block	Block the session when the negotiation is not supported.

Parameter	Description	Type	Size	Default
expired-server-cert	Action based on server certificate is expired.	option	-	block

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

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

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
cert-validation-failure	Action based on certificate validation failure.	option	-	block

Parameter	Description	Type	Size	Default
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable
	Option / **Description** *enable* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering. *strict* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection. *disable* — Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			

config ssh

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535	
status	Configure protocol inspection status.	option	-	disable
	Option / **Description** *disable* — Disable. *deep-inspection* — Full SSL inspection.			
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			

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

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

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

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

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

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

config dot

Parameter	Description	Type	Size	Default
status	Configure protocol inspection status.	option	-	disable

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

Parameter	Description	Type	Size	Default
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
client-certificate	Action based on received client certificate.	option	-	bypass

Parameter	Description	Type	Size	Default
	Option / **Description** *bypass* / Bypass the session. *inspect* / Inspect the session. *block* / Block the session.			
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block
	Option / **Description** *allow* / Bypass the session when the version is not supported. *block* / Block the session when the version is not supported.			
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	Option / **Description** *allow* / Bypass the session when the cipher is not supported. *block* / Block the session when the cipher is not supported.			
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow
	Option / **Description** *allow* / Bypass the session when the negotiation is not supported. *block* / Block the session when the negotiation is not supported.			
expired-server-cert	Action based on server certificate is expired.	option	-	block
	Option / **Description** *allow* / Allow the server certificate. *block* / Block the session. *ignore* / Re-sign the server certificate as trusted.			
revoked-server-cert	Action based on server certificate is revoked.	option	-	block
	Option / **Description** *allow* / Allow the server certificate.			

Parameter	Description	Type	Size	Default
	Option / **Description** *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
cert-validation-failure	Action based on certificate validation failure.	option	-	block
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable
	Option / **Description** *enable* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering. *strict* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection. *disable* — Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			

config ssl-client-certificate

Parameter	Description	Type	Size	Default
status	Configure SSL client certificate status.	option	-	do-not-offer

Option	Description
do-not-offer	Do not offer SSL client certificate.
keyring-list	For authenticated users, offer matching SSL client certificate from keyring list.
ca-sign	For authenticated users, offer SSL client certificate signed by configured CA.

keyring-list	Keyring list used to find client certificate.	string	Maximum length: 35	
caname	CA certificate used to sign client certificate.	string	Maximum length: 35	Fortinet_CA_SSL

config ssl-exempt

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

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

fortiguard-category	FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 255	0
address	IPv4 address object.	string	Maximum length: 79	
address6	IPv6 address object.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
wildcard-fqdn	Exempt servers by wildcard FQDN.	string	Maximum length: 79	
regex	Exempt servers by regular expression.	string	Maximum length: 255	
finger-print-category	Finger print platform.	option	-	android

Option	Description
unknown	Unknown clients.
firefox	Firefox.
chrome	Chrome.
safari	Safari.
edge	Edge.
ie	Internet Explorer.
android	Android applications.
ios	iOS applications.
windows	Windows applications.

config ssl-server

Parameter	Description	Type	Size	Default
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified	0.0.0.0
https-client-certificate	Action based on received client certificate during the HTTPS handshake.	option	-	bypass

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

smtps-client-certificate	Action based on received client certificate during the SMTPS handshake.	option	-	bypass

Parameter	Description	Type	Size	Default
	Option / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.			
pop3s-client-certificate	Action based on received client certificate during the POP3S handshake.	option	-	bypass
	Option / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.			
imaps-client-certificate	Action based on received client certificate during the IMAPS handshake.	option	-	bypass
	Option / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.			
ftps-client-certificate	Action based on received client certificate during the FTPS handshake.	option	-	bypass
	Option / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.			
ssl-other-client-certificate	Action based on received client certificate during an SSL protocol handshake.	option	-	bypass
	Option / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.			

config firewall ssl default-certificate

SSL default certificate.

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

config firewall ssl default-certificate

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

config firewall ssl keyring-list

SSL keyring list.

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

config firewall ssl keyring-list

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

config firewall ssl setting

SSL proxy settings.

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

config firewall ssl setting

Parameter	Description	Type	Size	Default
proxy-connect-timeout	Time limit to make an internal connection to the appropriate proxy process .	integer	Minimum value: 1 Maximum value: 60	30
ssl-dh-bits	Bit-size of Diffie-Hellman .	option	-	2048

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

Parameter	Description	Type	Size	Default
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid attack on CBC IV (for SSL 3.0 and TLS 1.0 only).	option	-	enable

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

Parameter	Description	Type	Size	Default
no-matching-cipher-action	Bypass or drop the connection when no matching cipher is found.	option	-	bypass

Option	Description
bypass	Bypass connection.

Parameter	Description	Type	Size	Default
	Option / **Description** *drop* / Drop connection.			
cert-cache-capacity	Maximum capacity of the host certificate cache .	integer	Minimum value: 0 Maximum value: 500	200
cert-cache-timeout	Time limit to keep certificate cache .	integer	Minimum value: 1 Maximum value: 120	10
session-cache-capacity	Capacity of the SSL session cache .	integer	Minimum value: 0 Maximum value: 1000	500
session-cache-timeout	Time limit to keep SSL session state .	integer	Minimum value: 1 Maximum value: 60	20
abbreviate-handshake	Enable/disable use of SSL abbreviated handshake.	option	-	enable
	Option / **Description** *enable* / Enable use of SSL abbreviated handshake. *disable* / Disable use of SSL abbreviated handshake.			

config firewall traffic-class

Configure names for shaping classes.

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

config firewall traffic-class

Parameter	Description	Type	Size	Default
class-name	Define the name for this class-id.	string	Maximum length: 35	

config firewall ttl-policy

Configure TTL policies.

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

config firewall ttl-policy

Parameter	Description	Type	Size	Default
status	Enable/disable this TTL policy.	option	-	enable
	Option / **Description** *enable* — Enable this TTL policy. *disable* — Disable this TTL policy.			
action	Action to be performed on traffic matching this policy .	option	-	deny
	Option / **Description** *accept* — Allow traffic matching this policy. *deny* — Deny or block traffic matching this policy.			
srcintf	Source interface name from available interfaces.	string	Maximum length: 35	
srcaddr <name>	Source address object(s) from available options. Separate multiple names with a space. Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
service <name>	Service object(s) from available options. Separate multiple names with a space. Service name.	string	Maximum length: 79	
schedule	Schedule object from available options.	string	Maximum length: 35	
ttl	Value/range to match against the packet's Time to Live value .	user	Not Specified	

config firewall vendor-mac-summary

Vendor MAC database summary.

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

config firewall vendor-mac

Show vendor and the MAC address they have.

```
config firewall vendor-mac
    Description: Show vendor and the MAC address they have.
    edit <id>
        set name {string}
        set mac-number {integer}
        set obsolete {integer}
    next
end
```

config firewall vendor-mac

Parameter	Description	Type	Size	Default
name	Vendor name.	string	Maximum length: 63	
mac-number	Total number of MAC addresses.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
obsolete	Indicates whether the Vendor ID can be used.	integer	Minimum value: 0 Maximum value: 255	0

config firewall vip

Configure virtual IP for IPv4.

```
config firewall vip
    Description: Configure virtual IP for IPv4.
    edit <name>
        set id {integer}
        set uuid {uuid}
        set comment {var-string}
        set type [static-nat|access-proxy]
        set extip {user}
        set mappedip <range1>, <range2>, ...
        set extintf {string}
        set arp-reply [disable|enable]
        set server-type [http|https|...]
        set http-redirect [enable|disable]
        set portforward [disable|enable]
        set status [disable|enable]
        set protocol [tcp|udp|...]
        set extport {user}
        set mappedport {user}
        set gratuitous-arp-interval {integer}
        set ssl-certificate {string}
        set ssl-dh-bits [768|1024|...]
        set ssl-algorithm [high|medium|...]
        set ssl-pfs [require|deny|...]
        set ssl-min-version [ssl-3.0|tls-1.0|...]
        set ssl-max-version [ssl-3.0|tls-1.0|...]
        set color {integer}
    next
end
```

config firewall vip

Parameter	Description	Type	Size	Default
id	Custom defined ID.	integer	Minimum value: 0 Maximum value: 65535	0

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
comment	Comment.	var-string	Maximum length: 255	
type	Configure between a static NAT and access proxy VIP.	option	-	static-nat
	Option / **Description** *static-nat* — Static NAT. *access-proxy* — Access proxy.			
extip	IP address or address range on the external interface that you want to map to an address or address range on the destination network.	user	Not Specified	
mappedip `<range>`	IP address or address range on the destination network to which the external IP address is mapped. Mapped IP range.	string	Maximum length: 79	
extintf	Interface connected to the source network that receives the packets that will be forwarded to the destination network.	string	Maximum length: 35	
arp-reply	Enable to respond to ARP requests for this virtual IP address. Enabled by default.	option	-	enable
	Option / **Description** *disable* — Disable ARP reply. *enable* — Enable ARP reply.			
server-type	Protocol to be load balanced by the virtual server (also called the server load balance virtual IP).	option	-	
	Option / **Description** *http* — HTTP. *https* — HTTPS. *imaps* — IMAPS. *pop3s* — POP3S. *smtps* — SMTPS.			

Parameter	Description	Type	Size	Default
	Option / **Description** *ssl* — SSL. *tcp* — TCP. *udp* — UDP. *ip* — IP.			
http-redirect	Enable/disable redirection of HTTP to HTTPS.	option	-	disable
	Option / **Description** *enable* — Enable redirection of HTTP to HTTPS. *disable* — Disable redirection of HTTP to HTTPS.			
portforward	Enable/disable port forwarding.	option	-	disable
	Option / **Description** *disable* — Disable port forward. *enable* — Enable port forward.			
status	Enable/disable VIP.	option	-	enable
	Option / **Description** *disable* — Disable the VIP. *enable* — Enable the VIP.			
protocol	Protocol to use when forwarding packets.	option	-	tcp
	Option / **Description** *tcp* — TCP. *udp* — UDP. *sctp* — SCTP. *icmp* — ICMP.			
extport	Incoming port number range that you want to map to a port number range on the destination network.	user	Not Specified	
mappedport	Port number range on the destination network to which the external port number range is mapped.	user	Not Specified	

Parameter	Description	Type	Size	Default
gratuitous-arp-interval	Enable to have the VIP send gratuitous ARPs. 0=disabled. Set from 5 up to 8640000 seconds to enable.	integer	Minimum value: 5 Maximum value: 8640000	0
ssl-certificate	The name of the certificate to use for SSL handshake.	string	Maximum length: 35	
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048

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

ssl-algorithm	Permitted encryption algorithms for SSL sessions according to encryption strength.	option	-	low

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

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

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

ssl-min-version	Lowest SSL/TLS version acceptable from a client.	option	-	ssl-3.0

Parameter	Description	Type	Size	Default
	Option / **Description** *ssl-3.0* — SSL 3.0. *tls-1.0* — TLS 1.0. *tls-1.1* — TLS 1.1. *tls-1.2* — TLS 1.2.			
ssl-max-version	Highest SSL/TLS version acceptable from a client.	option	-	tls-1.2
	Option / **Description** *ssl-3.0* — SSL 3.0. *tls-1.0* — TLS 1.0. *tls-1.1* — TLS 1.1. *tls-1.2* — TLS 1.2.			
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0

config firewall vipgrp

Configure IPv4 virtual IP groups.

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

config firewall vipgrp

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
interface	Interface.	string	Maximum length: 35	
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0
comments	Comment.	var-string	Maximum length: 255	
member <name>	Member VIP objects of the group (Separate multiple objects with a space). VIP name.	string	Maximum length: 79	

config firewall wildcard-fqdn custom

Config global/VDOM Wildcard FQDN address.

```
config firewall wildcard-fqdn custom
    Description: Config global/VDOM Wildcard FQDN address.
    edit <name>
        set uuid {uuid}
        set wildcard-fqdn {string}
        set color {integer}
        set comment {var-string}
    next
end
```

config firewall wildcard-fqdn custom

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
wildcard-fqdn	Wildcard FQDN.	string	Maximum length: 255	

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

config firewall wildcard-fqdn group

Config global Wildcard FQDN address groups.

```
config firewall wildcard-fqdn group
    Description: Config global Wildcard FQDN address groups.
    edit <name>
        set uuid {uuid}
        set member <name1>, <name2>, ...
        set color {integer}
        set comment {var-string}
    next
end
```

config firewall wildcard-fqdn group

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
member <name>	Address group members. Address name.	string	Maximum length: 79	
color	GUI icon color.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	

ftp-proxy

This section includes syntax for the following commands:

config ftp-proxy explicit

Configure explicit FTP proxy settings.

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

config ftp-proxy explicit

Parameter	Description	Type	Size	Default
status	Enable/disable the explicit FTP proxy.	option	-	disable
	Option / **Description** *enable* — Enable the explicit FTP proxy. *disable* — Disable the explicit FTP proxy.			
incoming-port	Accept incoming FTP requests on one or more ports.	user	Not Specified	
incoming-ip	Accept incoming FTP requests from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	0.0.0.0
outgoing-ip	Outgoing FTP requests will leave from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	

Parameter	Description	Type	Size	Default
sec-default-action	Accept or deny explicit FTP proxy sessions when no FTP proxy firewall policy exists.	option	-	deny
	Option / **Description** *accept* — Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not *deny* — Deny requests unless there is a matching explicit FTP proxy policy.			
server-data-mode	Determine mode of data session on FTP server side.	option	-	client
	Option / **Description** *client* — Use the same transmission mode for client and server data sessions. *passive* — Use passive mode on server data session.			
ssl	Enable/disable the explicit FTPS proxy.	option	-	disable
	Option / **Description** *enable* — Enable the explicit FTPS proxy. *disable* — Disable the explicit FTPS proxy.			
ssl-cert	Name of certificate for SSL connections to this server .	string	Maximum length: 35	Fortinet_CA_SSL
ssl-dh-bits	Bit-size of Diffie-Hellman .	option	-	2048
	Option / **Description** *768* — 768-bit Diffie-Hellman prime. *1024* — 1024-bit Diffie-Hellman prime. *1536* — 1536-bit Diffie-Hellman prime. *2048* — 2048-bit Diffie-Hellman prime.			
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-	high
	Option / **Description** *high* — High encryption. Allow only AES and ChaCha *medium* — Medium encryption. Allow AES, ChaCha, 3DES, and RC4. *low* — Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.			

hardware

This section includes syntax for the following commands:

config hardware cpu

Display detailed information for all installed CPU(s).

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

config hardware memory

Display system memory information.

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

config hardware nic

Display NIC information.

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

config hardware nic

Parameter	Description	Type	Size	Default
<nic>	NIC name.	string	Maximum length: -1	

config hardware status

Hardware status.

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

icap

This section includes syntax for the following commands:

config icap local-server

Configure ICAP local server.

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

config icap local-server

Parameter	Description	Type	Size	Default
status	Enable/disable status for icap server network profile.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Disable the status for ipv4 in network-profile. *enable* — Enable the status for ipv4 in network-profile.			
secure-connection	Enable/disable status for secured icap server network profile.	option	-	disable
	Option / **Description** *disable* — Disable the status for ipv4 ssl in network-profile. *enable* — Enable the status for ipv4 ssl in network-profile.			
status-ipv6	Enable/disable status for icap server service ipv6.	option	-	disable
	Option / **Description** *disable* — Disable the status for ipv6 in network-profile. *enable* — Enable the status for ipv6 in network-profile.			
icap-incoming-port	Accept incoming ICAP requests on one or more ports .	integer	Minimum value: 1 Maximum value: 65535	1344
icap-incoming-ssl-port	Accept incoming secured ICAP requests on one or more ports .	integer	Minimum value: 1 Maximum value: 65535	11344
interface	Interface name	string	Maximum length: 15	
incoming-ip	Restrict the ICAP server to only accept sessions from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	0.0.0.0
incoming-ipv6	Restrict the ICAP server to only accept sessions from this IPv6 address. An interface must have this IPv6 address.	ipv6-address	Not Specified	::
ssl-cert	SSL certificate for SSL interception.	string	Maximum length: 35	Fortinet_SSL
strict-scheme-check	Enable/disable strict check of scheme.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* / Disable strict check of scheme. *enable* / Enable strict check of scheme.			
srcaddr	Source address name.	string	Maximum length: 79	

config icap-service

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

config icap profile

Configure ICAP profiles.

```
config icap profile
    Description: Configure ICAP profiles.
    edit <name>
```

```
        set replacemsg-group {string}
        set request [disable|enable]
        set response [disable|enable]
        set file-transfer {option1}, {option2}, ...
        set streaming-content-bypass [disable|enable]
        set 204-size-limit {integer}
        set allow-204-response [disable|enable]
        set preview [disable|enable]
        set preview-data-length {integer}
        set request-server {string}
        set response-server {string}
        set file-transfer-server {string}
        set request-failure [error|bypass]
        set response-failure [error|bypass]
        set file-transfer-failure [error|bypass]
        set request-path {string}
        set response-path {string}
        set file-transfer-path {string}
        set methods {option1}, {option2}, ...
        set response-req-hdr [disable|enable]
        set respmod-default-action [forward|bypass]
        set icap-block-log [disable|enable]
        set chunk-encap [disable|enable]
        set extension-feature {option1}, {option2}, ...
        set scan-progress-interval {integer}
        set timeout {integer}
        config icap-headers
            Description: Configure ICAP forwarded request headers.
            edit <id>
                set name {string}
                set content {string}
                set base64-encoding [disable|enable]
            next
        end
        config respmod-forward-rules
            Description: ICAP response mode forward rules.
            edit <name>
                set host {string}
                config header-group
                    Description: HTTP header group.
                    edit <id>
                        set header-name {string}
                        set header {string}
                        set case-sensitivity [disable|enable]
                    next
                end
                set action [forward|bypass]
                set http-resp-status-code <code1>, <code2>, ...
            next
        end
    next
end
```

config icap profile

Parameter	Description	Type	Size	Default
replacemsg-group	Replacement message group.	string	Maximum length: 35	
request	Enable/disable whether an HTTP request is passed to an ICAP server.	option	-	disable
	Option / **Description** *disable* — Disable HTTP request passing to ICAP server. *enable* — Enable HTTP request passing to ICAP server.			
response	Enable/disable whether an HTTP response is passed to an ICAP server.	option	-	disable
	Option / **Description** *disable* — Disable HTTP response passing to ICAP server. *enable* — Enable HTTP response passing to ICAP server.			
file-transfer	Configure the file transfer protocols to pass transferred files to an ICAP server as REQMOD.	option	-	
	Option / **Description** *ssh* — Forward file transfer with SSH protocol to ICAP server for further processing. *ftp* — Forward file transfer with FTP protocol to ICAP server for further processing.			
streaming-content-bypass	Enable/disable bypassing of ICAP server for streaming content.	option	-	disable
	Option / **Description** *disable* — Disable bypassing of ICAP server for streaming content. *enable* — Enable bypassing of ICAP server for streaming content.			
204-size-limit	Allow 204 size limit to be saved by ICAP client.	integer	Minimum value: 1 Maximum value: 10	1
allow-204-response	Enable/disable allowing of 204 response from ICAP server.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Disable allowing of 204 response from ICAP server. *enable* — Enable allowing of 204 response from ICAP server.			
preview	Enable/disable preview of data to ICAP server.	option	-	disable
	Option / **Description** *disable* — Disable preview of data to ICAP server. *enable* — Enable preview of data to ICAP server.			
preview-data-length	Preview data length to be sent to ICAP server.	integer	Minimum value: 0 Maximum value: 4096	0
request-server	ICAP server to use for an HTTP request.	string	Maximum length: 63	
response-server	ICAP server to use for an HTTP response.	string	Maximum length: 63	
file-transfer-server	ICAP server to use for a file transfer.	string	Maximum length: 63	
request-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP request.	option	-	error
	Option / **Description** *error* — Error. *bypass* — Bypass.			
response-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP response.	option	-	error
	Option / **Description** *error* — Error. *bypass* — Bypass.			
file-transfer-failure	Action to take if the ICAP server cannot be contacted when processing a file transfer.	option	-	error
	Option / **Description** *error* — Error. *bypass* — Bypass.			

Parameter	Description	Type	Size	Default
request-path	Path component of the ICAP URI that identifies the HTTP request processing service.	string	Maximum length: 127	
response-path	Path component of the ICAP URI that identifies the HTTP response processing service.	string	Maximum length: 127	
file-transfer-path	Path component of the ICAP URI that identifies the file transfer processing service.	string	Maximum length: 127	
methods	The allowed HTTP methods that will be sent to ICAP server for further processing.	option	-	delete get head options post put trace connect other

Option	Description
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.
connect	Forward HTTP request or response with CONNECT method to ICAP server for further processing.
other	Forward HTTP request or response with All other methods to ICAP server for further processing.

Parameter	Description	Type	Size	Default
response-req-hdr	Enable/disable addition of req-hdr for ICAP response modification (respmod) processing.	option	-	enable

Option	Description
disable	Do not add req-hdr for response modification (respmod) processing.

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Add req-hdr for response modification (respmod) processing.			
respmod-default-action	Default action to ICAP response modification (respmod) processing.	option	-	forward
	Option / **Description** *forward* — Forward response to ICAP server unless a rule specifies not to. *bypass* — Don't forward request to ICAP server unless a rule specifies to forward the request.			
icap-block-log	Enable/disable UTM log when infection found .	option	-	disable
	Option / **Description** *disable* — Disable UTM log when infection found. *enable* — Enable UTM log when infection found.			
chunk-encap	Enable/disable chunked encapsulation .	option	-	disable
	Option / **Description** *disable* — Do not encapsulate chunked data. *enable* — Encapsulate chunked data into a new chunk.			
extension-feature	Enable/disable ICAP extension features.	option	-	
	Option / **Description** *scan-progress* — Support X-Scan-Progress-Interval ICAP header.			
scan-progress-interval	Scan progress interval value.	integer	Minimum value: 5 Maximum value: 30	10
timeout	Time (in seconds) that ICAP client waits for the response from ICAP server.	integer	Minimum value: 30 Maximum value: 3600	30

config icap-headers

Parameter	Description	Type	Size	Default
name	HTTP forwarded header name.	string	Maximum length: 79	
content	HTTP header content.	string	Maximum length: 255	
base64-encoding	Enable/disable use of base64 encoding of HTTP content.	option	-	disable

Option	Description
disable	Disable use of base64 encoding of HTTP content.
enable	Enable use of base64 encoding of HTTP content.

config respmod-forward-rules

Parameter	Description	Type	Size	Default
host	Address object for the host.	string	Maximum length: 79	
action	Action to be taken for ICAP server.	option	-	forward

Option	Description
forward	Forward request to ICAP server when this rule is matched.
bypass	Don't forward request to ICAP server when this rule is matched.

http-resp-status-code <code>	HTTP response status code. HTTP response status code.	integer	Minimum value: 100 Maximum value: 599	4203762324

config header-group

Parameter	Description	Type	Size	Default
header-name	HTTP header.	string	Maximum length: 79	
header	HTTP header regular expression.	string	Maximum length: 255	
case-sensitivity	Enable/disable case sensitivity when matching header.	option	-	disable

Parameter	Description	Type	Size	Default

Option	Description
disable	Ignore case when matching header.
enable	Do not ignore case when matching header.

config icap remote-server-group

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

```
config icap remote-server-group
    Description: Configure an ICAP remote server group consisting of multiple forward
servers. Supports failover and load balancing.
    edit <name>
        set ldb-method [weighted|least-session|...]
        config server-list
            Description: Add ICAP remote servers to a list to form a server group.
Optionally assign weights to each server.
            edit <name>
                set weight {integer}
            next
        end
    next
end
```

config icap remote-server-group

Parameter	Description	Type	Size	Default
ldb-method	Load balance method.	option	-	weighted

Option	Description
weighted	Load balance traffic to forward servers based on assigned weights.
least-session	Send new sessions to the server with lowest session count.
active-passive	Send new sessions to active server with high weight.

config server-list

Parameter	Description	Type	Size	Default
weight	Optionally assign a weight of the ICAP remote server for weighted load balancing	integer	Minimum value: 1 Maximum value: 100	10

config icap remote-server

Configure ICAP servers.

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

config icap remote-server

Parameter	Description	Type	Size	Default
addr-type	Address type of the remote ICAP server: IPv4, IPv6 or FQDN.	option	-	ip4
	Option / **Description** *ip4* — Use an IPv4 address for the remote ICAP server. *ip6* — Use an IPv6 address for the remote ICAP server. *fqdn* — Use the FQDN for the remote ICAP server.			
ip-address	IPv4 address of the ICAP server.	ipv4-address-any	Not Specified	0.0.0.0
ip6-address	IPv6 address of the ICAP server.	ipv6-address	Not Specified	::
fqdn	ICAP remote server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255	
port	ICAP server port.	integer	Minimum value: 1 Maximum value: 65535	1344

Parameter	Description	Type	Size	Default
max-connections	Maximum number of concurrent connections to ICAP server . Must not be less than wad-worker-count.	integer	Minimum value: 0 Maximum value: 4294967295	100
secure	Enable/disable secure connection to ICAP server.	option	-	disable
	Option / **Description** *disable* — Disable connection to secure ICAP server. *enable* — Enable connection to secure ICAP server.			
ssl-cert	CA certificate name.	string	Maximum length: 79	
healthcheck	Enable/disable ICAP remote server health checking. Attempts to connect to the remote ICAP server to verify that the server is operating normally.	option	-	disable
	Option / **Description** *disable* — Disable health checking. *enable* — Enable health checking.			
healthcheck-service	ICAP Service name to use for health checks.	string	Maximum length: 127	

image-analyzer

This section includes syntax for the following commands:

config image-analyzer profile

Configure image analyzer profiles

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

config image-analyzer profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
alcohol-block-strictness-level	Higher value means an image is more likely to be blocked.	integer	Minimum value: 0 Maximum value: 100	30
alcohol-status	Allow/deny/monitor the category image.	option	-	deny

Option	Description
allow	Allow the category image.
deny	Deny the category image.
monitor	Monitor the category image.

Parameter	Description	Type	Size	Default
drugs-block-strictness-level	Higher value means an image is more likely to be blocked.	integer	Minimum value: 0 Maximum value: 100	30
drugs-status	Allow/deny/monitor the category image.	option	-	deny

Option	Description
allow	Allow the category image.
deny	Deny the category image.
monitor	Monitor the category image.

Parameter	Description	Type	Size	Default
extremism-block-strictness-level	Higher value means an image is more likely to be blocked.	integer	Minimum value: 0 Maximum value: 100	30
extremism-status	Allow/deny/monitor the category image.	option	-	deny

Option	Description
allow	Allow the category image.
deny	Deny the category image.
monitor	Monitor the category image.

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

Parameter	Description	Type	Size	Default
swim_ underwear-status	Allow/deny/monitor the category image.	option	-	deny

Option	Description
allow	Allow the category image.
deny	Deny the category image.
monitor	Monitor the category image.

Parameter	Description	Type	Size	Default
weapons-block-strictness-level	Higher value means an image is more likely to be blocked.	integer	Minimum value: 0 Maximum value: 100	30
weapons-status	Allow/deny/monitor the category image.	option	-	deny

Option	Description
allow	Allow the category image.
deny	Deny the category image.
monitor	Monitor the category image.

Parameter	Description	Type	Size	Default
image-skip-size	Image skip rating size.	integer	Minimum value: 0 Maximum value: 2048	1
image-skip-width	Image skip rating width(min. 5 pixel).	integer	Minimum value: 5 Maximum value: 2147483647	30
image-skip-height	Image skip rating height(min. 5 pixel).	integer	Minimum value: 5 Maximum value: 2147483647	30
log-option	Log option for the inspected image result.	option	-	violation

Option	Description
all	Log all image result.
violation	Log only violation image result.

Parameter	Description	Type	Size	Default
source-url	Enable/disable source url in the image search result.	option	-	enable
	Option / **Description** *enable* — Enable source url in image search. *disable* — Disable source url in image search.			
blocked-img-cache	Enable/disable saving blocked images in ram disk.	option	-	disable
	Option / **Description** *enable* — Enable caching. *disable* — Disable caching.			
rating-err-action	Actions when image rating error.	option	-	pass
	Option / **Description** *block* — Block. *pass* — Pass.			
replace-image	Specify replacement image.	string	Maximum length: 35	

ips

This section includes syntax for the following commands:

config ips custom

Configure IPS custom signature.

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

config ips custom

Parameter	Description	Type	Size	Default
signature	Custom signature enclosed in single quotes.	var-string	Maximum length: 4095	

Parameter	Description	Type	Size	Default
rule-id	Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified	
location	Protect client or server traffic.	user	Not Specified	
os	Operating system(s) that the signature protects. Blank for all operating systems.	user	Not Specified	
application	Applications to be protected. Blank for all applications.	user	Not Specified	
protocol	Protocol(s) that the signature scans. Blank for all protocols.	user	Not Specified	
status	Enable/disable this signature.	option	-	enable
	Option / **Description** *disable* — Disable status. *enable* — Enable status.			
log	Enable/disable logging.	option	-	enable
	Option / **Description** *disable* — Disable logging. *enable* — Enable logging.			
log-packet	Enable/disable packet logging.	option	-	disable
	Option / **Description** *disable* — Disable packet logging. *enable* — Enable packet logging.			
action	Default action (pass or block) for this signature.	option	-	pass
	Option / **Description** *pass* — Pass or allow matching traffic. *block* — Block or drop matching traffic.			
comment	Comment.	string	Maximum length: 63	

config ips decoder

Configure IPS decoder.

```
config ips decoder
    Description: Configure IPS decoder.
    edit <name>
        config parameter
            Description: IPS group parameters.
            edit <name>
                set value {string}
            next
        end
    next
end
```

config parameter

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

config ips global

Configure IPS global parameter.

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

config ips global

Parameter	Description	Type	Size	Default
fail-open	Enable to allow traffic if the IPS buffer is full. Default is disable and IPS traffic is blocked when the IPS buffer is full.	option	-	disable

Option	Description
enable	Enable IPS fail open.
disable	Disable IPS fail open.

Parameter	Description	Type	Size	Default
database	Regular or extended IPS database. Regular protects against the latest common and in-the-wild attacks. Extended includes protection from legacy attacks.	option	-	extended

Option	Description
regular	IPS regular database package.
extended	IPS extended database package.

Parameter	Description	Type	Size	Default
traffic-submit	Enable/disable submitting attack data found by this FortiProxy to FortiGuard.	option	-	disable

Option	Description
enable	Enable traffic submit.
disable	Disable traffic submit.

Parameter	Description	Type	Size	Default
anomaly-mode	Global blocking mode for rate-based anomalies.	option	-	continuous

Option	Description
periodical	After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.
continuous	Block packets once an anomaly is detected. Overrides individual anomaly settings.

Parameter	Description	Type	Size	Default
session-limit-mode	Method of counting concurrent sessions used by session limit anomalies. Choose between greater accuracy (accurate) or improved performance (heuristics).	option	-	heuristic

Option	Description
accurate	Accurately count concurrent sessions, demands more resources.

Parameter	Description	Type	Size	Default
	Option / **Description** *heuristic* — Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.			
socket-size	IPS socket buffer size. Max and default value depend on available memory. Can be changed to tune performance.	integer	Minimum value: 0 Maximum value: 128	64
engine-count	Number of IPS engines running. If set to the default value of 0, FortiProxy sets the number to optimize performance depending on the number of CPU cores.	integer	Minimum value: 0 Maximum value: 255	0
sync-session-ttl	Enable/disable use of kernel session TTL for IPS sessions.	option	-	enable
	Option / **Description** *enable* — Enable use of kernel session TTL for IPS sessions. *disable* — Disable use of kernel session TTL for IPS sessions.			
deep-app-insp-timeout	Timeout for Deep application inspection .	integer	Minimum value: 0 Maximum value: 2147483647	0
deep-app-insp-db-limit	Limit on number of entries in deep application inspection database .	integer	Minimum value: 0 Maximum value: 2147483647	0
exclude-signatures	Excluded signatures.	option	-	industrial
	Option / **Description** *none* — No signatures excluded. *industrial* — Exclude industrial signatures.			
packet-log-queue-depth	Packet/pcap log queue depth per IPS engine.	integer	Minimum value: 128 Maximum value: 4096	128

config tls-active-probe

Parameter	Description	Type	Size	Default
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
vdom	Virtual domain name for TLS active probe.	string	Maximum length: 31	
source-ip	Source IP address used for TLS active probe.	ipv4-address	Not Specified	0.0.0.0
source-ip6	Source IPv6 address used for TLS active probe.	ipv6-address	Not Specified	::

config ips rule-settings

Configure IPS rule setting.

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

config ips rule

Configure IPS rules.

```
config ips rule
    Description: Configure IPS rules.
    edit <name>
        set status [disable|enable]
        set log [disable|enable]
        set log-packet [disable|enable]
        set action [pass|block]
        set group {string}
        set severity {user}
```

```
        set location {user}
        set os {user}
        set application {user}
        set service {user}
        set rule-id {integer}
        set rev {integer}
        set date {integer}
        config metadata
            Description: Meta data.
            edit <id>
                set metaid {integer}
                set valueid {integer}
            next
        end
    next
end
```

config ips rule

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

Option	Description
disable	Disable status.
enable	Enable status.

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

Option	Description
disable	Disable logging.
enable	Enable logging.

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

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

Parameter	Description	Type	Size	Default
action	Action.	option	-	pass

Option	Description
pass	Pass or allow matching traffic.
block	Block or drop matching traffic.

Parameter	Description	Type	Size	Default
group	Group.	string	Maximum length: 63	
severity	Severity.	user	Not Specified	
location	Vulnerable location.	user	Not Specified	
os	Vulnerable operation systems.	user	Not Specified	
application	Vulnerable applications.	user	Not Specified	
service	Vulnerable service.	user	Not Specified	
rule-id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
rev	Revision.	integer	Minimum value: 0 Maximum value: 4294967295	0
date	Date.	integer	Minimum value: 0 Maximum value: 4294967295	0

config metadata

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

config ips sensor

Configure IPS sensor.

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

config ips sensor

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
block-malicious-url	Enable/disable malicious URL blocking.	option	-	disable

Option	Description
disable	Disable malicious URL blocking.
enable	Enable malicious URL blocking.

Parameter	Description	Type	Size	Default
scan-botnet-connections	Block or monitor connections to Botnet servers, or disable Botnet scanning.	option	-	disable

Option	Description
disable	Do not scan connections to botnet servers.
block	Block connections to botnet servers.
monitor	Log connections to botnet servers.

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

Option	Description
enable	Enable setting.
disable	Disable setting.

config entries

Parameter	Description	Type	Size	Default
rule <id>	Identifies the predefined or custom IPS signatures to add to the sensor. Rule IPS.	integer	Minimum value: 0 Maximum value: 4294967295	
location	Protect client or server traffic.	user	Not Specified	all
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified	all

Parameter	Description	Type	Size	Default
protocol	Protocols to be examined. Use all for every protocol and other for unlisted protocols.	user	Not Specified	all
os	Operating systems to be protected. Use all for every operating system and other for unlisted operating systems.	user	Not Specified	all
application	Operating systems to be protected. Use all for every application and other for unlisted application.	user	Not Specified	all
cve <cve-entry>	List of CVE IDs of the signatures to add to the sensor. CVE IDs or CVE wildcards.	string	Maximum length: 19	
status	Status of the signatures included in filter. Only those filters with a status to enable are used.	option	-	default
	Option / **Description** *disable* — Disable status of selected rules. *enable* — Enable status of selected rules. *default* — Default.			
log	Enable/disable logging of signatures included in filter.	option	-	enable
	Option / **Description** *disable* — Disable logging of selected rules. *enable* — Enable logging of selected rules.			
log-packet	Enable/disable packet logging. Enable to save the packet that triggers the filter. You can download the packets in pcap format for diagnostic use.	option	-	disable
	Option / **Description** *disable* — Disable packet logging of selected rules. *enable* — Enable packet logging of selected rules.			
log-attack-context	Enable/disable logging of attack context: URL buffer, header buffer, body buffer, packet buffer.	option	-	disable
	Option / **Description** *disable* — Disable logging of detailed attack context. *enable* — Enable logging of detailed attack context.			

Parameter	Description	Type	Size	Default
action	Action taken with traffic in which signatures are detected.	option	-	default

Option	Description
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.

Parameter	Description	Type	Size	Default
rate-count	Count of the rate.	integer	Minimum value: 0 Maximum value: 65535	0
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535	60
rate-mode	Rate limit mode.	option	-	continuous

Option	Description
periodical	Allow configured number of packets every rate-duration.
continuous	Block packets once the rate is reached.

Parameter	Description	Type	Size	Default
rate-track	Track the packet protocol field.	option	-	none

Option	Description
none	none
src-ip	Source IP.
dest-ip	Destination IP.
dhcp-client-mac	DHCP client.
dns-domain	DNS domain.

Parameter	Description	Type	Size	Default
quarantine	Quarantine method.	option	-	none

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

Parameter	Description	Type	Size	Default
quarantine-expiry	Duration of quarantine. . Requires quarantine set to attacker.	user	Not Specified	5m
quarantine-log	Enable/disable quarantine logging.	option	-	enable

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

config exempt-ip

Parameter	Description	Type	Size	Default
src-ip	Source IP address and netmask (applies to packet matching the signature).	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
dst-ip	Destination IP address and netmask (applies to packet matching the signature).	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config ips session

Session status.

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

config ips settings

Configure IPS VDOM parameter.

```
config ips settings
    Description: Configure IPS VDOM parameter.
    set packet-log-history {integer}
    set packet-log-post-attack {integer}
    set packet-log-memory {integer}
    set ips-packet-quota {integer}
end
```

config ips settings

Parameter	Description	Type	Size	Default
packet-log-history	Number of packets to capture before and including the one in which the IPS signature is detected .	integer	Minimum value: 1 Maximum value: 255	1
packet-log-post-attack	Number of packets to log after the IPS signature is detected .	integer	Minimum value: 0 Maximum value: 255	0
packet-log-memory	Maximum memory can be used by packet log .	integer	Minimum value: 64 Maximum value: 8192	256
ips-packet-quota	Maximum amount of disk space in MB for logged packets when logging to disk. Range depends on disk size.	integer	Minimum value: 0 Maximum value: 4294967295	0

config ips view-map

Configure IPS view-map.

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

config ips view-map

Parameter	Description	Type	Size	Default
vdom-id	VDOM ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
policy-id	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
id-policy-id	ID-based policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
which	Policy.	option	-	firewall

Option	Description
firewall	Firewall policy.

ipsec

This section includes syntax for the following commands:

config ipsec tunnel

IPsec tunnel.

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

isolator

This section includes syntax for the following commands:

config isolator profile

Configure isolator profiles.

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

config isolator profile

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

config entries

Parameter	Description	Type	Size	Default
proxy-address	Choose the proxy-address for this isolator profile entry.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
action	Choose the action for this isolator entry.	option	-	isolate

Option	Description
isolate	Open the website in an isolator instead of the client.
freeze	Freeze the website. The user is able to unfreeze and get access to the website when they accept the risk.
block	Block the traffic to the website.
allow	Bypass the traffic to the website.

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

Option	Description
enable	Enable this entry.
disable	Disable this entry.

Parameter	Description	Type	Size	Default
right-click	Enable/disable right-click.	option	-	enable

Option	Description
enable	Enable right-click.
disable	Disable right-click.

Parameter	Description	Type	Size	Default
copy-paste	Enable/disable copy-paste.	option	-	enable

Option	Description
enable	Enable copy-paste.
disable	Disable copy-paste.

log

This section includes syntax for the following commands:

config log custom-field

Configure custom log fields.

```
config log custom-field
    Description: Configure custom log fields.
    edit <id>
        set name {string}
        set value {string}
    next
end
```

config log custom-field

Parameter	Description	Type	Size	Default
name	Field name (max: 15 characters).	string	Maximum length: 15	
value	Field value (max: 15 characters).	string	Maximum length: 15	

config log disk filter

Configure filters for local disk logging. Use these filters to determine the log messages to record according to severity and type.

```
config log disk filter
    Description: Configure filters for local disk logging. Use these filters to determine
the log messages to record according to severity and type.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set dlp-archive [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log disk filter

Parameter	Description	Type	Size	Default
severity	Log to disk every message above and including this severity level.	option	-	information

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

forward-traffic	Enable/disable forward traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable forward traffic logging. *disable* Disable forward traffic logging.			
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option **Description** *enable* Enable local in or out traffic logging. *disable* Disable local in or out traffic logging.			
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
anomaly	Enable/disable anomaly logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable anomaly logging. *disable* — Disable anomaly logging.			
voip	Enable/disable VoIP logging.	option	-	enable
	Option / **Description** *enable* — Enable VoIP logging. *disable* — Disable VoIP logging.			
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	Option / **Description** *enable* — Enable DLP archive logging. *disable* — Disable DLP archive logging.			

config free-style

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

Parameter	Description	Type	Size	Default
	Option / **Description** *ssh* — SSH log. *ssl* — SSL log. *file-filter* — File filter log. *icap* — ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter. **Option** / **Description** *include* — Include logs that match the filter. *exclude* — Exclude logs that match the filter.	option	-	include

config log disk setting

Settings for local disk logging.

```
config log disk setting
    Description: Settings for local disk logging.
    set status [enable|disable]
    set ips-archive [enable|disable]
    set max-log-file-size {integer}
    set max-policy-packet-capture-size {integer}
    set roll-schedule [daily|weekly]
    set roll-day {option1}, {option2}, ...
    set roll-time {user}
    set diskfull [overwrite|nolog]
    set log-quota {integer}
    set dlp-archive-quota {integer}
    set report-quota {integer}
    set maximum-log-age {integer}
    set upload [enable|disable]
    set upload-destination {option}
    set uploadip {ipv4-address}
    set uploadport {integer}
    set source-ip {ipv4-address}
    set uploaduser {string}
    set uploadpass {password}
    set uploaddir {string}
    set uploadtype {option1}, {option2}, ...
    set uploadsched [disable|enable]
    set uploadtime {user}
    set upload-delete-files [enable|disable]
    set upload-ssl-conn [default|high|...]
```

```
    set full-first-warning-threshold {integer}
    set full-second-warning-threshold {integer}
    set full-final-warning-threshold {integer}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log disk setting

Parameter	Description	Type	Size	Default
status	Enable/disable local disk logging.	option	-	enable
	Option **Description** *enable* Log to local disk. *disable* Do not log to local disk.			
ips-archive	Enable/disable IPS packet archiving to the local disk.	option	-	enable
	Option **Description** *enable* Enable IPS packet archiving. *disable* Disable IPS packet archiving.			
max-log-file-size	Maximum log file size before rolling .	integer	Minimum value: 1 Maximum value: 100	20
max-policy-packet-capture-size	Maximum size of policy sniffer in MB (0 means unlimited).	integer	Minimum value: 0 Maximum value: 4294967295	100
roll-schedule	Frequency to check log file for rolling.	option	-	daily
	Option **Description** *daily* Check the log file once a day. *weekly* Check the log file once a week.			
roll-day	Day of week on which to roll log file.	option	-	sunday
	Option **Description** *sunday* Sunday			

Parameter	Description	Type	Size	Default
	Option / **Description** *monday* / Monday *tuesday* / Tuesday *wednesday* / Wednesday *thursday* / Thursday *friday* / Friday *saturday* / Saturday			
roll-time	Time of day to roll the log file (hh:mm).	user	Not Specified	
diskfull	Action to take when disk is full. The system can overwrite the oldest log messages or stop logging when the disk is full .	option	-	overwrite
	Option / **Description** *overwrite* / Overwrite the oldest logs when the log disk is full. *nolog* / Stop logging when the log disk is full.			
log-quota	Disk log quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0
dlp-archive-quota	DLP archive quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0
report-quota	Report db quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0
maximum-log-age	Delete log files older than (days).	integer	Minimum value: 0 Maximum value: 3650	7
upload	Enable/disable uploading log files when they are rolled.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable uploading log files when they are rolled. *disable* / Disable uploading log files when they are rolled.			
upload-destination	The type of server to upload log files to. Only FTP is currently supported. **Option** / **Description** *ftp-server* / Upload rolled log files to an FTP server.	option	-	ftp-server
uploadip	IP address of the FTP server to upload log files to.	ipv4-address	Not Specified	0.0.0.0
uploadport	TCP port to use for communicating with the FTP server .	integer	Minimum value: 0 Maximum value: 65535	21
source-ip	Source IP address to use for uploading disk log files.	ipv4-address	Not Specified	0.0.0.0
uploaduser	Username required to log into the FTP server to upload disk log files.	string	Maximum length: 35	
uploadpass	Password required to log into the FTP server to upload disk log files.	password	Not Specified	
uploaddir	The remote directory on the FTP server to upload log files to.	string	Maximum length: 63	
uploadtype	Types of log files to upload. Separate multiple entries with a space. **Option** / **Description** *traffic* / Upload traffic log. *event* / Upload event log. *virus* / Upload anti-virus log.	option	-	traffic event virus webfilter IPS emailfilter dlp-archive anomaly voip dlp app-ctrl waf dns ssh ssl

Parameter	Description	Type	Size	Default
	Option / **Description** *webfilter* — Upload web filter log. *IPS* — Upload IPS log. *emailfilter* — Upload spam filter log. *dlp-archive* — Upload DLP archive. *anomaly* — Upload anomaly log. *voip* — Upload VoIP log. *dlp* — Upload DLP log. *app-ctrl* — Upload application control log. *waf* — Upload web application firewall log. *dns* — Upload DNS log. *ssh* — Upload SSH log. *ssl* — Upload SSL log. *file-filter* — Upload file-filter log. *icap* — Upload ICAP log.			
uploadsched	Set the schedule for uploading log files to the FTP server . **Option** / **Description** *disable* — Upload when rolling. *enable* — Scheduled upload.	option	-	disable
uploadtime	Time of day at which log files are uploaded if uploadsched is enabled (hh:mm or hh).	user	Not Specified	
upload-delete-files	Delete log files after uploading . **Option** / **Description** *enable* — Delete log files after uploading. *disable* — Do not delete log files after uploading.	option	-	enable
upload-ssl-conn	Enable/disable encrypted FTPS communication to upload log files.	option	-	default

Parameter	Description	Type	Size	Default
	Option / **Description** *default* — FTPS with high and medium encryption algorithms. *high* — FTPS with high encryption algorithms. *low* — FTPS with low encryption algorithms. *disable* — Disable FTPS communication.			
full-first-warning-threshold	Log full first warning threshold as a percent .	integer	Minimum value: 1 Maximum value: 98	75
full-second-warning-threshold	Log full second warning threshold as a percent .	integer	Minimum value: 2 Maximum value: 99	90
full-final-warning-threshold	Log full final warning threshold as a percent .	integer	Minimum value: 3 Maximum value: 100	95
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log eventfilter

Configure log event filters.

```
config log eventfilter
    Description: Configure log event filters.
    set event [enable|disable]
    set system [enable|disable]
    set vpn [enable|disable]
    set user [enable|disable]
    set router [enable|disable]
    set wireless-activity [enable|disable]
```

```
    set wan-opt [enable|disable]
    set endpoint [enable|disable]
    set ha [enable|disable]
    set security-rating [enable|disable]
    set fortiextender [enable|disable]
    set connector [enable|disable]
    set sdwan [enable|disable]
    set cifs [enable|disable]
    set switch-controller [enable|disable]
    set wcs [enable|disable]
    set wdb [enable|disable]
    set aggd [enable|disable]
    set crwl [enable|disable]
    set rest-api [enable|disable]
end
```

config log eventfilter

Parameter	Description	Type	Size	Default
event	Enable/disable event logging.	option	-	enable
	Option / **Description** *enable* / Enable event logging. *disable* / Disable event logging.			
system	Enable/disable system event logging.	option	-	enable
	Option / **Description** *enable* / Enable system event logging. *disable* / Disable system event logging.			
vpn	Enable/disable VPN event logging.	option	-	enable
	Option / **Description** *enable* / Enable VPN event logging. *disable* / Disable VPN event logging.			
user	Enable/disable user authentication event logging.	option	-	enable
	Option / **Description** *enable* / Enable user authentication event logging. *disable* / Disable user authentication event logging.			
router	Enable/disable router event logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable router event logging. *disable* Disable router event logging.			
wireless-activity	Enable/disable wireless event logging.	option	-	enable
	Option **Description** *enable* Enable wireless event logging. *disable* Disable wireless event logging.			
wan-opt	Enable/disable WAN optimization event logging.	option	-	enable
	Option **Description** *enable* Enable WAN optimization event logging. *disable* Disable WAN optimization event logging.			
endpoint	Enable/disable endpoint event logging.	option	-	enable
	Option **Description** *enable* Enable endpoint event logging. *disable* Disable endpoint event logging.			
ha	Enable/disable ha event logging.	option	-	enable
	Option **Description** *enable* Enable ha event logging. *disable* Disable ha event logging.			
security-rating	Enable/disable Security Rating result logging.	option	-	enable
	Option **Description** *enable* Enable Security Fabric audit result logging. *disable* Disable Security Fabric audit result logging.			
fortiextender	Enable/disable FortiExtender logging.	option	-	enable
	Option **Description** *enable* Enable Forti-Extender logging. *disable* Disable Forti-Extender logging.			

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

Option	Description
enable	Enable SDN connector logging.
disable	Disable SDN connector logging.

Parameter	Description	Type	Size	Default
sdwan	Enable/disable SD-WAN logging.	option	-	enable

Option	Description
enable	Enable SD-WAN logging.
disable	Disable SD-WAN logging.

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

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

Parameter	Description	Type	Size	Default
switch-controller	Enable/disable Switch-Controller logging.	option	-	enable

Option	Description
enable	Enable Switch-Controller logging.
disable	Disable Switch-Controller logging.

Parameter	Description	Type	Size	Default
wcs	Enable/disable log for wcs events.	option	-	enable

Option	Description
enable	Enable Switch-Controller logging.
disable	Disable Switch-Controller logging.

Parameter	Description	Type	Size	Default
wdb	Enable/disable log for wdb events.	option	-	enable

Option	Description
enable	Enable Switch-Controller logging.
disable	Disable Switch-Controller logging.

Parameter	Description	Type	Size	Default
aggd	Enable/disable log for aggd events.	option	-	enable

Option	Description
enable	Enable Switch-Controller logging.

Parameter	Description	Type	Size	Default
	Option: *disable* — Description: Disable Switch-Controller logging.			
crwl	Enable/disable log for crwl events.	option	-	enable
	Option: *enable* — Description: Enable Switch-Controller logging. Option: *disable* — Description: Disable Switch-Controller logging.			
rest-api	Enable/disable REST API logging.	option	-	enable
	Option: *enable* — Description: Enable REST API logging. Option: *disable* — Description: Disable REST API logging.			

config log fortianalyzer-cloud filter

Filters for FortiAnalyzer Cloud.

```
config log fortianalyzer-cloud filter
    Description: Filters for FortiAnalyzer Cloud.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set dlp-archive [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log fortianalyzer-cloud filter

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

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

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

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size	Default
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

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

Option	Description
enable	Enable multicast traffic logging.
disable	Disable multicast traffic logging.

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

Option	Description
enable	Enable sniffer traffic logging.
disable	Disable sniffer traffic logging.

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

Option	Description
enable	Enable ztna traffic logging.
disable	Disable ztna traffic logging.

Parameter	Description	Type	Size	Default
http-transaction	Enable/disable log http-transaction messages.	option	-	enable

Option	Description
enable	Enable ztna traffic logging.
disable	Disable ztna traffic logging.

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

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

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

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

Parameter	Description	Type	Size	Default
dlp-archive	Enable/disable DLP archive logging.	option	-	disable

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

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Option	Description
traffic	Traffic log.
event	Event log.

Parameter	Description	Type	Size	Default
	Option / **Description** *virus* — Antivirus log. *webfilter* — Web filter log. *attack* — Attack log. *spam* — Antispam log. *anomaly* — Anomaly log. *voip* — VoIP log. *dlp* — DLP log. *app-ctrl* — Application control log. *waf* — Web application firewall log. *dns* — DNS detail log. *ssh* — SSH log. *ssl* — SSL log. *file-filter* — File filter log. *icap* — ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter. **Option** / **Description** *include* — Include logs that match the filter. *exclude* — Exclude logs that match the filter.	option	-	include

config log fortianalyzer-cloud override-filter

Override filters for FortiAnalyzer Cloud.

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

```
    set anomaly [enable|disable]
    set voip [enable|disable]
    set dlp-archive [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log fortianalyzer-cloud override-filter

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

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

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

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size	Default
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

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

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option **Description** *enable* Enable anomaly logging. *disable* Disable anomaly logging.			
voip	Enable/disable VoIP logging.	option	-	enable
	Option **Description** *enable* Enable VoIP logging. *disable* Disable VoIP logging.			
dlp-archive	Enable/disable DLP archive logging.	option	-	disable
	Option **Description** *enable* Enable DLP archive logging. *disable* Disable DLP archive logging.			

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Option	Description
traffic	Traffic log.
event	Event log.
virus	Antivirus log.
webfilter	Web filter log.
attack	Attack log.
spam	Antispam log.
anomaly	Anomaly log.
voip	VoIP log.
dlp	DLP log.
app-ctrl	Application control log.
waf	Web application firewall log.
dns	DNS detail log.
ssh	SSH log.
ssl	SSL log.
file-filter	File filter log.
icap	ICAP log.

filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Option	Description
include	Include logs that match the filter.
exclude	Exclude logs that match the filter.

config log fortianalyzer-cloud override-setting

Override FortiAnalyzer Cloud settings.

```
config log fortianalyzer-cloud override-setting
    Description: Override FortiAnalyzer Cloud settings.
    set status [enable|disable]
end
```

config log fortianalyzer-cloud override-setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable

Option	Description
enable	Enable logging to FortiAnalyzer.
disable	Disable logging to FortiAnalyzer.

config log fortianalyzer-cloud setting

Global FortiAnalyzer Cloud settings.

```
config log fortianalyzer-cloud setting
    Description: Global FortiAnalyzer Cloud settings.
    set status [enable|disable]
    set ips-archive [enable|disable]
    set certificate-verification [enable|disable]
    set serial <name1>, <name2>, ...
    set preshared-key {string}
    set access-config [enable|disable]
    set hmac-algorithm [sha256|sha1]
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set conn-timeout {integer}
    set monitor-keepalive-period {integer}
    set monitor-failure-retry-period {integer}
    set certificate {string}
    set source-ip {string}
    set upload-option [store-and-upload|realtime|...]
    set upload-interval [daily|weekly|...]
    set upload-day {user}
    set upload-time {user}
    set priority [default|low]
    set max-log-rate {integer}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log fortianalyzer-cloud setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	Option / **Description** *enable* — Enable logging to FortiAnalyzer. *disable* — Disable logging to FortiAnalyzer.			
ips-archive	Enable/disable IPS packet archive logging.	option	-	disable
	Option / **Description** *enable* — Enable IPS packet archive logging. *disable* — Disable IPS packet archive logging.			
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable
	Option / **Description** *enable* — Enable identity verification of FortiAnalyzer by use of certificate. *disable* — Disable identity verification of FortiAnalyzer by use of certificate.			
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable
	Option / **Description** *enable* — Enable FortiAnalyzer access to configuration and data. *disable* — Disable FortiAnalyzer access to configuration and data.			
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256
	Option / **Description** *sha256* — Use SHA256 as HMAC algorithm. *sha1* — Step down to SHA1 as the HMAC algorithm.			
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	low

Parameter	Description	Type	Size	Default
	Option / **Description** *high-medium* — Encrypt logs using high and medium encryption algorithms. *high* — Encrypt logs using high encryption algorithms. *low* — Encrypt logs using all encryption algorithms.			
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35	
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute
	Option / **Description** *store-and-upload* — Log to hard disk and then upload to FortiAnalyzer.			

Parameter	Description	Type	Size	Default
	Option / **Description** *realtime* — Log directly to FortiAnalyzer in real time. *1-minute* — Log directly to FortiAnalyzer at least every 1 minute. *5-minute* — Log directly to FortiAnalyzer at least every 5 minutes.			
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily
	Option / **Description** *daily* — Upload log files to FortiAnalyzer once a day. *weekly* — Upload log files to FortiAnalyzer once a week. *monthly* — Upload log files to FortiAnalyzer once a month.			
upload-day	Day of week (month) to upload logs.	user	Not Specified	
upload-time	Time to upload logs (hh:mm).	user	Not Specified	
priority	Set log transmission priority.	option	-	default
	Option / **Description** *default* — Set FortiAnalyzer log transmission priority to default. *low* — Set FortiAnalyzer log transmission priority to low.			
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log fortianalyzer2 filter

Filters for FortiAnalyzer.

```
config log fortianalyzer2 filter
    Description: Filters for FortiAnalyzer.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set dlp-archive [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log fortianalyzer2 filter

Parameter	Description	Type	Size	Default
severity	Log every message above and including this severity level.	option	-	information

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

forward-traffic	Enable/disable forward traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable forward traffic logging. *disable* Disable forward traffic logging.			
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option **Description** *enable* Enable local in or out traffic logging. *disable* Disable local in or out traffic logging.			
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
anomaly	Enable/disable anomaly logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable anomaly logging. *disable* — Disable anomaly logging.			
voip	Enable/disable VoIP logging.	option	-	enable
	Option / **Description** *enable* — Enable VoIP logging. *disable* — Disable VoIP logging.			
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	Option / **Description** *enable* — Enable DLP archive logging. *disable* — Disable DLP archive logging.			

config free-style

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

Parameter	Description	Type	Size	Default
	Option / **Description** *ssh* — SSH log. *ssl* — SSL log. *file-filter* — File filter log. *icap* — ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option / **Description** *include* — Include logs that match the filter. *exclude* — Exclude logs that match the filter.			

config log fortianalyzer2 override-filter

Override filters for FortiAnalyzer.

```
config log fortianalyzer2 override-filter
    Description: Override filters for FortiAnalyzer.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set dlp-archive [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log fortianalyzer2 override-filter

Parameter	Description	Type	Size	Default
severity	Log every message above and including this severity level.	option	-	information

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

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

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size	Default
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

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

Option	Description
enable	Enable multicast traffic logging.
disable	Disable multicast traffic logging.

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

Option	Description
enable	Enable sniffer traffic logging.
disable	Disable sniffer traffic logging.

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

Option	Description
enable	Enable ztna traffic logging.
disable	Disable ztna traffic logging.

Parameter	Description	Type	Size	Default
http-transaction	Enable/disable log http-transaction messages.	option	-	enable

Option	Description
enable	Enable ztna traffic logging.
disable	Disable ztna traffic logging.

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

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

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

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

Parameter	Description	Type	Size	Default
dlp-archive	Enable/disable DLP archive logging.	option	-	enable

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

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Option	Description
traffic	Traffic log.
event	Event log.

Parameter	Description	Type	Size	Default
	Option / **Description** *virus* / Antivirus log. *webfilter* / Web filter log. *attack* / Attack log. *spam* / Antispam log. *anomaly* / Anomaly log. *voip* / VoIP log. *dlp* / DLP log. *app-ctrl* / Application control log. *waf* / Web application firewall log. *dns* / DNS detail log. *ssh* / SSH log. *ssl* / SSL log. *file-filter* / File filter log. *icap* / ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option / **Description** *include* / Include logs that match the filter. *exclude* / Exclude logs that match the filter.			

config log fortianalyzer2 override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer2 override-setting
    Description: Override FortiAnalyzer settings.
    set use-management-vdom [enable|disable]
    set status [enable|disable]
    set ips-archive [enable|disable]
    set server {string}
    set certificate-verification [enable|disable]
    set serial <name1>, <name2>, ...
    set preshared-key {string}
```

```
    set access-config [enable|disable]
    set hmac-algorithm [sha256|sha1]
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set conn-timeout {integer}
    set monitor-keepalive-period {integer}
    set monitor-failure-retry-period {integer}
    set certificate {string}
    set source-ip {string}
    set upload-option [store-and-upload|realtime|...]
    set upload-interval [daily|weekly|...]
    set upload-day {user}
    set upload-time {user}
    set reliable [enable|disable]
    set priority [default|low]
    set max-log-rate {integer}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log fortianalyzer2 override-setting

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

Option	Description
enable	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.
disable	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable

Option	Description
enable	Enable logging to FortiAnalyzer.
disable	Disable logging to FortiAnalyzer.

Parameter	Description	Type	Size	Default
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable

Option	Description
enable	Enable IPS packet archive logging.
disable	Disable IPS packet archive logging.

Parameter	Description	Type	Size	Default
server	The remote FortiAnalyzer.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable
	Option / **Description** *enable* — Enable identity verification of FortiAnalyzer by use of certificate. *disable* — Disable identity verification of FortiAnalyzer by use of certificate.			
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable
	Option / **Description** *enable* — Enable FortiAnalyzer access to configuration and data. *disable* — Disable FortiAnalyzer access to configuration and data.			
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256
	Option / **Description** *sha256* — Use SHA256 as HMAC algorithm. *sha1* — Step down to SHA1 as the HMAC algorithm.			
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	low
	Option / **Description** *high-medium* — Encrypt logs using high and medium encryption algorithms. *high* — Encrypt logs using high encryption algorithms. *low* — Encrypt logs using all encryption algorithms.			
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1.			

Parameter	Description	Type	Size	Default
	Option / **Description** *TLSv1-1* / TLSv1.1. *TLSv1-2* / TLSv1.2.			
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35	
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute
	Option / **Description** *store-and-upload* / Log to hard disk and then upload to FortiAnalyzer. *realtime* / Log directly to FortiAnalyzer in real time. *1-minute* / Log directly to FortiAnalyzer at least every 1 minute. *5-minute* / Log directly to FortiAnalyzer at least every 5 minutes.			
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily
	Option / **Description** *daily* / Upload log files to FortiAnalyzer once a day. *weekly* / Upload log files to FortiAnalyzer once a week. *monthly* / Upload log files to FortiAnalyzer once a month.			

Parameter	Description	Type	Size	Default
upload-day	Day of week (month) to upload logs.	user	Not Specified	
upload-time	Time to upload logs (hh:mm).	user	Not Specified	
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable
	Option / **Description** *enable* — Enable reliable logging to FortiAnalyzer. *disable* — Disable reliable logging to FortiAnalyzer.			
priority	Set log transmission priority.	option	-	default
	Option / **Description** *default* — Set FortiAnalyzer log transmission priority to default. *low* — Set FortiAnalyzer log transmission priority to low.			
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log fortianalyzer2 setting

Global FortiAnalyzer settings.

```
config log fortianalyzer2 setting
    Description: Global FortiAnalyzer settings.
    set status [enable|disable]
    set ips-archive [enable|disable]
    set server {string}
    set certificate-verification [enable|disable]
```

```
    set serial <name1>, <name2>, ...
    set preshared-key {string}
    set access-config [enable|disable]
    set hmac-algorithm [sha256|sha1]
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set conn-timeout {integer}
    set monitor-keepalive-period {integer}
    set monitor-failure-retry-period {integer}
    set certificate {string}
    set source-ip {string}
    set upload-option [store-and-upload|realtime|...]
    set upload-interval [daily|weekly|...]
    set upload-day {user}
    set upload-time {user}
    set reliable [enable|disable]
    set priority [default|low]
    set max-log-rate {integer}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log fortianalyzer2 setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	Option / **Description** *enable* — Enable logging to FortiAnalyzer. *disable* — Disable logging to FortiAnalyzer.			
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable
	Option / **Description** *enable* — Enable IPS packet archive logging. *disable* — Disable IPS packet archive logging.			
server	The remote FortiAnalyzer.	string	Maximum length: 127	
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable
	Option / **Description** *enable* — Enable identity verification of FortiAnalyzer by use of certificate. *disable* — Disable identity verification of FortiAnalyzer by use of certificate.			

Parameter	Description	Type	Size	Default
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable
	Option / **Description** *enable* — Enable FortiAnalyzer access to configuration and data. *disable* — Disable FortiAnalyzer access to configuration and data.			
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256
	Option / **Description** *sha256* — Use SHA256 as HMAC algorithm. *sha1* — Step down to SHA1 as the HMAC algorithm.			
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	low
	Option / **Description** *high-medium* — Encrypt logs using high and medium encryption algorithms. *high* — Encrypt logs using high encryption algorithms. *low* — Encrypt logs using all encryption algorithms.			
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10

Parameter	Description	Type	Size	Default
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35	
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute

Option	Description
store-and-upload	Log to hard disk and then upload to FortiAnalyzer.
realtime	Log directly to FortiAnalyzer in real time.
1-minute	Log directly to FortiAnalyzer at least every 1 minute.
5-minute	Log directly to FortiAnalyzer at least every 5 minutes.

upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily

Option	Description
daily	Upload log files to FortiAnalyzer once a day.
weekly	Upload log files to FortiAnalyzer once a week.
monthly	Upload log files to FortiAnalyzer once a month.

upload-day	Day of week (month) to upload logs.	user	Not Specified	
upload-time	Time to upload logs (hh:mm).	user	Not Specified	
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable

Option	Description
enable	Enable reliable logging to FortiAnalyzer.
disable	Disable reliable logging to FortiAnalyzer.

Parameter	Description	Type	Size	Default
priority	Set log transmission priority.	option	-	default
	Option / **Description** *default* — Set FortiAnalyzer log transmission priority to default. *low* — Set FortiAnalyzer log transmission priority to low.			
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log fortianalyzer3 filter

Filters for FortiAnalyzer.

```
config log fortianalyzer3 filter
    Description: Filters for FortiAnalyzer.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set dlp-archive [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
```

```
    end
end
```

config log fortianalyzer3 filter

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

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

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

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size	Default
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

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

Option	Description
enable	Enable multicast traffic logging.
disable	Disable multicast traffic logging.

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

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option **Description** *enable* Enable anomaly logging. *disable* Disable anomaly logging.			
voip	Enable/disable VoIP logging.	option	-	enable
	Option **Description** *enable* Enable VoIP logging. *disable* Disable VoIP logging.			
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	Option **Description** *enable* Enable DLP archive logging. *disable* Disable DLP archive logging.			

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Parameter	Description	Type	Size	Default
	Option / **Description** *traffic* / Traffic log. *event* / Event log. *virus* / Antivirus log. *webfilter* / Web filter log. *attack* / Attack log. *spam* / Antispam log. *anomaly* / Anomaly log. *voip* / VoIP log. *dlp* / DLP log. *app-ctrl* / Application control log. *waf* / Web application firewall log. *dns* / DNS detail log. *ssh* / SSH log. *ssl* / SSL log. *file-filter* / File filter log. *icap* / ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option / **Description** *include* / Include logs that match the filter. *exclude* / Exclude logs that match the filter.			

config log fortianalyzer3 override-filter

Override filters for FortiAnalyzer.

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

```
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set dlp-archive [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log fortianalyzer3 override-filter

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

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

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

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size	Default
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

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

Option	Description
enable	Enable multicast traffic logging.
disable	Disable multicast traffic logging.

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

Option	Description
enable	Enable sniffer traffic logging.
disable	Disable sniffer traffic logging.

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

Option	Description
enable	Enable ztna traffic logging.
disable	Disable ztna traffic logging.

Parameter	Description	Type	Size	Default
http-transaction	Enable/disable log http-transaction messages.	option	-	enable

Option	Description
enable	Enable ztna traffic logging.
disable	Disable ztna traffic logging.

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

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

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

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

Parameter	Description	Type	Size	Default
dlp-archive	Enable/disable DLP archive logging.	option	-	enable

Parameter	Description	Type	Size	Default

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

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Option	Description
traffic	Traffic log.
event	Event log.
virus	Antivirus log.
webfilter	Web filter log.
attack	Attack log.
spam	Antispam log.
anomaly	Anomaly log.
voip	VoIP log.
dlp	DLP log.
app-ctrl	Application control log.
waf	Web application firewall log.
dns	DNS detail log.
ssh	SSH log.
ssl	SSL log.
file-filter	File filter log.
icap	ICAP log.

filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Option	Description
include	Include logs that match the filter.
exclude	Exclude logs that match the filter.

config log fortianalyzer3 override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer3 override-setting
    Description: Override FortiAnalyzer settings.
    set use-management-vdom [enable|disable]
    set status [enable|disable]
    set ips-archive [enable|disable]
    set server {string}
    set certificate-verification [enable|disable]
    set serial <name1>, <name2>, ...
    set preshared-key {string}
    set access-config [enable|disable]
    set hmac-algorithm [sha256|sha1]
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set conn-timeout {integer}
    set monitor-keepalive-period {integer}
    set monitor-failure-retry-period {integer}
    set certificate {string}
    set source-ip {string}
    set upload-option [store-and-upload|realtime|...]
    set upload-interval [daily|weekly|...]
    set upload-day {user}
    set upload-time {user}
    set reliable [enable|disable]
    set priority [default|low]
    set max-log-rate {integer}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log fortianalyzer3 override-setting

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

Option	Description
enable	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.
disable	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.

status	Enable/disable logging to FortiAnalyzer.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable logging to FortiAnalyzer. *disable* — Disable logging to FortiAnalyzer.			
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable
	Option / **Description** *enable* — Enable IPS packet archive logging. *disable* — Disable IPS packet archive logging.			
server	The remote FortiAnalyzer.	string	Maximum length: 127	
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable
	Option / **Description** *enable* — Enable identity verification of FortiAnalyzer by use of certificate. *disable* — Disable identity verification of FortiAnalyzer by use of certificate.			
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable
	Option / **Description** *enable* — Enable FortiAnalyzer access to configuration and data. *disable* — Disable FortiAnalyzer access to configuration and data.			
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256
	Option / **Description** *sha256* — Use SHA256 as HMAC algorithm. *sha1* — Step down to SHA1 as the HMAC algorithm.			
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	low

Parameter	Description	Type	Size	Default
	Option / **Description** *high-medium* — Encrypt logs using high and medium encryption algorithms. *high* — Encrypt logs using high encryption algorithms. *low* — Encrypt logs using all encryption algorithms.			
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35	
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute
	Option / **Description** *store-and-upload* — Log to hard disk and then upload to FortiAnalyzer.			

Parameter	Description	Type	Size	Default
	Option / **Description** *realtime* — Log directly to FortiAnalyzer in real time. *1-minute* — Log directly to FortiAnalyzer at least every 1 minute. *5-minute* — Log directly to FortiAnalyzer at least every 5 minutes.			
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily
	Option / **Description** *daily* — Upload log files to FortiAnalyzer once a day. *weekly* — Upload log files to FortiAnalyzer once a week. *monthly* — Upload log files to FortiAnalyzer once a month.			
upload-day	Day of week (month) to upload logs.	user	Not Specified	
upload-time	Time to upload logs (hh:mm).	user	Not Specified	
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable
	Option / **Description** *enable* — Enable reliable logging to FortiAnalyzer. *disable* — Disable reliable logging to FortiAnalyzer.			
priority	Set log transmission priority.	option	-	default
	Option / **Description** *default* — Set FortiAnalyzer log transmission priority to default. *low* — Set FortiAnalyzer log transmission priority to low.			
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules.			

Parameter	Description	Type	Size	Default
	Option: *specify* — Description: Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log fortianalyzer3 setting

Global FortiAnalyzer settings.

```
config log fortianalyzer3 setting
    Description: Global FortiAnalyzer settings.
    set status [enable|disable]
    set ips-archive [enable|disable]
    set server {string}
    set certificate-verification [enable|disable]
    set serial <name1>, <name2>, ...
    set preshared-key {string}
    set access-config [enable|disable]
    set hmac-algorithm [sha256|sha1]
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set conn-timeout {integer}
    set monitor-keepalive-period {integer}
    set monitor-failure-retry-period {integer}
    set certificate {string}
    set source-ip {string}
    set upload-option [store-and-upload|realtime|...]
    set upload-interval [daily|weekly|...]
    set upload-day {user}
    set upload-time {user}
    set reliable [enable|disable]
    set priority [default|low]
    set max-log-rate {integer}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log fortianalyzer3 setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable logging to FortiAnalyzer. *disable* — Disable logging to FortiAnalyzer.			
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable
	Option / **Description** *enable* — Enable IPS packet archive logging. *disable* — Disable IPS packet archive logging.			
server	The remote FortiAnalyzer.	string	Maximum length: 127	
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable
	Option / **Description** *enable* — Enable identity verification of FortiAnalyzer by use of certificate. *disable* — Disable identity verification of FortiAnalyzer by use of certificate.			
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable
	Option / **Description** *enable* — Enable FortiAnalyzer access to configuration and data. *disable* — Disable FortiAnalyzer access to configuration and data.			
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256
	Option / **Description** *sha256* — Use SHA256 as HMAC algorithm. *sha1* — Step down to SHA1 as the HMAC algorithm.			
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	low

Parameter	Description	Type	Size	Default
	Option / **Description** *high-medium* — Encrypt logs using high and medium encryption algorithms. *high* — Encrypt logs using high encryption algorithms. *low* — Encrypt logs using all encryption algorithms.			
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35	
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute
	Option / **Description** *store-and-upload* — Log to hard disk and then upload to FortiAnalyzer.			

Parameter	Description	Type	Size	Default
	Option / **Description** *realtime* / Log directly to FortiAnalyzer in real time. *1-minute* / Log directly to FortiAnalyzer at least every 1 minute. *5-minute* / Log directly to FortiAnalyzer at least every 5 minutes.			
upload-interval	Frequency to upload log files to FortiAnalyzer. **Option** / **Description** *daily* / Upload log files to FortiAnalyzer once a day. *weekly* / Upload log files to FortiAnalyzer once a week. *monthly* / Upload log files to FortiAnalyzer once a month.	option	-	daily
upload-day	Day of week (month) to upload logs.	user	Not Specified	
upload-time	Time to upload logs (hh:mm).	user	Not Specified	
reliable	Enable/disable reliable logging to FortiAnalyzer. **Option** / **Description** *enable* / Enable reliable logging to FortiAnalyzer. *disable* / Disable reliable logging to FortiAnalyzer.	option	-	disable
priority	Set log transmission priority. **Option** / **Description** *default* / Set FortiAnalyzer log transmission priority to default. *low* / Set FortiAnalyzer log transmission priority to low.	option	-	default
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

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

config log fortianalyzer filter

Filters for FortiAnalyzer.

```
config log fortianalyzer filter
    Description: Filters for FortiAnalyzer.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set dlp-archive [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log fortianalyzer filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option: *emergency* — Emergency level.			

Parameter	Description	Type	Size	Default
	Option / **Description** *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.			
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable forward traffic logging. *disable* — Disable forward traffic logging.			
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable local in or out traffic logging. *disable* — Disable local in or out traffic logging.			
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable multicast traffic logging. *disable* — Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable sniffer traffic logging. *disable* — Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable ztna traffic logging.			

Parameter	Description	Type	Size	Default
	Option **Description** *disable* Disable ztna traffic logging.			
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option **Description** *enable* Enable anomaly logging. *disable* Disable anomaly logging.			
voip	Enable/disable VoIP logging.	option	-	enable
	Option **Description** *enable* Enable VoIP logging. *disable* Disable VoIP logging.			
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	Option **Description** *enable* Enable DLP archive logging. *disable* Disable DLP archive logging.			

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option **Description** *traffic* Traffic log. *event* Event log. *virus* Antivirus log. *webfilter* Web filter log.			

Parameter	Description	Type	Size	Default
	Option / **Description** *attack* — Attack log. *spam* — Antispam log. *anomaly* — Anomaly log. *voip* — VoIP log. *dlp* — DLP log. *app-ctrl* — Application control log. *waf* — Web application firewall log. *dns* — DNS detail log. *ssh* — SSH log. *ssl* — SSL log. *file-filter* — File filter log. *icap* — ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter. **Option** / **Description** *include* — Include logs that match the filter. *exclude* — Exclude logs that match the filter.	option	-	include

config log fortianalyzer override-filter

Override filters for FortiAnalyzer.

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

```
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log fortianalyzer override-filter

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

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

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

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size	Default
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

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

Option	Description
enable	Enable multicast traffic logging.

Parameter	Description	Type	Size	Default
	Option **Description** *disable* Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option **Description** *enable* Enable anomaly logging. *disable* Disable anomaly logging.			
voip	Enable/disable VoIP logging.	option	-	enable
	Option **Description** *enable* Enable VoIP logging. *disable* Disable VoIP logging.			
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	Option **Description** *enable* Enable DLP archive logging. *disable* Disable DLP archive logging.			

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Option	Description
traffic	Traffic log.
event	Event log.
virus	Antivirus log.
webfilter	Web filter log.
attack	Attack log.
spam	Antispam log.
anomaly	Anomaly log.
voip	VoIP log.
dlp	DLP log.
app-ctrl	Application control log.
waf	Web application firewall log.
dns	DNS detail log.
ssh	SSH log.
ssl	SSL log.
file-filter	File filter log.
icap	ICAP log.

filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Option	Description
include	Include logs that match the filter.
exclude	Exclude logs that match the filter.

config log fortianalyzer override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer override-setting
    Description: Override FortiAnalyzer settings.
    set use-management-vdom [enable|disable]
    set status [enable|disable]
    set ips-archive [enable|disable]
    set server {string}
    set certificate-verification [enable|disable]
    set serial <name1>, <name2>, ...
    set preshared-key {string}
    set access-config [enable|disable]
    set hmac-algorithm [sha256|sha1]
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set conn-timeout {integer}
    set monitor-keepalive-period {integer}
    set monitor-failure-retry-period {integer}
    set certificate {string}
    set source-ip {string}
    set upload-option [store-and-upload|realtime|...]
    set upload-interval [daily|weekly|...]
    set upload-day {user}
    set upload-time {user}
    set reliable [enable|disable]
    set priority [default|low]
    set max-log-rate {integer}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log fortianalyzer override-setting

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

Option	Description
enable	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.
disable	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable

Option	Description
enable	Enable logging to FortiAnalyzer.
disable	Disable logging to FortiAnalyzer.

Parameter	Description	Type	Size	Default
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable
	Option / **Description** *enable* / Enable IPS packet archive logging. *disable* / Disable IPS packet archive logging.			
server	The remote FortiAnalyzer.	string	Maximum length: 127	
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable
	Option / **Description** *enable* / Enable identity verification of FortiAnalyzer by use of certificate. *disable* / Disable identity verification of FortiAnalyzer by use of certificate.			
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable
	Option / **Description** *enable* / Enable FortiAnalyzer access to configuration and data. *disable* / Disable FortiAnalyzer access to configuration and data.			
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256
	Option / **Description** *sha256* / Use SHA256 as HMAC algorithm. *sha1* / Step down to SHA1 as the HMAC algorithm.			
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	low
	Option / **Description** *high-medium* / Encrypt logs using high and medium encryption algorithms. *high* / Encrypt logs using high encryption algorithms. *low* / Encrypt logs using all encryption algorithms.			

Parameter	Description	Type	Size	Default
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections . **Option** — **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.	option	-	default
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35	
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer. **Option** — **Description** *store-and-upload* — Log to hard disk and then upload to FortiAnalyzer. *realtime* — Log directly to FortiAnalyzer in real time. *1-minute* — Log directly to FortiAnalyzer at least every 1 minute. *5-minute* — Log directly to FortiAnalyzer at least every 5 minutes.	option	-	5-minute
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily

Parameter	Description	Type	Size	Default
	Option / **Description** *daily* — Upload log files to FortiAnalyzer once a day. *weekly* — Upload log files to FortiAnalyzer once a week. *monthly* — Upload log files to FortiAnalyzer once a month.			
upload-day	Day of week (month) to upload logs.	user	Not Specified	
upload-time	Time to upload logs (hh:mm).	user	Not Specified	
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable
	Option / **Description** *enable* — Enable reliable logging to FortiAnalyzer. *disable* — Disable reliable logging to FortiAnalyzer.			
priority	Set log transmission priority.	option	-	default
	Option / **Description** *default* — Set FortiAnalyzer log transmission priority to default. *low* — Set FortiAnalyzer log transmission priority to low.			
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log fortianalyzer setting

Global FortiAnalyzer settings.

```
config log fortianalyzer setting
    Description: Global FortiAnalyzer settings.
    set status [enable|disable]
    set ips-archive [enable|disable]
    set server {string}
    set certificate-verification [enable|disable]
    set serial <name1>, <name2>, ...
    set preshared-key {string}
    set access-config [enable|disable]
    set hmac-algorithm [sha256|sha1]
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set conn-timeout {integer}
    set monitor-keepalive-period {integer}
    set monitor-failure-retry-period {integer}
    set certificate {string}
    set source-ip {string}
    set upload-option [store-and-upload|realtime|...]
    set upload-interval [daily|weekly|...]
    set upload-day {user}
    set upload-time {user}
    set reliable [enable|disable]
    set priority [default|low]
    set max-log-rate {integer}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log fortianalyzer setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable

Option	Description
enable	Enable logging to FortiAnalyzer.
disable	Disable logging to FortiAnalyzer.

Parameter	Description	Type	Size	Default
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable

Option	Description
enable	Enable IPS packet archive logging.
disable	Disable IPS packet archive logging.

Parameter	Description	Type	Size	Default
server	The remote FortiAnalyzer.	string	Maximum length: 127	
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable

Option	Description
enable	Enable identity verification of FortiAnalyzer by use of certificate.
disable	Disable identity verification of FortiAnalyzer by use of certificate.

serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable

Option	Description
enable	Enable FortiAnalyzer access to configuration and data.
disable	Disable FortiAnalyzer access to configuration and data.

hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256

Option	Description
sha256	Use SHA256 as HMAC algorithm.
sha1	Step down to SHA1 as the HMAC algorithm.

enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	low

Option	Description
high-medium	Encrypt logs using high and medium encryption algorithms.
high	Encrypt logs using high encryption algorithms.
low	Encrypt logs using all encryption algorithms.

ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default

Parameter	Description	Type	Size	Default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35	
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute
	Option / **Description** *store-and-upload* — Log to hard disk and then upload to FortiAnalyzer. *realtime* — Log directly to FortiAnalyzer in real time. *1-minute* — Log directly to FortiAnalyzer at least every 1 minute. *5-minute* — Log directly to FortiAnalyzer at least every 5 minutes.			
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily

Parameter	Description	Type	Size	Default
	Option / **Description** *daily* — Upload log files to FortiAnalyzer once a day. *weekly* — Upload log files to FortiAnalyzer once a week. *monthly* — Upload log files to FortiAnalyzer once a month.			
upload-day	Day of week (month) to upload logs.	user	Not Specified	
upload-time	Time to upload logs (hh:mm).	user	Not Specified	
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable
	Option / **Description** *enable* — Enable reliable logging to FortiAnalyzer. *disable* — Disable reliable logging to FortiAnalyzer.			
priority	Set log transmission priority.	option	-	default
	Option / **Description** *default* — Set FortiAnalyzer log transmission priority to default. *low* — Set FortiAnalyzer log transmission priority to low.			
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log fortiguard filter

Filters for FortiCloud.

```
config log fortiguard filter
    Description: Filters for FortiCloud.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log fortiguard filter

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

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

forward-traffic	Enable/disable forward traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable forward traffic logging. *disable* Disable forward traffic logging.			
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option **Description** *enable* Enable local in or out traffic logging. *disable* Disable local in or out traffic logging.			
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
anomaly	Enable/disable anomaly logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable anomaly logging. *disable* — Disable anomaly logging.			
voip	Enable/disable VoIP logging.	option	-	enable
	Option / **Description** *enable* — Enable VoIP logging. *disable* — Disable VoIP logging.			

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option / **Description** *traffic* — Traffic log. *event* — Event log. *virus* — Antivirus log. *webfilter* — Web filter log. *attack* — Attack log. *spam* — Antispam log. *anomaly* — Anomaly log. *voip* — VoIP log. *dlp* — DLP log. *app-ctrl* — Application control log. *waf* — Web application firewall log. *dns* — DNS detail log. *ssh* — SSH log. *ssl* — SSL log. *file-filter* — File filter log. *icap* — ICAP log.			

Parameter	Description	Type	Size	Default
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Option	Description
include	Include logs that match the filter.
exclude	Exclude logs that match the filter.

config log fortiguard override-filter

Override filters for FortiCloud.

```
config log fortiguard override-filter
    Description: Override filters for FortiCloud.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log fortiguard override-filter

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

Option	Description
emergency	Emergency level.
alert	Alert level.

Parameter	Description	Type	Size	Default
	Option / **Description** *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.			
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable forward traffic logging. *disable* — Disable forward traffic logging.			
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable local in or out traffic logging. *disable* — Disable local in or out traffic logging.			
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable multicast traffic logging. *disable* — Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable sniffer traffic logging. *disable* — Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable ztna traffic logging. *disable* — Disable ztna traffic logging.			

Parameter	Description	Type	Size	Default
http-transaction	Enable/disable log http-transaction messages.	option	-	enable

Option	Description
enable	Enable ztna traffic logging.
disable	Disable ztna traffic logging.

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

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

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

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

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Option	Description
traffic	Traffic log.
event	Event log.
virus	Antivirus log.
webfilter	Web filter log.
attack	Attack log.
spam	Antispam log.
anomaly	Anomaly log.
voip	VoIP log.
dlp	DLP log.
app-ctrl	Application control log.

Parameter	Description	Type	Size	Default
	Option / **Description** *waf* / Web application firewall log. *dns* / DNS detail log. *ssh* / SSH log. *ssl* / SSL log. *file-filter* / File filter log. *icap* / ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter. **Option** / **Description** *include* / Include logs that match the filter. *exclude* / Exclude logs that match the filter.	option	-	include

config log fortiguard override-setting

Override global FortiCloud logging settings for this VDOM.

```
config log fortiguard override-setting
    Description: Override global FortiCloud logging settings for this VDOM.
    set override [enable|disable]
    set status [enable|disable]
    set upload-option [store-and-upload|realtime|...]
    set upload-interval [daily|weekly|...]
    set upload-day {user}
    set upload-time {user}
    set priority [default|low]
    set max-log-rate {integer}
    set access-config [enable|disable]
end
```

config log fortiguard override-setting

Parameter	Description	Type	Size	Default
override	Overriding FortiCloud settings for this VDOM or use global settings.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Override FortiCloud logging settings. *disable* — Use global FortiCloud logging settings.			
status	Enable/disable logging to FortiCloud.	option	-	disable
	Option / **Description** *enable* — Enable logging to FortiCloud. *disable* — Disable logging to FortiCloud.			
upload-option	Configure how log messages are sent to FortiCloud.	option	-	5-minute
	Option / **Description** *store-and-upload* — Log to the hard disk and then upload logs to FortiCloud. *realtime* — Log directly to FortiCloud in real time. *1-minute* — Log directly to FortiCloud at 1-minute intervals. *5-minute* — Log directly to FortiCloud at 5-minute intervals.			
upload-interval	Frequency of uploading log files to FortiCloud.	option	-	daily
	Option / **Description** *daily* — Upload log files to FortiCloud once a day. *weekly* — Upload log files to FortiCloud once a week. *monthly* — Upload log files to FortiCloud once a month.			
upload-day	Day of week to roll logs.	user	Not Specified	
upload-time	Time of day to roll logs (hh:mm).	user	Not Specified	
priority	Set log transmission priority.	option	-	default
	Option / **Description** *default* — Set FortiCloud log transmission priority to default. *low* — Set FortiCloud log transmission priority to low.			

Parameter	Description	Type	Size	Default
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
access-config	Enable/disable FortiCloud access to configuration and data.	option	-	enable

Option	Description
enable	Enable FortiCloud access to configuration and data.
disable	Disable FortiCloud access to configuration and data.

config log fortiguard setting

Configure logging to FortiCloud.

```
config log fortiguard setting
    Description: Configure logging to FortiCloud.
    set status [enable|disable]
    set upload-option [store-and-upload|realtime|...]
    set upload-interval [daily|weekly|...]
    set upload-day {user}
    set upload-time {user}
    set priority [default|low]
    set max-log-rate {integer}
    set access-config [enable|disable]
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set conn-timeout {integer}
    set source-ip {ipv4-address}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log fortiguard setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiCloud.	option	-	disable

Option	Description
enable	Enable logging to FortiCloud.
disable	Disable logging to FortiCloud.

Parameter	Description	Type	Size	Default
upload-option	Configure how log messages are sent to FortiCloud.	option	-	5-minute
	Option / **Description** *store-and-upload* — Log to the hard disk and then upload logs to FortiCloud. *realtime* — Log directly to FortiCloud in real time. *1-minute* — Log directly to FortiCloud at 1-minute intervals. *5-minute* — Log directly to FortiCloud at 5-minute intervals.			
upload-interval	Frequency of uploading log files to FortiCloud.	option	-	daily
	Option / **Description** *daily* — Upload log files to FortiCloud once a day. *weekly* — Upload log files to FortiCloud once a week. *monthly* — Upload log files to FortiCloud once a month.			
upload-day	Day of week to roll logs.	user	Not Specified	
upload-time	Time of day to roll logs (hh:mm).	user	Not Specified	
priority	Set log transmission priority.	option	-	default
	Option / **Description** *default* — Set FortiCloud log transmission priority to default. *low* — Set FortiCloud log transmission priority to low.			
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
access-config	Enable/disable FortiCloud access to configuration and data.	option	-	enable
	Option / **Description** *enable* — Enable FortiCloud access to configuration and data. *disable* — Disable FortiCloud access to configuration and data.			
enc-algorithm	Configure the level of SSL protection for secure communication with FortiCloud.	option	-	low

Parameter	Description	Type	Size	Default
	Option / **Description** *high-medium* — Encrypt logs using high and medium encryption. *high* — Encrypt logs using high encryption. *low* — Encrypt logs using low encryption.			
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			
conn-timeout	FortiProxy Cloud connection timeout in seconds.	integer	Minimum value: 1 Maximum value: 3600	10
source-ip	Source IP address used to connect FortiCloud.	ipv4-address	Not Specified	0.0.0.0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log gui-display

Configure how log messages are displayed on the GUI.

```
config log gui-display
    Description: Configure how log messages are displayed on the GUI.
    set resolve-hosts [enable|disable]
```

```
    set resolve-apps [enable|disable]
    set fortiview-unscanned-apps [enable|disable]
end
```

config log gui-display

Parameter	Description	Type	Size	Default
resolve-hosts	Enable/disable resolving IP addresses to hostname in log messages on the GUI using reverse DNS lookup.	option	-	enable

Option	Description
enable	Enable resolving IP addresses to hostnames.
disable	Disable resolving IP addresses to hostnames.

Parameter	Description	Type	Size	Default
resolve-apps	Resolve unknown applications on the GUI using Fortinet's remote application database.	option	-	enable

Option	Description
enable	Enable unknown applications on the GUI.
disable	Disable unknown applications on the GUI.

Parameter	Description	Type	Size	Default
fortiview-unscanned-apps	Enable/disable showing unscanned traffic in FortiView application charts.	option	-	disable

Option	Description
enable	Enable showing unscanned traffic.
disable	Disable showing unscanned traffic.

config log memory filter

Filters for memory buffer.

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

```
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log memory filter

Parameter	Description	Type	Size	Default
severity	Log every message above and including this severity level.	option	-	information

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

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

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size	Default
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

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

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option **Description** *enable* Enable anomaly logging. *disable* Disable anomaly logging.			
voip	Enable/disable VoIP logging.	option	-	enable
	Option **Description** *enable* Enable VoIP logging. *disable* Disable VoIP logging.			

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Parameter	Description	Type	Size	Default
	Option / **Description** *traffic* / Traffic log. *event* / Event log. *virus* / Antivirus log. *webfilter* / Web filter log. *attack* / Attack log. *spam* / Antispam log. *anomaly* / Anomaly log. *voip* / VoIP log. *dlp* / DLP log. *app-ctrl* / Application control log. *waf* / Web application firewall log. *dns* / DNS detail log. *ssh* / SSH log. *ssl* / SSL log. *file-filter* / File filter log. *icap* / ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option / **Description** *include* / Include logs that match the filter. *exclude* / Exclude logs that match the filter.			

config log memory global-setting

Global settings for memory logging.

```
config log memory global-setting
    Description: Global settings for memory logging.
    set max-size {integer}
    set full-first-warning-threshold {integer}
    set full-second-warning-threshold {integer}
```

```
    set full-final-warning-threshold {integer}
end
```

config log memory global-setting

Parameter	Description	Type	Size	Default
max-size	Maximum amount of memory that can be used for memory logging in bytes.	integer	Minimum value: 0 Maximum value: 4294967295	10345676
full-first-warning-threshold	Log full first warning threshold as a percent .	integer	Minimum value: 1 Maximum value: 98	75
full-second-warning-threshold	Log full second warning threshold as a percent .	integer	Minimum value: 2 Maximum value: 99	90
full-final-warning-threshold	Log full final warning threshold as a percent .	integer	Minimum value: 3 Maximum value: 100	95

config log memory setting

Settings for memory buffer.

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

config log memory setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to the FortiProxy's memory.	option	-	disable

Option	Description
enable	Enable logging to memory.
disable	Disable logging to memory.

config log null-device filter

Filters for null device logging.

```
config log null-device filter
    Description: Filters for null device logging.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log null-device filter

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

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

forward-traffic	Enable/disable forward traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable forward traffic logging. *disable* Disable forward traffic logging.			
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option **Description** *enable* Enable local in or out traffic logging. *disable* Disable local in or out traffic logging.			
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
anomaly	Enable/disable anomaly logging.	option	-	enable

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

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option / **Description** *traffic* / Traffic log. *event* / Event log. *virus* / Antivirus log. *webfilter* / Web filter log. *attack* / Attack log. *spam* / Antispam log. *anomaly* / Anomaly log. *voip* / VoIP log. *dlp* / DLP log. *app-ctrl* / Application control log. *waf* / Web application firewall log. *dns* / DNS detail log. *ssh* / SSH log. *ssl* / SSL log. *file-filter* / File filter log. *icap* / ICAP log.			

Parameter	Description	Type	Size	Default
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Option	Description
include	Include logs that match the filter.
exclude	Exclude logs that match the filter.

config log null-device setting

Settings for null device logging.

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

config log null-device setting

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

Option	Description
enable	Enable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).
disable	Disable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).

config log setting

Configure general log settings.

```
config log setting
    Description: Configure general log settings.
    set resolve-ip [enable|disable]
    set resolve-port [enable|disable]
    set log-user-in-upper [enable|disable]
```

```
    set fwpolicy-implicit-log [enable|disable]
    set fwpolicy6-implicit-log [enable|disable]
    set log-invalid-packet [enable|disable]
    set local-in-allow [enable|disable]
    set local-in-deny-unicast [enable|disable]
    set local-in-deny-broadcast [enable|disable]
    set local-out [enable|disable]
    set daemon-log [enable|disable]
    set neighbor-event [enable|disable]
    set brief-traffic-format [enable|disable]
    set user-anonymize [enable|disable]
    set expolicy-implicit-log [enable|disable]
    set log-policy-comment [enable|disable]
    set faz-override [enable|disable]
    set syslog-override [enable|disable]
    set rest-api-set [enable|disable]
    set rest-api-get [enable|disable]
    set custom-log-fields <field-id1>, <field-id2>, ...
    set anonymization-hash {string}
end
```

config log setting

Parameter	Description	Type	Size	Default
resolve-ip	Enable/disable adding resolved domain names to traffic logs if possible.	option	-	disable
	Option / **Description** *enable* — Enable adding resolved domain names to traffic logs. *disable* — Disable adding resolved domain names to traffic logs.			
resolve-port	Enable/disable adding resolved service names to traffic logs.	option	-	enable
	Option / **Description** *enable* — Enable adding resolved service names to traffic logs. *disable* — Disable adding resolved service names to traffic logs.			
log-user-in-upper	Enable/disable logs with user-in-upper.	option	-	disable
	Option / **Description** *enable* — Enable logs with user-in-upper. *disable* — Disable logs with user-in-upper.			
fwpolicy-implicit-log	Enable/disable implicit firewall policy logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable implicit firewall policy logging. *disable* Disable implicit firewall policy logging.			
fwpolicy6-implicit-log	Enable/disable implicit firewall policy6 logging.	option	-	disable
	Option **Description** *enable* Enable implicit firewall policy6 logging. *disable* Disable implicit firewall policy6 logging.			
log-invalid-packet	Enable/disable invalid packet traffic logging.	option	-	disable
	Option **Description** *enable* Enable invalid packet traffic logging. *disable* Disable invalid packet traffic logging.			
local-in-allow	Enable/disable local-in-allow logging.	option	-	disable
	Option **Description** *enable* Enable local-in-allow logging. *disable* Disable local-in-allow logging.			
local-in-deny-unicast	Enable/disable local-in-deny-unicast logging.	option	-	disable
	Option **Description** *enable* Enable local-in-deny-unicast logging. *disable* Disable local-in-deny-unicast logging.			
local-in-deny-broadcast	Enable/disable local-in-deny-broadcast logging.	option	-	disable
	Option **Description** *enable* Enable local-in-deny-broadcast logging. *disable* Disable local-in-deny-broadcast logging.			
local-out	Enable/disable local-out logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable local-out logging. *disable* Disable local-out logging.			
daemon-log	Enable/disable daemon logging.	option	-	disable
	Option **Description** *enable* Enable daemon logging. *disable* Disable daemon logging.			
neighbor-event	Enable/disable neighbor event logging.	option	-	disable
	Option **Description** *enable* Enable neighbor event logging. *disable* Disable neighbor event logging.			
brief-traffic-format	Enable/disable brief format traffic logging.	option	-	disable
	Option **Description** *enable* Enable brief format traffic logging. *disable* Disable brief format traffic logging.			
user-anonymize	Enable/disable anonymizing user names in log messages.	option	-	disable
	Option **Description** *enable* Enable anonymizing user names in log messages. *disable* Disable anonymizing user names in log messages.			
expolicy-implicit-log	Enable/disable explicit proxy firewall implicit policy logging.	option	-	disable
	Option **Description** *enable* Enable explicit proxy firewall implicit policy logging. *disable* Disable explicit proxy firewall implicit policy logging.			
log-policy-comment	Enable/disable inserting policy comments into traffic logs.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable inserting policy comments into traffic logs. *disable* — Disable inserting policy comments into traffic logs.			
faz-override	Enable/disable override FortiAnalyzer settings.	option	-	disable
	Option / **Description** *enable* — Enable override FortiAnalyzer settings. *disable* — Disable override FortiAnalyzer settings.			
syslog-override	Enable/disable override Syslog settings.	option	-	disable
	Option / **Description** *enable* — Enable override Syslog settings. *disable* — Disable override Syslog settings.			
rest-api-set	Enable/disable REST API POST/PUT/DELETE request logging.	option	-	disable
	Option / **Description** *enable* — Enable POST/PUT/DELETE REST API logging. *disable* — Disable POST/PUT/DELETE REST API logging.			
rest-api-get	Enable/disable REST API GET request logging.	option	-	disable
	Option / **Description** *enable* — Enable GET REST API logging. *disable* — Disable GET REST API logging.			
custom-log-fields `<field-id>`	Custom fields to append to all log messages. Custom log field.	string	Maximum length: 35	
anonymization-hash	User name anonymization hash salt.	string	Maximum length: 32	

config log syslogd2 filter

Filters for remote system server.

```
config log syslogd2 filter
    Description: Filters for remote system server.
    set severity [emergency|alert|...]
```

```
        set forward-traffic [enable|disable]
        set local-traffic [enable|disable]
        set multicast-traffic [enable|disable]
        set sniffer-traffic [enable|disable]
        set ztna-traffic [enable|disable]
        set http-transaction [enable|disable]
        set anomaly [enable|disable]
        set voip [enable|disable]
        config free-style
            Description: Free style filters.
            edit <id>
                set category [traffic|event|...]
                set filter {string}
                set filter-type [include|exclude]
            next
        end
    end
```

config log syslogd2 filter

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

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

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

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size	Default
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Option	Description
enable	Enable local in or out traffic logging.

Parameter	Description	Type	Size	Default
	Option **Description** *disable* Disable local in or out traffic logging.			
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option **Description** *enable* Enable anomaly logging. *disable* Disable anomaly logging.			
voip	Enable/disable VoIP logging.	option	-	enable
	Option **Description** *enable* Enable VoIP logging. *disable* Disable VoIP logging.			

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Option	Description
traffic	Traffic log.
event	Event log.
virus	Antivirus log.
webfilter	Web filter log.
attack	Attack log.
spam	Antispam log.
anomaly	Anomaly log.
voip	VoIP log.
dlp	DLP log.
app-ctrl	Application control log.
waf	Web application firewall log.
dns	DNS detail log.
ssh	SSH log.
ssl	SSL log.
file-filter	File filter log.
icap	ICAP log.

filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Option	Description
include	Include logs that match the filter.
exclude	Exclude logs that match the filter.

config log syslogd2 override-filter

Override filters for remote system server.

```
config log syslogd2 override-filter
    Description: Override filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log syslogd2 override-filter

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

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

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

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size	Default
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable local in or out traffic logging. *disable* — Disable local in or out traffic logging.			
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable multicast traffic logging. *disable* — Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable sniffer traffic logging. *disable* — Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable ztna traffic logging. *disable* — Disable ztna traffic logging.			
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option / **Description** *enable* — Enable ztna traffic logging. *disable* — Disable ztna traffic logging.			
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option / **Description** *enable* — Enable anomaly logging. *disable* — Disable anomaly logging.			
voip	Enable/disable VoIP logging.	option	-	enable
	Option / **Description** *enable* — Enable VoIP logging. *disable* — Disable VoIP logging.			

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Option	Description
traffic	Traffic log.
event	Event log.
virus	Antivirus log.
webfilter	Web filter log.
attack	Attack log.
spam	Antispam log.
anomaly	Anomaly log.
voip	VoIP log.
dlp	DLP log.
app-ctrl	Application control log.
waf	Web application firewall log.
dns	DNS detail log.
ssh	SSH log.
ssl	SSL log.
file-filter	File filter log.
icap	ICAP log.

filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Option	Description
include	Include logs that match the filter.
exclude	Exclude logs that match the filter.

config log syslogd2 override-setting

Override settings for remote syslog server.

```
config log syslogd2 override-setting
    Description: Override settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log syslogd2 override-setting

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

Parameter	Description	Type	Size	Default
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7

Option	Description
kernel	Kernel messages.
user	Random user-level messages.
mail	Mail system.
daemon	System daemons.
auth	Security/authorization messages.
syslog	Messages generated internally by syslog.
lpr	Line printer subsystem.
news	Network news subsystem.
uucp	Network news subsystem.
cron	Clock daemon.
authpriv	Security/authorization messages (private).
ftp	FTP daemon.
ntp	NTP daemon.
audit	Log audit.
alert	Log alert.
clock	Clock daemon.
local0	Reserved for local use.
local1	Reserved for local use.
local2	Reserved for local use.
local3	Reserved for local use.
local4	Reserved for local use.
local5	Reserved for local use.
local6	Reserved for local use.
local7	Reserved for local use.

Parameter	Description	Type	Size	Default
source-ip	Source IP address of syslog.	string	Maximum length: 63	
format	Log format.	option	-	default

Option	Description
default	Syslog format.
csv	CSV (Comma Separated Values) format.
cef	CEF (Common Event Format) format.
rfc5424	Syslog RFC5424 format.

priority	Set log transmission priority.	option	-	default

Option	Description
default	Set Syslog transmission priority to default.
low	Set Syslog transmission priority to low.

max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable

Option	Description
high-medium	SSL communication with high and medium encryption algorithms.
high	SSL communication with high encryption algorithms.
low	SSL communication with low encryption algorithms.
disable	Disable SSL communication.

ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	Set outgoing interface manually.

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

config custom-field-name

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

config log syslogd2 setting

Global settings for remote syslog server.

```
config log syslogd2 setting
    Description: Global settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
```

```
            set custom {string}
        next
    end
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log syslogd2 setting

Parameter	Description	Type	Size	Default
status	Enable/disable remote syslog logging.	option	-	disable
	Option / **Description** *enable* — Log to remote syslog server. *disable* — Do not log to remote syslog server.			
server	Address of remote syslog server.	string	Maximum length: 127	
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp
	Option / **Description** *udp* — Enable syslogging over UDP. *legacy-reliable* — Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog). *reliable* — Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).			
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7
	Option / **Description** *kernel* — Kernel messages. *user* — Random user-level messages. *mail* — Mail system. *daemon* — System daemons. *auth* — Security/authorization messages. *syslog* — Messages generated internally by syslog.			

Parameter	Description	Type	Size	Default
	Option / **Description** *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.			
source-ip	Source IP address of syslog.	string	Maximum length: 63	
format	Log format.	option	-	default
	Option / **Description** *default* — Syslog format. *csv* — CSV (Comma Separated Values) format. *cef* — CEF (Common Event Format) format. *rfc5424* — Syslog RFC5424 format.			
priority	Set log transmission priority.	option	-	default

Parameter	Description	Type	Size	Default
	Option / **Description** *default* — Set Syslog transmission priority to default. *low* — Set Syslog transmission priority to low.			
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	Option / **Description** *high-medium* — SSL communication with high and medium encryption algorithms. *high* — SSL communication with high encryption algorithms. *low* — SSL communication with low encryption algorithms. *disable* — Disable SSL communication.			
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config custom-field-name

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

config log syslogd3 filter

Filters for remote system server.

```
config log syslogd3 filter
    Description: Filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log syslogd3 filter

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

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.

Parameter	Description	Type	Size	Default
	Option / **Description** *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.			
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable forward traffic logging. *disable* — Disable forward traffic logging.			
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable local in or out traffic logging. *disable* — Disable local in or out traffic logging.			
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable multicast traffic logging. *disable* — Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable sniffer traffic logging. *disable* — Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable ztna traffic logging. *disable* — Disable ztna traffic logging.			

Parameter	Description	Type	Size	Default
http-transaction	Enable/disable log http-transaction messages.	option	-	enable

Option	Description
enable	Enable ztna traffic logging.
disable	Disable ztna traffic logging.

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

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

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

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

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Option	Description
traffic	Traffic log.
event	Event log.
virus	Antivirus log.
webfilter	Web filter log.
attack	Attack log.
spam	Antispam log.
anomaly	Anomaly log.
voip	VoIP log.
dlp	DLP log.
app-ctrl	Application control log.

Parameter	Description	Type	Size	Default
	Option / **Description** *waf* / Web application firewall log. *dns* / DNS detail log. *ssh* / SSH log. *ssl* / SSL log. *file-filter* / File filter log. *icap* / ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option / **Description** *include* / Include logs that match the filter. *exclude* / Exclude logs that match the filter.			

config log syslogd3 override-filter

Override filters for remote system server.

```
config log syslogd3 override-filter
    Description: Override filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log syslogd3 override-filter

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

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

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

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size	Default
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

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

Option	Description
enable	Enable multicast traffic logging.
disable	Disable multicast traffic logging.

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

Option	Description
enable	Enable sniffer traffic logging.
disable	Disable sniffer traffic logging.

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

Option	Description
enable	Enable ztna traffic logging.
disable	Disable ztna traffic logging.

Parameter	Description	Type	Size	Default
http-transaction	Enable/disable log http-transaction messages.	option	-	enable

Option	Description
enable	Enable ztna traffic logging.
disable	Disable ztna traffic logging.

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

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

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

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

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Option	Description
traffic	Traffic log.
event	Event log.
virus	Antivirus log.
webfilter	Web filter log.
attack	Attack log.
spam	Antispam log.

Parameter	Description	Type	Size	Default
	Option / **Description** *anomaly* — Anomaly log. *voip* — VoIP log. *dlp* — DLP log. *app-ctrl* — Application control log. *waf* — Web application firewall log. *dns* — DNS detail log. *ssh* — SSH log. *ssl* — SSL log. *file-filter* — File filter log. *icap* — ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option / **Description** *include* — Include logs that match the filter. *exclude* — Exclude logs that match the filter.			

config log syslogd3 override-setting

Override settings for remote syslog server.

```
config log syslogd3 override-setting
    Description: Override settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
```

```
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log syslogd3 override-setting

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

Option	Description
enable	Log to remote syslog server.
disable	Do not log to remote syslog server.

server	Address of remote syslog server.	string	Maximum length: 127	
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp

Option	Description
udp	Enable syslogging over UDP.
legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).

port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7

Option	Description
kernel	Kernel messages.
user	Random user-level messages.
mail	Mail system.
daemon	System daemons.
auth	Security/authorization messages.

Parameter	Description	Type	Size	Default
	Option / **Description** *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.			
source-ip	Source IP address of syslog.	string	Maximum length: 63	
format	Log format.	option	-	default
	Option / **Description** *default* — Syslog format. *csv* — CSV (Comma Separated Values) format. *cef* — CEF (Common Event Format) format. *rfc5424* — Syslog RFC5424 format.			
priority	Set log transmission priority.	option	-	default

Parameter	Description	Type	Size	Default
	Option / **Description** *default* — Set Syslog transmission priority to default. *low* — Set Syslog transmission priority to low.			
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	Option / **Description** *high-medium* — SSL communication with high and medium encryption algorithms. *high* — SSL communication with high encryption algorithms. *low* — SSL communication with low encryption algorithms. *disable* — Disable SSL communication.			
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config custom-field-name

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

config log syslogd3 setting

Global settings for remote syslog server.

```
config log syslogd3 setting
    Description: Global settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log syslogd3 setting

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

Option	Description
enable	Log to remote syslog server.
disable	Do not log to remote syslog server.

Parameter	Description	Type	Size	Default
server	Address of remote syslog server.	string	Maximum length: 127	
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp

Option	Description
udp	Enable syslogging over UDP.
legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).

Parameter	Description	Type	Size	Default
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7

Option	Description
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.

Parameter	Description	Type	Size	Default
	Option / **Description** *local0* / Reserved for local use. *local1* / Reserved for local use. *local2* / Reserved for local use. *local3* / Reserved for local use. *local4* / Reserved for local use. *local5* / Reserved for local use. *local6* / Reserved for local use. *local7* / Reserved for local use.			
source-ip	Source IP address of syslog.	string	Maximum length: 63	
format	Log format.	option	-	default
	Option / **Description** *default* / Syslog format. *csv* / CSV (Comma Separated Values) format. *cef* / CEF (Common Event Format) format. *rfc5424* / Syslog RFC5424 format.			
priority	Set log transmission priority.	option	-	default
	Option / **Description** *default* / Set Syslog transmission priority to default. *low* / Set Syslog transmission priority to low.			
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	Option / **Description** *high-medium* / SSL communication with high and medium encryption algorithms. *high* / SSL communication with high encryption algorithms.			

Parameter	Description	Type	Size	Default
	Option / **Description** *low* — SSL communication with low encryption algorithms. *disable* — Disable SSL communication.			
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config custom-field-name

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

config log syslogd4 filter

Filters for remote system server.

```
config log syslogd4 filter
    Description: Filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log syslogd4 filter

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

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

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

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size	Default
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable local in or out traffic logging. *disable* — Disable local in or out traffic logging.			
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable multicast traffic logging. *disable* — Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable sniffer traffic logging. *disable* — Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable ztna traffic logging. *disable* — Disable ztna traffic logging.			
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option / **Description** *enable* — Enable ztna traffic logging. *disable* — Disable ztna traffic logging.			
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option / **Description** *enable* — Enable anomaly logging. *disable* — Disable anomaly logging.			
voip	Enable/disable VoIP logging.	option	-	enable
	Option / **Description** *enable* — Enable VoIP logging. *disable* — Disable VoIP logging.			

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Option	Description
traffic	Traffic log.
event	Event log.
virus	Antivirus log.
webfilter	Web filter log.
attack	Attack log.
spam	Antispam log.
anomaly	Anomaly log.
voip	VoIP log.
dlp	DLP log.
app-ctrl	Application control log.
waf	Web application firewall log.
dns	DNS detail log.
ssh	SSH log.
ssl	SSL log.
file-filter	File filter log.
icap	ICAP log.

filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Option	Description
include	Include logs that match the filter.
exclude	Exclude logs that match the filter.

config log syslogd4 override-filter

Override filters for remote system server.

```
config log syslogd4 override-filter
    Description: Override filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log syslogd4 override-filter

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

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

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

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size	Default
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable local in or out traffic logging. *disable* — Disable local in or out traffic logging.			
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable multicast traffic logging. *disable* — Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable sniffer traffic logging. *disable* — Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable ztna traffic logging. *disable* — Disable ztna traffic logging.			
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option / **Description** *enable* — Enable ztna traffic logging. *disable* — Disable ztna traffic logging.			
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option / **Description** *enable* — Enable anomaly logging. *disable* — Disable anomaly logging.			
voip	Enable/disable VoIP logging.	option	-	enable
	Option / **Description** *enable* — Enable VoIP logging. *disable* — Disable VoIP logging.			

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Option	Description
traffic	Traffic log.
event	Event log.
virus	Antivirus log.
webfilter	Web filter log.
attack	Attack log.
spam	Antispam log.
anomaly	Anomaly log.
voip	VoIP log.
dlp	DLP log.
app-ctrl	Application control log.
waf	Web application firewall log.
dns	DNS detail log.
ssh	SSH log.
ssl	SSL log.
file-filter	File filter log.
icap	ICAP log.

filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Option	Description
include	Include logs that match the filter.
exclude	Exclude logs that match the filter.

config log syslogd4 override-setting

Override settings for remote syslog server.

```
config log syslogd4 override-setting
    Description: Override settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log syslogd4 override-setting

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

Parameter	Description	Type	Size	Default
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7

Option	Description
kernel	Kernel messages.
user	Random user-level messages.
mail	Mail system.
daemon	System daemons.
auth	Security/authorization messages.
syslog	Messages generated internally by syslog.
lpr	Line printer subsystem.
news	Network news subsystem.
uucp	Network news subsystem.
cron	Clock daemon.
authpriv	Security/authorization messages (private).
ftp	FTP daemon.
ntp	NTP daemon.
audit	Log audit.
alert	Log alert.
clock	Clock daemon.
local0	Reserved for local use.
local1	Reserved for local use.
local2	Reserved for local use.
local3	Reserved for local use.
local4	Reserved for local use.
local5	Reserved for local use.
local6	Reserved for local use.
local7	Reserved for local use.

Parameter	Description	Type	Size	Default
source-ip	Source IP address of syslog.	string	Maximum length: 63	
format	Log format.	option	-	default

Option	Description
default	Syslog format.
csv	CSV (Comma Separated Values) format.
cef	CEF (Common Event Format) format.
rfc5424	Syslog RFC5424 format.

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

Option	Description
default	Set Syslog transmission priority to default.
low	Set Syslog transmission priority to low.

Parameter	Description	Type	Size	Default
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable

Option	Description
high-medium	SSL communication with high and medium encryption algorithms.
high	SSL communication with high encryption algorithms.
low	SSL communication with low encryption algorithms.
disable	Disable SSL communication.

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

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	Set outgoing interface manually.

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

config custom-field-name

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

config log syslogd4 setting

Global settings for remote syslog server.

```
config log syslogd4 setting
    Description: Global settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
```

```
            set custom {string}
        next
    end
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log syslogd4 setting

Parameter	Description	Type	Size	Default
status	Enable/disable remote syslog logging.	option	-	disable
	Option / **Description** *enable* — Log to remote syslog server. *disable* — Do not log to remote syslog server.			
server	Address of remote syslog server.	string	Maximum length: 127	
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp
	Option / **Description** *udp* — Enable syslogging over UDP. *legacy-reliable* — Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog). *reliable* — Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).			
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7
	Option / **Description** *kernel* — Kernel messages. *user* — Random user-level messages. *mail* — Mail system. *daemon* — System daemons. *auth* — Security/authorization messages. *syslog* — Messages generated internally by syslog.			

Parameter	Description	Type	Size	Default
	Option / **Description** *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.			
source-ip	Source IP address of syslog.	string	Maximum length: 63	
format	Log format.	option	-	default
	Option / **Description** *default* — Syslog format. *csv* — CSV (Comma Separated Values) format. *cef* — CEF (Common Event Format) format. *rfc5424* — Syslog RFC5424 format.			
priority	Set log transmission priority.	option	-	default

Parameter	Description	Type	Size	Default
	Option / **Description** *default* — Set Syslog transmission priority to default. *low* — Set Syslog transmission priority to low.			
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	Option / **Description** *high-medium* — SSL communication with high and medium encryption algorithms. *high* — SSL communication with high encryption algorithms. *low* — SSL communication with low encryption algorithms. *disable* — Disable SSL communication.			
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config custom-field-name

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

config log syslogd filter

Filters for remote system server.

```
config log syslogd filter
    Description: Filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log syslogd filter

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

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.

Parameter	Description	Type	Size	Default
	Option / **Description** *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.			
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable forward traffic logging. *disable* — Disable forward traffic logging.			
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable local in or out traffic logging. *disable* — Disable local in or out traffic logging.			
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable multicast traffic logging. *disable* — Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable sniffer traffic logging. *disable* — Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable ztna traffic logging. *disable* — Disable ztna traffic logging.			

Parameter	Description	Type	Size	Default
http-transaction	Enable/disable log http-transaction messages.	option	-	enable

Option	Description
enable	Enable ztna traffic logging.
disable	Disable ztna traffic logging.

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

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

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

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

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Option	Description
traffic	Traffic log.
event	Event log.
virus	Antivirus log.
webfilter	Web filter log.
attack	Attack log.
spam	Antispam log.
anomaly	Anomaly log.
voip	VoIP log.
dlp	DLP log.
app-ctrl	Application control log.

Parameter	Description	Type	Size	Default
	Option / **Description** *waf* / Web application firewall log. *dns* / DNS detail log. *ssh* / SSH log. *ssl* / SSL log. *file-filter* / File filter log. *icap* / ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option / **Description** *include* / Include logs that match the filter. *exclude* / Exclude logs that match the filter.			

config log syslogd override-filter

Override filters for remote system server.

```
config log syslogd override-filter
    Description: Override filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log syslogd override-filter

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

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

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

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size	Default
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

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

Option	Description
enable	Enable multicast traffic logging.
disable	Disable multicast traffic logging.

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

Option	Description
enable	Enable sniffer traffic logging.
disable	Disable sniffer traffic logging.

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

Option	Description
enable	Enable ztna traffic logging.
disable	Disable ztna traffic logging.

Parameter	Description	Type	Size	Default
http-transaction	Enable/disable log http-transaction messages.	option	-	enable

Option	Description
enable	Enable ztna traffic logging.
disable	Disable ztna traffic logging.

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

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

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

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

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Option	Description
traffic	Traffic log.
event	Event log.
virus	Antivirus log.
webfilter	Web filter log.
attack	Attack log.
spam	Antispam log.

Parameter	Description	Type	Size	Default
	Option / **Description** *anomaly* — Anomaly log. *voip* — VoIP log. *dlp* — DLP log. *app-ctrl* — Application control log. *waf* — Web application firewall log. *dns* — DNS detail log. *ssh* — SSH log. *ssl* — SSL log. *file-filter* — File filter log. *icap* — ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option / **Description** *include* — Include logs that match the filter. *exclude* — Exclude logs that match the filter.			

config log syslogd override-setting

Override settings for remote syslog server.

```
config log syslogd override-setting
    Description: Override settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
```

```
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log syslogd override-setting

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

Option	Description
enable	Log to remote syslog server.
disable	Do not log to remote syslog server.

Parameter	Description	Type	Size	Default
server	Address of remote syslog server.	string	Maximum length: 127	
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp

Option	Description
udp	Enable syslogging over UDP.
legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).

Parameter	Description	Type	Size	Default
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7

Option	Description
kernel	Kernel messages.
user	Random user-level messages.
mail	Mail system.
daemon	System daemons.
auth	Security/authorization messages.

Parameter	Description	Type	Size	Default
	Option / **Description** *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.			
source-ip	Source IP address of syslog.	string	Maximum length: 63	
format	Log format.	option	-	default
	Option / **Description** *default* — Syslog format. *csv* — CSV (Comma Separated Values) format. *cef* — CEF (Common Event Format) format. *rfc5424* — Syslog RFC5424 format.			
priority	Set log transmission priority.	option	-	default

Parameter	Description	Type	Size	Default
	Option / **Description** *default* — Set Syslog transmission priority to default. *low* — Set Syslog transmission priority to low.			
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	Option / **Description** *high-medium* — SSL communication with high and medium encryption algorithms. *high* — SSL communication with high encryption algorithms. *low* — SSL communication with low encryption algorithms. *disable* — Disable SSL communication.			
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config custom-field-name

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

config log syslogd setting

Global settings for remote syslog server.

```
config log syslogd setting
    Description: Global settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config log syslogd setting

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

Option	Description
enable	Log to remote syslog server.
disable	Do not log to remote syslog server.

Parameter	Description	Type	Size	Default
server	Address of remote syslog server.	string	Maximum length: 127	
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp

Option	Description
udp	Enable syslogging over UDP.
legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).

Parameter	Description	Type	Size	Default
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7

Option	Description
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.

Parameter	Description	Type	Size	Default
	Option / **Description** *local0* / Reserved for local use. *local1* / Reserved for local use. *local2* / Reserved for local use. *local3* / Reserved for local use. *local4* / Reserved for local use. *local5* / Reserved for local use. *local6* / Reserved for local use. *local7* / Reserved for local use.			
source-ip	Source IP address of syslog.	string	Maximum length: 63	
format	Log format.	option	-	default
	Option / **Description** *default* / Syslog format. *csv* / CSV (Comma Separated Values) format. *cef* / CEF (Common Event Format) format. *rfc5424* / Syslog RFC5424 format.			
priority	Set log transmission priority.	option	-	default
	Option / **Description** *default* / Set Syslog transmission priority to default. *low* / Set Syslog transmission priority to low.			
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	Option / **Description** *high-medium* / SSL communication with high and medium encryption algorithms. *high* / SSL communication with high encryption algorithms.			

Parameter	Description	Type	Size	Default
	Option / **Description** *low* — SSL communication with low encryption algorithms. *disable* — Disable SSL communication.			
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections . **Option** / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.	option	-	default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server. **Option** / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.	option	-	auto
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config custom-field-name

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

config log tacacs+accounting2 filter

Settings for TACACS+ accounting events filter.

```
config log tacacs+accounting2 filter
    Description: Settings for TACACS+ accounting events filter.
    set login-audit [enable|disable]
    set config-change-audit [enable|disable]
    set cli-cmd-audit [enable|disable]
end
```

config log tacacs+accounting2 filter

Parameter	Description	Type	Size	Default
login-audit	Enable/disable TACACS+ accounting for login events audit.	option	-	enable

Option	Description
enable	Enable TACACS+ accounting for login events audit.
disable	Disable TACACS+ accounting for login events audit.

Parameter	Description	Type	Size	Default
config-change-audit	Enable/disable TACACS+ accounting for configuration change events audit.	option	-	enable

Option	Description
enable	Enable TACACS+ accounting for configuration change events audit.
disable	Disable TACACS+ accounting for configuration change events audit.

Parameter	Description	Type	Size	Default
cli-cmd-audit	Enable/disable TACACS+ accounting for CLI commands audit.	option	-	enable

Option	Description
enable	Enable TACACS+ accounting for CLI commands audit.
disable	Disable TACACS+ accounting for CLI commands audit.

config log tacacs+accounting2 setting

Settings for TACACS+ accounting.

```
config log tacacs+accounting2 setting
    Description: Settings for TACACS+ accounting.
    set status [enable|disable]
    set server {string}
    set server-key {password}
end
```

config log tacacs+accounting2 setting

Parameter	Description	Type	Size	Default
status	Enable/disable TACACS+ accounting.	option	-	disable
	Option / **Description** *enable* — Enable TACACS+ accounting. *disable* — Disable TACACS+ accounting.			
server	Address of TACACS+ server.	string	Maximum length: 63	
server-key	Key to access the TACACS+ server.	password	Not Specified	

config log tacacs+accounting3 filter

Settings for TACACS+ accounting events filter.

```
config log tacacs+accounting3 filter
    Description: Settings for TACACS+ accounting events filter.
    set login-audit [enable|disable]
    set config-change-audit [enable|disable]
    set cli-cmd-audit [enable|disable]
end
```

config log tacacs+accounting3 filter

Parameter	Description	Type	Size	Default
login-audit	Enable/disable TACACS+ accounting for login events audit.	option	-	enable
	Option / **Description** *enable* — Enable TACACS+ accounting for login events audit. *disable* — Disable TACACS+ accounting for login events audit.			
config-change-audit	Enable/disable TACACS+ accounting for configuration change events audit.	option	-	enable
	Option / **Description** *enable* — Enable TACACS+ accounting for configuration change events audit. *disable* — Disable TACACS+ accounting for configuration change events audit.			

Parameter	Description	Type	Size	Default
cli-cmd-audit	Enable/disable TACACS+ accounting for CLI commands audit.	option	-	enable

Option	Description
enable	Enable TACACS+ accounting for CLI commands audit.
disable	Disable TACACS+ accounting for CLI commands audit.

config log tacacs+accounting3 setting

Settings for TACACS+ accounting.

```
config log tacacs+accounting3 setting
    Description: Settings for TACACS+ accounting.
    set status [enable|disable]
    set server {string}
    set server-key {password}
end
```

config log tacacs+accounting3 setting

Parameter	Description	Type	Size	Default
status	Enable/disable TACACS+ accounting.	option	-	disable

Option	Description
enable	Enable TACACS+ accounting.
disable	Disable TACACS+ accounting.

server	Address of TACACS+ server.	string	Maximum length: 63	
server-key	Key to access the TACACS+ server.	password	Not Specified	

config log tacacs+accounting filter

Settings for TACACS+ accounting events filter.

```
config log tacacs+accounting filter
    Description: Settings for TACACS+ accounting events filter.
    set login-audit [enable|disable]
    set config-change-audit [enable|disable]
```

```
    set cli-cmd-audit [enable|disable]
end
```

config log tacacs+accounting filter

Parameter	Description	Type	Size	Default
login-audit	Enable/disable TACACS+ accounting for login events audit.	option	-	enable

Option	Description
enable	Enable TACACS+ accounting for login events audit.
disable	Disable TACACS+ accounting for login events audit.

Parameter	Description	Type	Size	Default
config-change-audit	Enable/disable TACACS+ accounting for configuration change events audit.	option	-	enable

Option	Description
enable	Enable TACACS+ accounting for configuration change events audit.
disable	Disable TACACS+ accounting for configuration change events audit.

Parameter	Description	Type	Size	Default
cli-cmd-audit	Enable/disable TACACS+ accounting for CLI commands audit.	option	-	enable

Option	Description
enable	Enable TACACS+ accounting for CLI commands audit.
disable	Disable TACACS+ accounting for CLI commands audit.

config log tacacs+accounting setting

Settings for TACACS+ accounting.

```
config log tacacs+accounting setting
    Description: Settings for TACACS+ accounting.
    set status [enable|disable]
    set server {string}
    set server-key {password}
end
```

config log tacacs+accounting setting

Parameter	Description	Type	Size	Default
status	Enable/disable TACACS+ accounting.	option	-	disable
	Option / **Description** *enable* — Enable TACACS+ accounting. *disable* — Disable TACACS+ accounting.			
server	Address of TACACS+ server.	string	Maximum length: 63	
server-key	Key to access the TACACS+ server.	password	Not Specified	

config log threat-weight

Configure threat weight settings.

```
config log threat-weight
    Description: Configure threat weight settings.
    set status [enable|disable]
    config level
        Description: Score mapping for threat weight levels.
        set low {integer}
        set medium {integer}
        set high {integer}
        set critical {integer}
    end
    set blocked-connection [disable|low|...]
    set failed-connection [disable|low|...]
    set url-block-detected [disable|low|...]
    set botnet-connection-detected [disable|low|...]
    config malware
        Description: Anti-virus malware threat weight settings.
        set virus-infected [disable|low|...]
        set fortindr [disable|low|...]
        set file-blocked [disable|low|...]
        set command-blocked [disable|low|...]
        set oversized [disable|low|...]
        set virus-scan-error [disable|low|...]
        set switch-proto [disable|low|...]
        set mimefragmented [disable|low|...]
        set virus-file-type-executable [disable|low|...]
        set virus-outbreak-prevention [disable|low|...]
        set content-disarm [disable|low|...]
        set malware-list [disable|low|...]
        set ems-threat-feed [disable|low|...]
        set fsa-malicious [disable|low|...]
```

```
        set fsa-high-risk [disable|low|...]
        set fsa-medium-risk [disable|low|...]
    end
    config ips
        Description: IPS threat weight settings.
        set info-severity [disable|low|...]
        set low-severity [disable|low|...]
        set medium-severity [disable|low|...]
        set high-severity [disable|low|...]
        set critical-severity [disable|low|...]
    end
    config web
        Description: Web filtering threat weight settings.
        edit <id>
            set category {integer}
            set level [disable|low|...]
        next
    end
    config geolocation
        Description: Geolocation-based threat weight settings.
        edit <id>
            set country {string}
            set level [disable|low|...]
        next
    end
    config application
        Description: Application-control threat weight settings.
        edit <id>
            set category {integer}
            set level [disable|low|...]
        next
    end
end
```

config log threat-weight

Parameter	Description	Type	Size	Default
status	Enable/disable the threat weight feature.	option	-	enable

Option	Description
enable	Enable the threat weight feature.
disable	Disable the threat weight feature.

Parameter	Description	Type	Size	Default
blocked-connection	Threat weight score for blocked connections.	option	-	high

Option	Description
disable	Disable threat weight scoring for blocked connections.

Parameter	Description	Type	Size	Default
	Option / **Description** *low* — Use the low level score for blocked connections. *medium* — Use the medium level score for blocked connections. *high* — Use the high level score for blocked connections. *critical* — Use the critical level score for blocked connections.			
failed-connection	Threat weight score for failed connections.	option	-	low
	Option / **Description** *disable* — Disable threat weight scoring for failed connections. *low* — Use the low level score for failed connections. *medium* — Use the medium level score for failed connections. *high* — Use the high level score for failed connections. *critical* — Use the critical level score for failed connections.			
url-block-detected	Threat weight score for URL blocking.	option	-	high
	Option / **Description** *disable* — Disable threat weight scoring for URL blocking. *low* — Use the low level score for URL blocking. *medium* — Use the medium level score for URL blocking. *high* — Use the high level score for URL blocking. *critical* — Use the critical level score for URL blocking.			
botnet-connection-detected	Threat weight score for detected botnet connections.	option	-	critical
	Option / **Description** *disable* — Disable threat weight scoring for detected botnet connections. *low* — Use the low level score for detected botnet connections. *medium* — Use the medium level score for detected botnet connections. *high* — Use the high level score for detected botnet connections. *critical* — Use the critical level score for detected botnet connections.			

config level

Parameter	Description	Type	Size	Default
low	Low level score value .	integer	Minimum value: 1 Maximum value: 100	5
medium	Medium level score value .	integer	Minimum value: 1 Maximum value: 100	10
high	High level score value .	integer	Minimum value: 1 Maximum value: 100	30
critical	Critical level score value .	integer	Minimum value: 1 Maximum value: 100	50

config malware

Parameter	Description	Type	Size	Default
virus-infected	Threat weight score for virus (infected) detected.	option	-	critical

Option	Description
disable	Disable threat weight scoring for virus (infected) detected.
low	Use the low level score for virus (infected) detected.
medium	Use the medium level score for virus (infected) detected.
high	Use the high level score for virus (infected) detected.
critical	Use the critical level score for virus (infected) detected.

Parameter	Description	Type	Size	Default
fortindr	Threat weight score for FortiNDR-detected virus.	option	-	critical

Option	Description
disable	Disable threat weight scoring for virus detected by FortiNDR.
low	Use the low level score for virus detected by FortiNDR.
medium	Use the medium level score for virus detected by FortiNDR.
high	Use the high level score for virus detected by FortiNDR.

Parameter	Description	Type	Size	Default
	Option / **Description** *critical* — Use the critical level score for virus detected by FortiNDR.			
file-blocked	Threat weight score for blocked file detected.	option	-	low
	Option / **Description** *disable* — Disable threat weight scoring for blocked file detected. *low* — Use the low level score for blocked file detected. *medium* — Use the medium level score for blocked file detected. *high* — Use the high level score for blocked file detected. *critical* — Use the critical level score for blocked file detected.			
command-blocked	Threat weight score for blocked command detected.	option	-	disable
	Option / **Description** *disable* — Disable threat weight scoring for blocked command detected. *low* — Use the low level score for blocked command detected. *medium* — Use the medium level score for blocked command detected. *high* — Use the high level score for blocked command detected. *critical* — Use the critical level score for blocked command detected.			
oversized	Threat weight score for oversized file detected.	option	-	disable
	Option / **Description** *disable* — Disable threat weight scoring for oversized file detected. *low* — Use the low level score for oversized file detected. *medium* — Use the medium level score for oversized file detected. *high* — Use the high level score for oversized file detected. *critical* — Use the critical level score for oversized file detected.			
virus-scan-error	Threat weight score for virus (scan error) detected.	option	-	high
	Option / **Description** *disable* — Disable threat weight scoring for virus (scan error) detected. *low* — Use the low level score for virus (scan error) detected. *medium* — Use the medium level score for virus (scan error) detected.			

Parameter	Description	Type	Size	Default
	Option / **Description** *high* — Use the high level score for virus (scan error) detected. *critical* — Use the critical level score for virus (scan error) detected.			
switch-proto	Threat weight score for switch proto detected.	option	-	disable
	Option / **Description** *disable* — Disable threat weight scoring for switch proto detected. *low* — Use the low level score for switch proto detected. *medium* — Use the medium level score for switch proto detected. *high* — Use the high level score for switch proto detected. *critical* — Use the critical level score for switch proto detected.			
mimefragmented	Threat weight score for mimefragmented detected.	option	-	disable
	Option / **Description** *disable* — Disable threat weight scoring for mimefragmented detected. *low* — Use the low level score for mimefragmented detected. *medium* — Use the medium level score for mimefragmented detected. *high* — Use the high level score for mimefragmented detected. *critical* — Use the critical level score for mimefragmented detected.			
virus-file-type-executable	Threat weight score for virus (file type executable) detected.	option	-	medium
	Option / **Description** *disable* — Disable threat weight scoring for virus (filetype executable) detected. *low* — Use the low level score for virus (filetype executable) detected. *medium* — Use the medium level score for virus (filetype executable) detected. *high* — Use the high level score for virus (filetype executable) detected. *critical* — Use the critical level score for virus (filetype executable) detected.			
virus-outbreak-prevention	Threat weight score for virus (outbreak prevention) event.	option	-	critical

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Disable threat weight scoring for virus (outbreak prevention) event. *low* — Use the low level score for virus (outbreak prevention) event. *medium* — Use the medium level score for virus (outbreak prevention) event. *high* — Use the high level score for virus (outbreak prevention) event. *critical* — Use the critical level score for virus (outbreak prevention) event.			
content-disarm	Threat weight score for virus (content disarm) detected.	option	-	medium
	Option / **Description** *disable* — Disable threat weight scoring for virus (content disarm) detected. *low* — Use the low level score for virus (content disarm) detected. *medium* — Use the medium level score for virus (content disarm) detected. *high* — Use the high level score for virus (content disarm) detected. *critical* — Use the critical level score for virus (content disarm) detected.			
malware-list	Threat weight score for virus (malware list) detected.	option	-	medium
	Option / **Description** *disable* — Disable threat weight scoring for virus (malware list) detected. *low* — Use the low level score for virus (malware list) detected. *medium* — Use the medium level score for virus (malware list) detected. *high* — Use the high level score for virus (malware list) detected. *critical* — Use the critical level score for virus (malware list) detected.			
ems-threat-feed	Threat weight score for virus (EMS threat feed) detected.	option	-	medium
	Option / **Description** *disable* — Disable threat weight scoring for virus (EMS threat feed) detected. *low* — Use the low level score for virus (EMS threat feed) detected. *medium* — Use the medium level score for virus (EMS threat feed) detected. *high* — Use the high level score for virus (EMS threat feed) detected. *critical* — Use the critical level score for virus (EMS threat feed) detected.			

Parameter	Description	Type	Size	Default
fsa-malicious	Threat weight score for FortiSandbox malicious malware detected.	option	-	critical

Option	Description
disable	Disable threat weight scoring for FortiSandbox malicious malware detected.
low	Use the low level score for FortiSandbox malicious malware detected.
medium	Use the medium level score for FortiSandbox malicious malware detected.
high	Use the high level score for FortiSandbox malicious malware detected.
critical	Use the critical level score for FortiSandbox malicious malware detected.

fsa-high-risk	Threat weight score for FortiSandbox high risk malware detected.	option	-	high

Option	Description
disable	Disable threat weight scoring for FortiSandbox high risk malware detected.
low	Use the low level score for FortiSandbox high risk malware detected.
medium	Use the medium level score for FortiSandbox high risk malware detected.
high	Use the high level score for FortiSandbox high risk malware detected.
critical	Use the critical level score for FortiSandbox high risk malware detected.

fsa-medium-risk	Threat weight score for FortiSandbox medium risk malware detected.	option	-	medium

Option	Description
disable	Disable threat weight scoring for FortiSandbox medium risk malware detected.
low	Use the low level score for FortiSandbox medium risk malware detected.
medium	Use the medium level score for FortiSandbox medium risk malware detected.
high	Use the high level score for FortiSandbox medium risk malware detected.
critical	Use the critical level score for FortiSandbox medium risk malware detected.

config ips

Parameter	Description	Type	Size	Default
info-severity	Threat weight score for IPS info severity events.	option	-	disable

Option	Description
disable	Disable threat weight scoring for IPS info severity events.
low	Use the low level score for IPS info severity events.
medium	Use the medium level score for IPS info severity events.
high	Use the high level score for IPS info severity events.
critical	Use the critical level score for IPS info severity events.

Parameter	Description	Type	Size	Default
low-severity	Threat weight score for IPS low severity events.	option	-	low

Option	Description
disable	Disable threat weight scoring for IPS low severity events.
low	Use the low level score for IPS low severity events.
medium	Use the medium level score for IPS low severity events.
high	Use the high level score for IPS low severity events.
critical	Use the critical level score for IPS low severity events.

Parameter	Description	Type	Size	Default
medium-severity	Threat weight score for IPS medium severity events.	option	-	medium

Option	Description
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.

Parameter	Description	Type	Size	Default
high-severity	Threat weight score for IPS high severity events.	option	-	high

Option	Description
disable	Disable threat weight scoring for IPS high severity events.
low	Use the low level score for IPS high severity events.
medium	Use the medium level score for IPS high severity events.

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

config web

Parameter	Description	Type	Size	Default
category	Threat weight score for web category filtering matches.	integer	Minimum value: 0 Maximum value: 255	0
level	Threat weight score for web category filtering matches.	option	-	low
	Option / **Description** *disable* — Disable threat weight scoring for web category filtering matches. *low* — Use the low level score for web category filtering matches. *medium* — Use the medium level score for web category filtering matches. *high* — Use the high level score for web category filtering matches. *critical* — Use the critical level score for web category filtering matches.			

config geolocation

Parameter	Description	Type	Size	Default
country	Country code.	string	Maximum length: 2	

Parameter	Description	Type	Size	Default
level	Threat weight score for Geolocation-based events.	option	-	low

Option	Description
disable	Disable threat weight scoring for Geolocation-based events.
low	Use the low level score for Geolocation-based events.
medium	Use the medium level score for Geolocation-based events.
high	Use the high level score for Geolocation-based events.
critical	Use the critical level score for Geolocation-based events.

config application

Parameter	Description	Type	Size	Default
category	Application category.	integer	Minimum value: 0 Maximum value: 65535	0
level	Threat weight score for Application events.	option	-	low

Option	Description
disable	Disable threat weight scoring for Application events.
low	Use the low level score for Application events.
medium	Use the medium level score for Application events.
high	Use the high level score for Application events.
critical	Use the critical level score for Application events.

config log webtrends filter

Filters for WebTrends.

```
config log webtrends filter
    Description: Filters for WebTrends.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
```

```
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log webtrends filter

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

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

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

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size	Default
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

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

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.			
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.			
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option **Description** *enable* Enable ztna traffic logging. *disable* Disable ztna traffic logging.			
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option **Description** *enable* Enable anomaly logging. *disable* Disable anomaly logging.			
voip	Enable/disable VoIP logging.	option	-	enable
	Option **Description** *enable* Enable VoIP logging. *disable* Disable VoIP logging.			

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Parameter	Description	Type	Size	Default
	Option / **Description** *traffic* — Traffic log. *event* — Event log. *virus* — Antivirus log. *webfilter* — Web filter log. *attack* — Attack log. *spam* — Antispam log. *anomaly* — Anomaly log. *voip* — VoIP log. *dlp* — DLP log. *app-ctrl* — Application control log. *waf* — Web application firewall log. *dns* — DNS detail log. *ssh* — SSH log. *ssl* — SSL log. *file-filter* — File filter log. *icap* — ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option / **Description** *include* — Include logs that match the filter. *exclude* — Exclude logs that match the filter.			

config log webtrends setting

Settings for WebTrends.

```
config log webtrends setting
    Description: Settings for WebTrends.
    set status [enable|disable]
    set server {string}
end
```

config log webtrends setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to WebTrends.	option	-	disable
	Option / **Description** *enable* — Enable logging to WebTrends. *disable* — Disble logging to WebTrends.			
server	Address of the remote WebTrends server.	string	Maximum length: 63	

mgmt-data

This section includes syntax for the following commands:

config mgmt-data status

Status for mgmt-data.

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

report

This section includes syntax for the following commands:

config report layout

Report layout configuration.

```
config report layout
    Description: Report layout configuration.
    edit <name>
        set title {string}
        set subtitle {string}
        set description {string}
        set style-theme {string}
        set options {option1}, {option2}, ...
        set format {option1}, {option2}, ...
        set schedule-type [demand|daily|...]
        set day [sunday|monday|...]
        set time {user}
        set cutoff-option [run-time|custom]
        set cutoff-time {user}
        set email-send [enable|disable]
        set email-recipients {string}
        set max-pdf-report {integer}
        config page
            Description: Configure report page.
            set paper [a4|letter]
            set column-break-before {option1}, {option2}, ...
            set page-break-before {option1}, {option2}, ...
            set options {option1}, {option2}, ...
            config header
                Description: Configure report page header.
                set style {string}
                config header-item
                    Description: Configure report header item.
                    edit <id>
                        set description {string}
                        set type [text|image]
                        set style {string}
                        set content {string}
                        set img-src {string}
                    next
                end
            end
```

```
            config footer
                Description: Configure report page footer.
                set style {string}
                config footer-item
                    Description: Configure report footer item.
                    edit <id>
                        set description {string}
                        set type [text|image]
                        set style {string}
                        set content {string}
                        set img-src {string}
                    next
                end
            end
        end
        config body-item
            Description: Configure report body item.
            edit <id>
                set description {string}
                set type [text|image|...]
                set style {string}
                set top-n {integer}
                config parameters
                    Description: Parameters.
                    edit <id>
                        set name {string}
                        set value {string}
                    next
                end
                set text-component [text|heading1|...]
                set content {string}
                set img-src {string}
                set chart {string}
                set chart-options {option1}, {option2}, ...
                set misc-component [hline|page-break|...]
                set title {string}
            next
        end
    next
end
```

config report layout

Parameter	Description	Type	Size	Default
title	Report title.	string	Maximum length: 127	
subtitle	Report subtitle.	string	Maximum length: 127	
description	Description.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default
style-theme	Report style theme.	string	Maximum length: 35	
options	Report layout options.	option	-	include-table-of-content auto-numbering-heading view-chart-as-heading

Option	Description
include-table-of-content	Include table of content in the report.
auto-numbering-heading	Prepend heading with auto numbering.
view-chart-as-heading	Auto add heading for each chart.
show-html-navbar-before-heading	Show HTML navigation bar before each heading.
dummy-option	Use this option if you need none of the above options.

Parameter	Description	Type	Size	Default
format	Report format.	option	-	pdf

Option	Description
pdf	PDF.

Parameter	Description	Type	Size	Default
schedule-type	Report schedule type.	option	-	daily

Option	Description
demand	Run on demand.
daily	Schedule daily.
weekly	Schedule weekly.

Parameter	Description	Type	Size	Default
day	Schedule days of week to generate report.	option	-	sunday

Option	Description
sunday	Sunday.
monday	Monday.

Parameter	Description	Type	Size	Default
	Option / **Description** *tuesday* — Tuesday. *wednesday* — Wednesday. *thursday* — Thursday. *friday* — Friday. *saturday* — Saturday.			
time	Schedule time to generate report (format = hh:mm).	user	Not Specified	
cutoff-option	Cutoff-option is either run-time or custom.	option	-	run-time
	Option / **Description** *run-time* — Run time. *custom* — Custom.			
cutoff-time	Custom cutoff time to generate report (format = hh:mm).	user	Not Specified	
email-send	Enable/disable sending emails after reports are generated.	option	-	disable
	Option / **Description** *enable* — Enable sending emails after generating reports. *disable* — Disable sending emails after generating reports.			
email-recipients	Email recipients for generated reports.	string	Maximum length: 511	
max-pdf-report	Maximum number of PDF reports to keep at one time (oldest report is overwritten).	integer	Minimum value: 1 Maximum value: 365	31

config page

Parameter	Description	Type	Size	Default
paper	Report page paper.	option	-	a4
	Option / **Description** *a4* — A4 paper.			

Parameter	Description	Type	Size	Default
	Option **Description** *letter* Letter paper.			
column-break-before	Report page auto column break before heading.	option	-	
	Option **Description** *heading1* Column break before heading 1. *heading2* Column break before heading 2. *heading3* Column break before heading 3.			
page-break-before	Report page auto page break before heading.	option	-	
	Option **Description** *heading1* Page break before heading 1. *heading2* Page break before heading 2. *heading3* Page break before heading 3.			
options	Report page options.	option	-	
	Option **Description** *header-on-first-page* Show header on first page. *footer-on-first-page* Show footer on first page.			

config header

Parameter	Description	Type	Size	Default
style	Report header style.	string	Maximum length: 71	

config header-item

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 63	
type	Report item type.	option	-	text

Parameter	Description	Type	Size	Default
	Option **Description** *text* Text. *image* Image.			
style	Report item style.	string	Maximum length: 71	
content	Report item text content.	string	Maximum length: 511	
img-src	Report item image file name.	string	Maximum length: 127	

config footer

Parameter	Description	Type	Size	Default
style	Report footer style.	string	Maximum length: 71	

config footer-item

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 63	
type	Report item type.	option	-	text
	Option **Description** *text* Text. *image* Image.			
style	Report item style.	string	Maximum length: 71	
content	Report item text content.	string	Maximum length: 511	
img-src	Report item image file name.	string	Maximum length: 127	

config body-item

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 63	
type	Report item type.	option	-	text
	Option / **Description** *text* / Text. *image* / Image. *chart* / Chart. *misc* / Miscellaneous.			
style	Report item style.	string	Maximum length: 71	
top-n	Value of top.	integer	Minimum value: 0 Maximum value: 4294967295	0
text-component	Report item text component.	option	-	text
	Option / **Description** *text* / Normal text. *heading1* / Heading 1. *heading2* / Heading 2. *heading3* / Heading 3.			
content	Report item text content.	string	Maximum length: 511	
img-src	Report item image file name.	string	Maximum length: 127	
chart	Report item chart name.	string	Maximum length: 71	
chart-options	Report chart options.	option	-	include-no-data hide-title show-caption

Parameter	Description	Type	Size	Default
	Option / **Description** *include-no-data* / Include chart with no data. *hide-title* / Hide chart title. *show-caption* / Show chart caption.			
misc-component	Report item miscellaneous component.	option	-	hline
	Option / **Description** *hline* / Horizontal line. *page-break* / Page break. *column-break* / Column break. *section-start* / Section start.			
title	Report section title.	string	Maximum length: 511	

config parameters

Parameter	Description	Type	Size	Default
name	Field name that match field of parameters defined in dataset.	string	Maximum length: 127	
value	Value to replace corresponding field of parameters defined in dataset.	string	Maximum length: 1023	

config report setting

Report setting configuration.

```
config report setting
    Description: Report setting configuration.
    set pdf-report [enable|disable]
    set fortiview [enable|disable]
    set report-source {option1}, {option2}, ...
    set web-browsing-threshold {integer}
    set top-n {integer}
end
```

config report setting

Parameter	Description	Type	Size	Default
pdf-report	Enable/disable PDF report.	option	-	enable
	Option / **Description** *enable* — Enable PDF report. *disable* — Disable PDF report.			
fortiview	Enable/disable historical FortiView.	option	-	enable
	Option / **Description** *enable* — Enable historical FortiView. *disable* — Disable historical FortiView.			
report-source	Report log source.	option	-	forward-traffic
	Option / **Description** *forward-traffic* — Report includes forward traffic logs. *sniffer-traffic* — Report includes sniffer traffic logs. *local-deny-traffic* — Report includes local deny traffic logs.			
web-browsing-threshold	Web browsing time calculation threshold .	integer	Minimum value: 3 Maximum value: 15	3
top-n	Number of items to populate .	integer	Minimum value: 1000 Maximum value: 20000	1000

config report sql status

Show report database status.

```
config report sql status
    Description: Show report database status.
end
```

router

This section includes syntax for the following commands:

config router policy

Configure IPv4 routing policies.

```
config router policy
    Description: Configure IPv4 routing policies.
    edit <seq-num>
        set input-device <name1>, <name2>, ...
        set src <subnet1>, <subnet2>, ...
        set dst <subnet1>, <subnet2>, ...
        set action [deny|permit]
        set protocol {integer}
        set start-port {integer}
        set end-port {integer}
        set start-source-port {integer}
        set end-source-port {integer}
        set gateway {ipv4-address}
        set output-device {string}
        set status [enable|disable]
        set comments {var-string}
    next
end
```

config router policy

Parameter	Description	Type	Size	Default
input-device <name>	Incoming interface name. Interface name.	string	Maximum length: 79	
src <subnet>	Source IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79	
dst <subnet>	Destination IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79	
action	Action of the policy route.	option	-	permit

Parameter	Description	Type	Size	Default
	Option / **Description** *deny* / Do not search policy route table. *permit* / Use this policy route for forwarding.			
protocol	Protocol number .	integer	Minimum value: 0 Maximum value: 255	0
start-port	Start destination port number .	integer	Minimum value: 0 Maximum value: 65535	1
end-port	End destination port number .	integer	Minimum value: 0 Maximum value: 65535	65534
start-source-port	Start source port number .	integer	Minimum value: 0 Maximum value: 65535	1
end-source-port	End source port number .	integer	Minimum value: 0 Maximum value: 65535	65534
gateway	IP address of the gateway.	ipv4-address	Not Specified	0.0.0.0
output-device	Outgoing interface name.	string	Maximum length: 35	
status	Enable/disable this policy route.	option	-	enable
	Option / **Description** *enable* / Enable this policy route. *disable* / Disable this policy route.			
comments	Optional comments.	var-string	Maximum length: 255	

config router static

Configure IPv4 static routing tables.

```
config router static
    Description: Configure IPv4 static routing tables.
    edit <seq-num>
        set status [enable|disable]
        set dst {ipv4-classnet}
        set src {ipv4-classnet}
        set gateway {ipv4-address}
        set weight {integer}
        set priority {integer}
        set device {string}
        set comment {var-string}
        set blackhole [enable|disable]
        set sdwan-zone <name1>, <name2>, ...
        set dstaddr {string}
        set link-monitor-exempt [enable|disable]
    next
end
```

config router static

Parameter	Description	Type	Size	Default
status	Enable/disable this static route. **Option** / **Description** *enable* — Enable static route. *disable* — Disable static route.	option	-	enable
dst	Destination IP and mask for this route.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
src	Source prefix for this route.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
gateway	Gateway IP for this route.	ipv4-address	Not Specified	0.0.0.0
weight	Administrative weight .	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default
priority	Administrative priority .	integer	Minimum value: 1 Maximum value: 65535	1
device	Gateway out interface or tunnel.	string	Maximum length: 35	
comment	Optional comments.	var-string	Maximum length: 255	
blackhole	Enable/disable black hole.	option	-	disable
	Option / **Description** *enable* — Enable black hole. *disable* — Disable black hole.			
sdwan-zone <name>	Choose SD-WAN Zone. SD-WAN zone name.	string	Maximum length: 79	
dstaddr	Name of firewall address or address group.	string	Maximum length: 79	
link-monitor-exempt	Enable/disable withdrawal of this static route when link monitor or health check is down.	option	-	disable
	Option / **Description** *enable* — Keep this static route when link monitor or health check is down. *disable* — Withdraw this static route when link monitor or health check is down. (default)			

config router static6

Configure IPv6 static routing tables.

```
config router static6
    Description: Configure IPv6 static routing tables.
    edit <seq-num>
        set status [enable|disable]
        set dst {ipv6-network}
        set gateway {ipv6-address}
        set device {string}
        set devindex {integer}
        set priority {integer}
        set comment {var-string}
        set blackhole [enable|disable]
        set sdwan-zone <name1>, <name2>, ...
```

```
        set link-monitor-exempt [enable|disable]
    next
end
```

config router static6

Parameter	Description	Type	Size	Default
status	Enable/disable this static route.	option	-	enable
	Option / **Description** *enable* — Enable static route. *disable* — Disable static route.			
dst	Destination IPv6 prefix.	ipv6-network	Not Specified	::/0
gateway	IPv6 address of the gateway.	ipv6-address	Not Specified	::
device	Gateway out interface or tunnel.	string	Maximum length: 35	
devindex	Device index .	integer	Minimum value: 0 Maximum value: 4294967295	0
priority	Administrative priority .	integer	Minimum value: 1 Maximum value: 65535	1024
comment	Optional comments.	var-string	Maximum length: 255	
blackhole	Enable/disable black hole.	option	-	disable
	Option / **Description** *enable* — Enable black hole. *disable* — Disable black hole.			
sdwan-zone <name>	Choose SD-WAN Zone. SD-WAN zone name.	string	Maximum length: 79	
link-monitor-exempt	Enable/disable withdrawal of this static route when link monitor or health check is down.	option	-	disable

Parameter	Description	Type	Size	Default

Option	Description
enable	Keep this static route when link monitor or health check is down.
disable	Withdraw this static route when link monitor or health check is down. (default)

ssh-filter

This section includes syntax for the following commands:

config ssh-filter profile

Configure SSH filter profile.

```
config ssh-filter profile
    Description: Configure SSH filter profile.
    edit <name>
        set block {option1}, {option2}, ...
        set log {option1}, {option2}, ...
        set default-command-log [enable|disable]
        config shell-commands
            Description: SSH command filter.
            edit <id>
                set type [simple|regex]
                set pattern {string}
                set action [block|allow]
                set log [enable|disable]
                set alert [enable|disable]
                set severity [low|medium|...]
            next
        end
    next
end
```

config ssh-filter profile

Parameter	Description	Type	Size	Default
block	SSH blocking options.	option	-	

Option	Description
x11	X server forwarding.
shell	SSH shell.
exec	SSH execution.
port-forward	Port forwarding.
tun-forward	Tunnel forwarding.

Parameter	Description	Type	Size	Default
	Option / **Description** *sftp* — SFTP. *scp* — SCP. *unknown* — Unknown channel.			
log	SSH logging options.	option	-	
	Option / **Description** *x11* — X server forwarding. *shell* — SSH shell. *exec* — SSH execution. *port-forward* — Port forwarding. *tun-forward* — Tunnel forwarding. *sftp* — SFTP. *scp* — SCP. *unknown* — Unknown channel.			
default-command-log	Enable/disable logging unmatched shell commands.	option	-	disable
	Option / **Description** *enable* — Enable log unmatched shell commands. *disable* — Disable log unmatched shell commands.			

config shell-commands

Parameter	Description	Type	Size	Default
type	Matching type.	option	-	simple
	Option / **Description** *simple* — Match single command. *regex* — Match command line using regular expression.			
pattern	SSH shell command pattern.	string	Maximum length: 128	
action	Action to take for SSH shell command matches.	option	-	block

Parameter	Description	Type	Size	Default
	Option / **Description** *block* — Block the SSH shell command. *allow* — Allow the SSH shell command.			
log	Enable/disable logging.	option	-	disable
	Option / **Description** *enable* — Enable logging. *disable* — Disable logging.			
alert	Enable/disable alert.	option	-	disable
	Option / **Description** *enable* — Enable alert. *disable* — Disable alert.			
severity	Log severity.	option	-	medium
	Option / **Description** *low* — Severity low. *medium* — Severity medium. *high* — Severity high. *critical* — Severity critical.			

system

This section includes syntax for the following commands:

config system accprofile

Configure access profiles for system administrators.

```
config system accprofile
    Description: Configure access profiles for system administrators.
    edit <name>
        set scope [vdom|global]
        set comments {var-string}
        set secfabgrp [none|read|...]
        set ftviewgrp [none|read|...]
        set authgrp [none|read|...]
        set sysgrp [none|read|...]
        set netgrp [none|read|...]
        set loggrp [none|read|...]
        set fwgrp [none|read|...]
        set vpngrp [none|read|...]
        set utmgrp [none|read|...]
        set wanoptgrp [none|read|...]
        config netgrp-permission
            Description: Custom network permission.
            set cfg [none|read|...]
            set packet-capture [none|read|...]
            set route-cfg [none|read|...]
        end
        config sysgrp-permission
            Description: Custom system permission.
            set admin [none|read|...]
            set upd [none|read|...]
            set cfg [none|read|...]
            set mnt [none|read|...]
        end
        config fwgrp-permission
            Description: Custom firewall permission.
            set policy [none|read|...]
            set address [none|read|...]
            set service [none|read|...]
            set schedule [none|read|...]
            set others [none|read|...]
        end
        config loggrp-permission
            Description: Custom Log & Report permission.
            set config [none|read|...]
            set data-access [none|read|...]
            set report-access [none|read|...]
            set threat-weight [none|read|...]
        end
        config utmgrp-permission
            Description: Custom Security Profile permissions.
            set antivirus [none|read|...]
            set ips [none|read|...]
            set webfilter [none|read|...]
            set emailfilter [none|read|...]
            set data-loss-prevention [none|read|...]
            set file-filter [none|read|...]
```

```
            set application-control [none|read|...]
            set icap [none|read|...]
            set voip [none|read|...]
            set waf [none|read|...]
            set dnsfilter [none|read|...]
            set endpoint-control [none|read|...]
        end
        set admintimeout-override [enable|disable]
        set admintimeout {integer}
        set system-diagnostics [enable|disable]
    next
end
```

config system accprofile

Parameter	Description	Type	Size	Default
scope	Scope of admin access: global or specific VDOM(s).	option	-	vdom
	Option / **Description** *vdom* — VDOM access. *global* — Global access.			
comments	Comment.	var-string	Maximum length: 255	
secfabgrp	Security Fabric.	option	-	none
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access.			
ftviewgrp	FortiView.	option	-	none
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access.			
authgrp	Administrator access to Users and Devices.	option	-	none
	Option / **Description** *none* — No access.			

Parameter	Description	Type	Size	Default
	Option / **Description** *read* — Read access. *read-write* — Read/write access.			
sysgrp	System Configuration.	option	-	none
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access. *custom* — Customized access.			
netgrp	Network Configuration.	option	-	none
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access. *custom* — Customized access.			
loggrp	Administrator access to Logging and Reporting including viewing log messages.	option	-	none
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access. *custom* — Customized access.			
fwgrp	Administrator access to the Firewall configuration.	option	-	none
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access. *custom* — Customized access.			

Parameter	Description	Type	Size	Default
vpngrp	Administrator access to IPsec, SSL, PPTP, and L2TP VPN.	option	-	none

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size	Default
utmgrp	Administrator access to Security Profiles.	option	-	none

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.
custom	Customized access.

Parameter	Description	Type	Size	Default
wanoptgrp	Administrator access to WAN Opt & Cache.	option	-	none

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size	Default
admintimeout-override	Enable/disable overriding the global administrator idle timeout.	option	-	disable

Option	Description
enable	Enable overriding the global administrator idle timeout.
disable	Disable overriding the global administrator idle timeout.

Parameter	Description	Type	Size	Default
admintimeout	Administrator timeout for this access profile .	integer	Minimum value: 1 Maximum value: 480	10
system-diagnostics	Enable/disable permission to run system diagnostic commands.	option	-	enable

Option	Description
enable	Enable permission to run system diagnostic commands.
disable	Disable permission to run system diagnostic commands.

config netgrp-permission

Parameter	Description	Type	Size	Default
cfg	Network Configuration.	option	-	none

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size	Default
packet-capture	Packet Capture Configuration.	option	-	none

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size	Default
route-cfg	Router Configuration.	option	-	none

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

config sysgrp-permission

Parameter	Description	Type	Size	Default
admin	Administrator Users.	option	-	none

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size	Default
upd	FortiGuard Updates.	option	-	none

Option	Description
none	No access.
read	Read access.

Parameter	Description	Type	Size	Default
	Option **Description** *read-write* Read/write access.			
cfg	System Configuration.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
mnt	Maintenance.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			

config fwgrp-permission

Parameter	Description	Type	Size	Default
policy	Policy Configuration.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
address	Address Configuration.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
service	Service Configuration.	option	-	none

Parameter	Description	Type	Size	Default
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
schedule	Schedule Configuration.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
others	Other Firewall Configuration.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			

config loggrp-permission

Parameter	Description	Type	Size	Default
config	Log & Report configuration.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
data-access	Log & Report Data Access.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
report-access	Log & Report Report Access.	option	-	none

Parameter	Description	Type	Size	Default
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
threat-weight	Log & Report Threat Weight.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			

config utmgrp-permission

Parameter	Description	Type	Size	Default
antivirus	Antivirus profiles and settings.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
ips	IPS profiles and settings.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
webfilter	Web Filter profiles and settings.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
emailfilter	Email Filter and settings.	option	-	none

Parameter	Description	Type	Size	Default
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
data-loss-prevention	DLP profiles and settings.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
file-filter	File-filter profiles and settings.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
application-control	Application Control profiles and settings.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
icap	ICAP profiles and settings.	option	-	none
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.			
voip	VoIP profiles and settings.	option	-	none

Parameter	Description	Type	Size	Default
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access.			
waf	Web Application Firewall profiles and settings.	option	-	none
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access.			
dnsfilter	DNS Filter profiles and settings.	option	-	none
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access.			
endpoint-control	FortiClient Profiles.	option	-	none
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access.			

config system acme

Configure ACME client.

```
config system acme
    Description: Configure ACME client.
    set interface <interface-name1>, <interface-name2>, ...
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    config accounts
        Description: ACME accounts list.
        edit <id>
            set status {string}
```

```
            set url {string}
            set ca_url {string}
            set email {string}
            set privatekey {string}
        next
    end
end
```

config system acme

Parameter	Description	Type	Size	Default
interface <interface-name>	Interface(s) on which the ACME client will listen for challenges. Interface name.	string	Maximum length: 79	
source-ip	Source IPv4 address used to connect to the ACME server.	ipv4-address	Not Specified	0.0.0.0
source-ip6	Source IPv6 address used to connect to the ACME server.	ipv6-address	Not Specified	::

config accounts

Parameter	Description	Type	Size	Default
status	Account status.	string	Maximum length: 127	
url	Account url.	string	Maximum length: 511	
ca_url	Account ca_url.	string	Maximum length: 255	
email	Account email.	string	Maximum length: 255	
privatekey	Account Private Key.	string	Maximum length: 8191	

config system admin

Configure admin users.

```
config system admin
    Description: Configure admin users.
    edit <name>
        set wildcard [enable|disable]
        set remote-auth [enable|disable]
```

```
        set remote-group {string}
        set password {password-2}
        set peer-auth [enable|disable]
        set peer-group {string}
        set trusthost1 {ipv4-classnet}
        set trusthost2 {ipv4-classnet}
        set trusthost3 {ipv4-classnet}
        set trusthost4 {ipv4-classnet}
        set trusthost5 {ipv4-classnet}
        set trusthost6 {ipv4-classnet}
        set trusthost7 {ipv4-classnet}
        set trusthost8 {ipv4-classnet}
        set trusthost9 {ipv4-classnet}
        set trusthost10 {ipv4-classnet}
        set ip6-trusthost1 {ipv6-prefix}
        set ip6-trusthost2 {ipv6-prefix}
        set ip6-trusthost3 {ipv6-prefix}
        set ip6-trusthost4 {ipv6-prefix}
        set ip6-trusthost5 {ipv6-prefix}
        set ip6-trusthost6 {ipv6-prefix}
        set ip6-trusthost7 {ipv6-prefix}
        set ip6-trusthost8 {ipv6-prefix}
        set ip6-trusthost9 {ipv6-prefix}
        set ip6-trusthost10 {ipv6-prefix}
        set accprofile {string}
        set allow-remove-admin-session [enable|disable]
        set comments {var-string}
        set vdom <name1>, <name2>, ...
        set ssh-public-key1 {user}
        set ssh-public-key2 {user}
        set ssh-public-key3 {user}
        set ssh-certificate {string}
        set schedule {string}
        set accprofile-override [enable|disable]
        set radius-vdom-override [enable|disable]
        set password-expire {user}
        set force-password-change [enable|disable]
        set two-factor [disable|fortitoken|...]
        set two-factor-authentication [fortitoken|email|...]
        set two-factor-notification [email|sms]
        set fortitoken {string}
        set email-to {string}
        set sms-server [fortiguard|custom]
        set sms-custom-server {string}
        set sms-phone {string}
        set guest-auth [disable|enable]
        set guest-usergroups <name1>, <name2>, ...
        set guest-lang {string}
    next
end
```

config system admin

Parameter	Description	Type	Size	Default
wildcard	Enable/disable wildcard RADIUS authentication.	option	-	disable
	Option / **Description** *enable* — Enable username wildcard. *disable* — Disable username wildcard.			
remote-auth	Enable/disable authentication using a remote RADIUS, LDAP, or TACACS+ server.	option	-	disable
	Option / **Description** *enable* — Enable remote authentication. *disable* — Disable remote authentication.			
remote-group	User group name used for remote auth.	string	Maximum length: 35	
password	Admin user password.	password-2	Not Specified	
peer-auth	Set to enable peer certificate authentication (for HTTPS admin access).	option	-	disable
	Option / **Description** *enable* — Enable peer. *disable* — Disable peer.			
peer-group	Name of peer group defined under config user group which has PKI members. Used for peer certificate authentication (for HTTPS admin access).	string	Maximum length: 35	
trusthost1	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost2	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost3	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

Parameter	Description	Type	Size	Default
trusthost4	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost5	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost6	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost7	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost8	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost9	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost10	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
ip6-trusthost1	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost2	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost3	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost4	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0

Parameter	Description	Type	Size	Default
ip6-trusthost5	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost6	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost7	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost8	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost9	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost10	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
accprofile	Access profile for this administrator. Access profiles control administrator access to FortiProxy features.	string	Maximum length: 35	
allow-remove-admin-session	Enable/disable allow admin session to be removed by privileged admin users.	option	-	enable

Option	Description
enable	Enable allow-remove option.
disable	Disable allow-remove option.

comments	Comment.	var-string	Maximum length: 255	
vdom `<name>`	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	
ssh-public-key1	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified	
ssh-public-key2	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified	

Parameter	Description	Type	Size	Default
ssh-public-key3	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified	
ssh-certificate	Select the certificate to be used by the FortiProxy for authentication with an SSH client.	string	Maximum length: 35	
schedule	Firewall schedule used to restrict when the administrator can log in. No schedule means no restrictions.	string	Maximum length: 35	
accprofile-override	Enable to use the name of an access profile provided by the remote authentication server to control the FortiProxy features that this administrator can access.	option	-	disable
	Option / **Description** *enable* — Enable access profile override. *disable* — Disable access profile override.			
radius-vdom-override	Enable to use the names of VDOMs provided by the remote authentication server to control the VDOMs that this administrator can access.	option	-	disable
	Option / **Description** *enable* — Enable VDOM override. *disable* — Disable VDOM override.			
password-expire	Password expire time.	user	Not Specified	
force-password-change	Enable/disable force password change on next login.	option	-	disable
	Option / **Description** *enable* — Enable force password change on next login. *disable* — Disable force password change on next login.			
two-factor	Enable/disable two-factor authentication.	option	-	disable
	Option / **Description** *disable* — Disable two-factor authentication. *fortitoken* — Use FortiToken or FortiToken mobile two-factor authentication.			

Parameter	Description	Type	Size	Default
	Option / **Description** *fortitoken-cloud* — FortiToken Cloud Service. *email* — Send a two-factor authentication code to the configured email-to email address. *sms* — Send a two-factor authentication code to the configured sms-server and sms-phone.			
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-	
	Option / **Description** *fortitoken* — FortiToken authentication. *email* — Email one time password. *sms* — SMS one time password.			
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-	
	Option / **Description** *email* — Email notification for activation code. *sms* — SMS notification for activation code.			
fortitoken	This administrator's FortiToken serial number.	string	Maximum length: 16	
email-to	This administrator's email address.	string	Maximum length: 63	
sms-server	Send SMS messages using the FortiGuard SMS server or a custom server.	option	-	fortiguard
	Option / **Description** *fortiguard* — Send SMS by FortiGuard. *custom* — Send SMS by custom server.			
sms-custom-server	Custom SMS server to send SMS messages to.	string	Maximum length: 35	
sms-phone	Phone number on which the administrator receives SMS messages.	string	Maximum length: 15	
guest-auth	Enable/disable guest authentication.	option	-	disable

Parameter	Description	Type	Size	Default
	Option: *disable* — Disable guest authentication. Option: *enable* — Enable guest authentication.			
guest-usergroups <name>	Select guest user groups. Select guest user groups.	string	Maximum length: 79	
guest-lang	Guest management portal language.	string	Maximum length: 35	

config system affinity-interrupt

Configure interrupt affinity.

```
config system affinity-interrupt
    Description: Configure interrupt affinity.
    edit <id>
        set interrupt {string}
        set affinity-cpumask {string}
    next
end
```

config system affinity-interrupt

Parameter	Description	Type	Size	Default
interrupt	Interrupt name.	string	Maximum length: 127	
affinity-cpumask	Affinity setting for VM throughput (64-bit hexadecimal value in the format of 0xxxxxxxxxxxxxxxx).	string	Maximum length: 127	

config system affinity-packet-redistribution

Configure packet redistribution.

```
config system affinity-packet-redistribution
    Description: Configure packet redistribution.
    edit <id>
        set interface {string}
        set rxqid {integer}
        set affinity-cpumask {string}
```

```
    next
end
```

config system affinity-packet-redistribution

Parameter	Description	Type	Size	Default
interface	Physical interface name on which to perform packet redistribution.	string	Maximum length: 127	
rxqid	ID of the receive queue (when the interface has multiple queues) on which to perform packet redistribution.	integer	Minimum value: 0 Maximum value: 255	0
affinity-cpumask	Affinity setting for VM throughput (64-bit hexadecimal value in the format of 0xxxxxxxxxxxxxxxx).	string	Maximum length: 127	

config system alarm

Configure alarm.

```
config system alarm
    Description: Configure alarm.
    set status [enable|disable]
    set audible [enable|disable]
    config groups
        Description: Alarm groups.
        edit <id>
            set period {integer}
            set admin-auth-failure-threshold {integer}
            set admin-auth-lockout-threshold {integer}
            set user-auth-failure-threshold {integer}
            set user-auth-lockout-threshold {integer}
            set replay-attempt-threshold {integer}
            set self-test-failure-threshold {integer}
            set log-full-warning-threshold {integer}
            set encryption-failure-threshold {integer}
            set decryption-failure-threshold {integer}
            config fw-policy-violations
                Description: Firewall policy violations.
                edit <id>
                    set threshold {integer}
                    set src-ip {ipv4-address}
                    set dst-ip {ipv4-address}
                    set src-port {integer}
                    set dst-port {integer}
                next
            end
            set fw-policy-id {integer}
            set fw-policy-id-threshold {integer}
```

```
        next
    end
end
```

config system alarm

Parameter	Description	Type	Size	Default
status	Enable/disable alarm.	option	-	disable
	Option / **Description** *enable* — Enable alarm. *disable* — Disable alarm.			
audible	Enable/disable audible alarm.	option	-	disable
	Option / **Description** *enable* — Enable audible alarm. *disable* — Disable audible alarm.			

config groups

Parameter	Description	Type	Size	Default
period	Time period in seconds (0 = from start up).	integer	Minimum value: 0 Maximum value: 4294967295	0
admin-auth-failure-threshold	Admin authentication failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
admin-auth-lockout-threshold	Admin authentication lockout threshold.	integer	Minimum value: 0 Maximum value: 1024	0
user-auth-failure-threshold	User authentication failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0

Parameter	Description	Type	Size	Default
user-auth-lockout-threshold	User authentication lockout threshold.	integer	Minimum value: 0 Maximum value: 1024	0
replay-attempt-threshold	Replay attempt threshold.	integer	Minimum value: 0 Maximum value: 1024	0
self-test-failure-threshold	Self-test failure threshold.	integer	Minimum value: 0 Maximum value: 1	0
log-full-warning-threshold	Log full warning threshold.	integer	Minimum value: 0 Maximum value: 1024	0
encryption-failure-threshold	Encryption failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
decryption-failure-threshold	Decryption failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
fw-policy-id	Firewall policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
fw-policy-id-threshold	Firewall policy ID threshold.	integer	Minimum value: 0 Maximum value: 1024	0

config fw-policy-violations

Parameter	Description	Type	Size	Default
threshold	Firewall policy violation threshold.	integer	Minimum value: 0 Maximum value: 1024	0

Parameter	Description	Type	Size	Default
src-ip	Source IP (0=all).	ipv4-address	Not Specified	0.0.0.0
dst-ip	Destination IP (0=all).	ipv4-address	Not Specified	0.0.0.0
src-port	Source port (0=all).	integer	Minimum value: 0 Maximum value: 65535	0
dst-port	Destination port (0=all).	integer	Minimum value: 0 Maximum value: 65535	0

config system alias

Configure alias command.

```
config system alias
    Description: Configure alias command.
    edit <name>
        set command {var-string}
    next
end
```

config system alias

Parameter	Description	Type	Size	Default
command	Command list to execute.	var-string	Maximum length: 255	

config system api-user

Configure API users.

```
config system api-user
    Description: Configure API users.
    edit <name>
        set comments {var-string}
        set api-key {password-2}
```

```
        set accprofile {string}
        set vdom <name1>, <name2>, ...
        set schedule {string}
        set cors-allow-origin {string}
        set peer-auth [enable|disable]
        set peer-group {string}
        config trusthost
            Description: Trusthost.
            edit <id>
                set type [ipv4-trusthost|ipv6-trusthost]
                set ipv4-trusthost {ipv4-classnet}
                set ipv6-trusthost {ipv6-prefix}
            next
        end
    next
end
```

config system api-user

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 255	
api-key	Admin user password.	password-2	Not Specified	
accprofile	Admin user access profile.	string	Maximum length: 35	
vdom <name>	Virtual domains. Virtual domain name.	string	Maximum length: 79	
schedule	Schedule name.	string	Maximum length: 35	
cors-allow-origin	Value for Access-Control-Allow-Origin on API responses. Avoid using '*' if possible.	string	Maximum length: 269	
peer-auth	Enable/disable peer authentication.	option	-	disable

Option	Description
enable	Enable peer.
disable	Disable peer.

peer-group	Peer group name.	string	Maximum length: 35	

config trusthost

Parameter	Description	Type	Size	Default
type	Trusthost type.	option	-	ipv4-trusthost
	Option / **Description** *ipv4-trusthost* / IPv4 trusthost. *ipv6-trusthost* / IPv6 trusthost.			
ipv4-trusthost	IPv4 trusted host address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
ipv6-trusthost	IPv6 trusted host address.	ipv6-prefix	Not Specified	::/0

config system arp-table

Configure ARP table.

```
config system arp-table
    Description: Configure ARP table.
    edit <id>
        set interface {string}
        set ip {ipv4-address}
        set mac {mac-address}
    next
end
```

config system arp-table

Parameter	Description	Type	Size	Default
interface	Interface name.	string	Maximum length: 15	
ip	IP address.	ipv4-address	Not Specified	0.0.0.0
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00

config system arp

IPv4 ARP table.

```
config system arp
    Description: IPv4 ARP table.
end
```

config system auto-install

Configure USB auto installation.

```
config system auto-install
    Description: Configure USB auto installation.
    set auto-install-config [enable|disable]
    set auto-install-image [enable|disable]
    set default-config-file {string}
    set default-image-file {string}
end
```

config system auto-install

Parameter	Description	Type	Size	Default
auto-install-config	Enable/disable auto install the config in USB disk.	option	-	disable
	Option / **Description** *enable* / Enable config. *disable* / Disable config.			
auto-install-image	Enable/disable auto install the image in USB disk.	option	-	disable
	Option / **Description** *enable* / Enable config. *disable* / Disable config.			
default-config-file	Default config file name in USB disk.	string	Maximum length: 127	fpx_system.conf
default-image-file	Default image file name in USB disk.	string	Maximum length: 127	image.out

config system auto-script

Configure auto script.

```
config system auto-script
    Description: Configure auto script.
    edit <name>
        set interval {integer}
        set repeat {integer}
        set start [manual|auto]
        set script {var-string}
        set password {password}
        set output-size {integer}
        set timeout {integer}
    next
end
```

config system auto-script

Parameter	Description	Type	Size	Default
interval	Repeat interval in seconds.	integer	Minimum value: 0 Maximum value: 31557600	0
repeat	Number of times to repeat this script (0 = infinite).	integer	Minimum value: 0 Maximum value: 65535	1
start	Script starting mode.	option	-	manual
	Option / **Description** *manual* — Starting manually. *auto* — Starting automatically.			
script	List of FortiProxy CLI commands to repeat.	var-string	Maximum length: 1023	
password	Script password to replace %%PASSWD%% tag in the script. Use cases include replacing a password tag for sftp/ftp server password.	password	Not Specified	
output-size	Number of megabytes to limit script output to .	integer	Minimum value: 10 Maximum value: 1024	10
timeout	Maximum running time for this script in seconds (0 = no timeout).	integer	Minimum value: 0 Maximum value: 300	0

config system auto-update status

Status of automatic updates.

```
config system auto-update status
    Description: Status of automatic updates.
end
```

config system auto-update versions

Update object versions.

```
config system auto-update versions
    Description: Update object versions.
end
```

config system automation-action

Action for automation stitches.

```
config system automation-action
    Description: Action for automation stitches.
    edit <name>
        set description {var-string}
        set action-type [email|fortiexplorer-notification|...]
        set tls-certificate {string}
        set email-to <name1>, <name2>, ...
        set email-from {var-string}
        set email-subject {var-string}
        set minimum-interval {integer}
        set aws-api-key {password}
        set azure-function-authorization [anonymous|function|...]
        set azure-api-key {password}
        set alicloud-function-authorization [anonymous|function]
        set alicloud-access-key-id {string}
        set alicloud-access-key-secret {password}
        set message-type [text|json]
        set message {string}
        set replacement-message [enable|disable]
        set replacemsg-group {string}
        set protocol [http|https]
        set method [post|put|...]
        set uri {var-string}
        set http-body {var-string}
        set port {integer}
        set headers <header1>, <header2>, ...
        set verify-host-cert [enable|disable]
        set script {var-string}
        set execute-security-fabric [enable|disable]
```

```
        set accprofile {string}
        set security-tag {string}
        set sdn-connector <name1>, <name2>, ...
    next
end
```

config system automation-action

Parameter	Description	Type	Size	Default
description	Description.	var-string	Maximum length: 255	
action-type	Action type.	option	-	alert

Option	Description
email	Send notification email.
fortiexplorer-notification	Send push notification to FortiExplorer.
alert	Generate FortiProxy dashboard alert.
disable-ssid	Disable interface.
quarantine	Quarantine host.
quarantine-forticlient	Quarantine FortiClient by EMS.
quarantine-nsx	Quarantine NSX instance.
quarantine-fortinac	Quarantine host by FortiNAC.
ban-ip	Ban IP address.
aws-lambda	Send log data to integrated AWS service.
azure-function	Send log data to an Azure function.
google-cloud-function	Send log data to a Google Cloud function.
alicloud-function	Send log data to an AliCloud function.
webhook	Send an HTTP request.
cli-script	Run CLI script.
slack-notification	Send a notification message to a Slack incoming webhook.
microsoft-teams-notification	Send a notification message to a Microsoft Teams incoming webhook.

Parameter	Description	Type	Size	Default
tls-certificate	Custom TLS certificate for API request.	string	Maximum length: 35	
email-to <name>	Email addresses. Email address.	string	Maximum length: 255	
email-from	Email sender name.	var-string	Maximum length: 127	
email-subject	Email subject.	var-string	Maximum length: 511	
minimum-interval	Limit execution to no more than once in this interval (in seconds).	integer	Minimum value: 0 Maximum value: 2592000	0
aws-api-key	AWS API Gateway API key.	password	Not Specified	
azure-function-authorization	Azure function authorization level.	option	-	anonymous

Option	Description
anonymous	Anonymous authorization level (No authorization required).
function	Function authorization level (Function or Host Key required).
admin	Admin authorization level (Master Host Key required).

azure-api-key	Azure function API key.	password	Not Specified	
alicloud-function-authorization	AliCloud function authorization type.	option	-	anonymous

Option	Description
anonymous	Anonymous authorization (No authorization required).
function	Function authorization (Authorization required).

alicloud-access-key-id	AliCloud AccessKey ID.	string	Maximum length: 35	
alicloud-access-key-secret	AliCloud AccessKey secret.	password	Not Specified	
message-type	Message type.	option	-	text

Parameter	Description	Type	Size	Default
	Option / **Description** *text* / Plaintext. *json* / Custom JSON.			
message	Message content.	string	Maximum length: 4095	%%log%%
replacement-message	Enable/disable replacement message.	option	-	disable
	Option / **Description** *enable* / Enable replacement message. *disable* / Disable replacement message.			
replacemsg-group	Replacement message group.	string	Maximum length: 35	
protocol	Request protocol.	option	-	http
	Option / **Description** *http* / HTTP. *https* / HTTPS.			
method	Request method (POST, PUT, GET, PATCH or DELETE).	option	-	post
	Option / **Description** *post* / POST. *put* / PUT. *get* / GET. *patch* / PATCH. *delete* / DELETE.			
uri	Request API URI.	var-string	Maximum length: 1023	
http-body	Request body (if necessary). Should be serialized json string.	var-string	Maximum length: 4095	

Parameter	Description	Type	Size	Default
port	Protocol port.	integer	Minimum value: 1 Maximum value: 65535	0
headers <header>	Request headers. Request header.	string	Maximum length: 255	
verify-host-cert	Enable/disable verification of the remote host certificate.	option	-	enable
	Option / **Description** *enable* — Enable verification of the remote host certificate. *disable* — Disable verification of the remote host certificate.			
script	CLI script.	var-string	Maximum length: 1023	
execute-security-fabric	Enable/disable execution of CLI script on all or only one FortiGate unit in the Security Fabric.	option	-	disable
	Option / **Description** *enable* — CLI script executes on all FortiGate units in the Security Fabric. *disable* — CLI script executes only on the FortiGate unit that the stitch is triggered.			
accprofile	Access profile for CLI script action to access FortiProxy features.	string	Maximum length: 35	
security-tag	NSX security tag.	string	Maximum length: 255	
sdn-connector <name>	NSX SDN connector names. SDN connector name.	string	Maximum length: 79	

config system automation-destination

Automation destinations.

```
config system automation-destination
    Description: Automation destinations.
    edit <name>
        set type [fortiproxy|ha-cluster]
        set destination <name1>, <name2>, ...
        set ha-group-id {integer}
    next
end
```

config system automation-destination

Parameter	Description	Type	Size	Default
type	Destination type.	option	-	fortiproxy
	Option / **Description** *fortiproxy* — FortiProxy set as destination. *ha-cluster* — HA cluster set as destination.			
destination <name>	Destinations. Destination.	string	Maximum length: 31	
ha-group-id	Cluster group ID set for this destination .	integer	Minimum value: 0 Maximum value: 255	0

config system automation-stitch

Automation stitches.

```
config system automation-stitch
    Description: Automation stitches.
    edit <name>
        set description {var-string}
        set status [enable|disable]
        set trigger {string}
        config actions
            Description: Configure stitch actions.
            edit <id>
                set action {string}
                set delay {integer}
                set required [enable|disable]
            next
        end
        set destination <name1>, <name2>, ...
    next
end
```

config system automation-stitch

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

Parameter	Description	Type	Size	Default
status	Enable/disable this stitch.	option	-	enable
	Option / **Description** *enable* — Enable stitch. *disable* — Disable stitch.			
trigger	Trigger name.	string	Maximum length: 35	
destination <name>	Serial number/HA group-name of destination devices. Destination name.	string	Maximum length: 79	

config actions

Parameter	Description	Type	Size	Default
action	Action name.	string	Maximum length: 64	
delay	Delay before execution (in seconds).	integer	Minimum value: 0 Maximum value: 3600	0
required	Required in action chain.	option	-	disable
	Option / **Description** *enable* — Required in action chain. *disable* — Not required in action chain.			

config system automation-trigger

Trigger for automation stitches.

```
config system automation-trigger
    Description: Trigger for automation stitches.
    edit <name>
        set description {var-string}
        set trigger-type [event-based|scheduled]
        set event-type [ioc|event-log|...]
        set license-type [forticare-support|fortiguard-webfilter|...]
        set ioc-level [medium|high]
        set report-type [posture|coverage|...]
        set logid <id1>, <id2>, ...
        set trigger-frequency [hourly|daily|...]
```

```
        set trigger-weekday [sunday|monday|...]
        set trigger-day {integer}
        set trigger-hour {integer}
        set trigger-minute {integer}
        config fields
            Description: Customized trigger field settings.
            edit <id>
                set name {string}
                set value {var-string}
            next
        end
        set faz-event-name {var-string}
        set faz-event-severity {var-string}
        set faz-event-tags {var-string}
        set serial {var-string}
        set fabric-event-name {var-string}
        set fabric-event-severity {var-string}
    next
end
```

config system automation-trigger

Parameter	Description	Type	Size	Default
description	Description.	var-string	Maximum length: 255	
trigger-type	Trigger type.	option	-	event-based

Option	Description
event-based	Event based trigger.
scheduled	Scheduled trigger.

Parameter	Description	Type	Size	Default
event-type	Event type.	option	-	ioc

Option	Description
ioc	Indicator of compromise detected.
event-log	Use log ID as trigger.
reboot	Device reboot.
low-memory	Conserve mode due to low memory.
high-cpu	High CPU usage.
license-near-expiry	License near expiration date.
ha-failover	HA failover.

Parameter	Description	Type	Size	Default
	Option / **Description** *config-change* — Configuration change. *security-rating-summary* — Security rating summary. *virus-ips-db-updated* — Virus and IPS database updated. *faz-event* — FortiAnalyzer event. *incoming-webhook* — Incoming webhook call. *fabric-event* — Fabric connector event.			
license-type	License type.	option	-	forticare-support
	Option / **Description** *forticare-support* — FortiCare support license. *fortiguard-webfilter* — FortiGuard web filter license. *fortiguard-antispam* — FortiGuard antispam license. *fortiguard-antivirus* — FortiGuard AntiVirus license. *fortiguard-ips* — FortiGuard IPS license. *fortiguard-management* — FortiGuard management service license. *forticloud* — FortiCloud license. *any* — Any license.			
ioc-level	IOC threat level.	option	-	high
	Option / **Description** *medium* — IOC level medium and high. *high* — IOC level high only.			
report-type	Security Rating report.	option	-	posture

Parameter	Description	Type	Size	Default
	Option / **Description** *posture* / Posture report. *coverage* / Coverage report. *optimization* / Optimization report *any* / Any report.			
logid <id>	Log IDs to trigger event. Log ID.	integer	Minimum value: 1 Maximum value: 65535	
trigger-frequency	Scheduled trigger frequency .	option	-	daily
	Option / **Description** *hourly* / Run hourly. *daily* / Run daily. *weekly* / Run weekly. *monthly* / Run monthly.			
trigger-weekday	Day of week for trigger.	option	-	
	Option / **Description** *sunday* / Sunday. *monday* / Monday. *tuesday* / Tuesday. *wednesday* / Wednesday. *thursday* / Thursday. *friday* / Friday. *saturday* / Saturday.			
trigger-day	Day within a month to trigger.	integer	Minimum value: 1 Maximum value: 31	1

Parameter	Description	Type	Size	Default
trigger-hour	Hour of the day on which to trigger .	integer	Minimum value: 0 Maximum value: 23	0
trigger-minute	Minute of the hour on which to trigger .	integer	Minimum value: 0 Maximum value: 59	0
faz-event-name	FortiAnalyzer event handler name.	var-string	Maximum length: 255	
faz-event-severity	FortiAnalyzer event severity.	var-string	Maximum length: 255	
faz-event-tags	FortiAnalyzer event tags.	var-string	Maximum length: 255	
serial	Fabric connector serial number.	var-string	Maximum length: 255	
fabric-event-name	Fabric connector event handler name.	var-string	Maximum length: 255	
fabric-event-severity	Fabric connector event severity.	var-string	Maximum length: 255	

config fields

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
value	Value.	var-string	Maximum length: 63	

config system autoupdate schedule

Configure update schedule.

```
config system autoupdate schedule
    Description: Configure update schedule.
    set status [enable|disable]
    set frequency [every|daily|...]
    set time {user}
    set day [Sunday|Monday|...]
end
```

config system autoupdate schedule

Parameter	Description	Type	Size	Default
status	Enable/disable scheduled updates.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
frequency	Update frequency.	option	-	automatic
	Option / **Description** *every* — Time interval. *daily* — Every day. *weekly* — Every week. *automatic* — Update automatically within every one hour period.			
time	Update time.	user	Not Specified	
day	Update day.	option	-	Monday
	Option / **Description** *Sunday* — Update every Sunday. *Monday* — Update every Monday. *Tuesday* — Update every Tuesday. *Wednesday* — Update every Wednesday. *Thursday* — Update every Thursday. *Friday* — Update every Friday. *Saturday* — Update every Saturday.			

config system autoupdate tunneling

Configure web proxy tunneling for the FDN.

```
config system autoupdate tunneling
    Description: Configure web proxy tunneling for the FDN.
    set status [enable|disable]
    set address {string}
    set port {integer}
    set username {string}
```

```
    set password {password}
end
```

config system autoupdate tunneling

Parameter	Description	Type	Size	Default
status	Enable/disable web proxy tunneling.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
address	Web proxy IP address or FQDN.	string	Maximum length: 63	
port	Web proxy port.	integer	Minimum value: 0 Maximum value: 65535	0
username	Web proxy username.	string	Maximum length: 49	
password	Web proxy password.	password	Not Specified	

config system central-management

Configure central management.

```
config system central-management
    Description: Configure central management.
    set mode [normal|backup]
    set type [fortimanager|fortiguard|...]
    set schedule-config-restore [enable|disable]
    set schedule-script-restore [enable|disable]
    set allow-push-configuration [enable|disable]
    set allow-push-firmware [enable|disable]
    set allow-remote-firmware-upgrade [enable|disable]
    set allow-monitor [enable|disable]
    set serial-number {user}
    set fmg {user}
    set fmg-source-ip {ipv4-address}
    set fmg-source-ip6 {ipv6-address}
    set local-cert {string}
    set ca-cert {user}
    set vdom {string}
```

```
    config server-list
        Description: Additional severs that the FortiProxy can use for updates (for AV, IPS,
updates) and ratings (for web filter and antispam ratings) servers.
        edit <id>
            set server-type {option1}, {option2}, ...
            set addr-type [ipv4|ipv6|...]
            set server-address {ipv4-address}
            set server-address6 {ipv6-address}
            set fqdn {string}
        next
    end
    set fmg-update-port [8890|443]
    set include-default-servers [enable|disable]
    set enc-algorithm [default|high|...]
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config system central-management

Parameter	Description	Type	Size	Default
mode	Central management mode.	option	-	normal
	Option / **Description** *normal* — Manage and configure this FortiProxy from FortiManager. *backup* — Manage and configure this FortiProxy locally and back up its configuration to FortiManager.			
type	Central management type.	option	-	none
	Option / **Description** *fortimanager* — FortiManager. *fortiguard* — Central management of this FortiProxy using FortiCloud. *none* — No central management.			
schedule-config-restore	Enable/disable allowing the central management server to restore the configuration of this FortiProxy.	option	-	enable
	Option / **Description** *enable* — Enable scheduled configuration restore. *disable* — Disable scheduled configuration restore.			
schedule-script-restore	Enable/disable allowing the central management server to restore the scripts stored on this FortiProxy.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable scheduled script restore. *disable* — Disable scheduled script restore.			
allow-push-configuration	Enable/disable allowing the central management server to push configuration changes to this FortiProxy.	option	-	enable
	Option / **Description** *enable* — Enable push configuration. *disable* — Disable push configuration.			
allow-push-firmware	Enable/disable allowing the central management server to push firmware updates to this FortiProxy.	option	-	enable
	Option / **Description** *enable* — Enable push firmware. *disable* — Disable push firmware.			
allow-remote-firmware-upgrade	Enable/disable remotely upgrading the firmware on this FortiProxy from the central management server.	option	-	enable
	Option / **Description** *enable* — Enable remote firmware upgrade. *disable* — Disable remote firmware upgrade.			
allow-monitor	Enable/disable allowing the central management server to remotely monitor this FortiProxy unit.	option	-	enable
	Option / **Description** *enable* — Enable remote monitoring of device. *disable* — Disable remote monitoring of device.			
serial-number	Serial number.	user	Not Specified	
fmg	IP address or FQDN of the FortiManager.	user	Not Specified	
fmg-source-ip	IPv4 source address that this FortiProxy uses when communicating with FortiManager.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
fmg-source-ip6	IPv6 source address that this FortiProxy uses when communicating with FortiManager.	ipv6-address	Not Specified	::
local-cert	Certificate to be used by FGFM protocol.	string	Maximum length: 35	
ca-cert	CA certificate to be used by FGFM protocol.	user	Not Specified	
vdom	Virtual domain (VDOM) name to use when communicating with FortiManager.	string	Maximum length: 31	root
fmg-update-port	Port used to communicate with FortiManager that is acting as a FortiGuard update server.	option	-	8890

Option	Description
8890	Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.
443	Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.

include-default-servers	Enable/disable inclusion of public FortiGuard servers in the override server list.	option	-	enable

Option	Description
enable	Enable inclusion of public FortiGuard servers in the override server list.
disable	Disable inclusion of public FortiGuard servers in the override server list.

enc-algorithm	Encryption strength for communications between the FortiProxy and central management.	option	-	low

Option	Description
default	High strength algorithms and medium-strength 128-bit key length algorithms.
high	128-bit and larger key length algorithms.
low	64-bit or 56-bit key length algorithms without export restrictions.

interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	Set outgoing interface manually.

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

config server-list

Parameter	Description	Type	Size	Default
server-type	FortiGuard service type.	option	-	
	Option / **Description** *update* — AV, IPS, and AV-query update server. *rating* — Web filter and anti-spam rating server.			
addr-type	Indicate whether the FortiProxy communicates with the override server using an IPv4 address, an IPv6 address or a FQDN.	option	-	ipv4
	Option / **Description** *ipv4* — IPv4 address. *ipv6* — IPv6 address. *fqdn* — FQDN.			
server-address	IPv4 address of override server.	ipv4-address	Not Specified	0.0.0.0
server-address6	IPv6 address of override server.	ipv6-address	Not Specified	::
fqdn	FQDN address of override server.	string	Maximum length: 255	

config system central-mgmt

Configuration of Central Management Service.

```
config system central-mgmt
    Description: Configuration of Central Management Service.
end
```

config system checksum status

System checksum.

```
config system checksum status
    Description: System checksum.
end
```

config system cmdb

System CMDB information.

```
config system cmdb
    Description: System CMDB information.
end
```

config system console

Configure console.

```
config system console
    Description: Configure console.
    set mode [batch|line]
    set baudrate [9600|19200|...]
    set output [standard|more]
    set login [enable|disable]
end
```

config system console

Parameter	Description	Type	Size	Default
mode	Console mode.	option	-	line

Option	Description
batch	Batch mode.
line	Line mode.

Parameter	Description	Type	Size	Default
baudrate	Console baud rate.	option	-	9600

Option	Description
9600	9600
19200	19200
38400	38400
57600	57600
115200	115200

Parameter	Description	Type	Size	Default
output	Console output mode.	option	-	more

Option	Description
standard	Standard output.
more	More page output.

Parameter	Description	Type	Size	Default
login	Enable/disable serial console and FortiExplorer.	option	-	enable

Option	Description
enable	Console login enable.
disable	Console login disable.

config system csf

Add this FortiProxy to a Security Fabric or set up a new Security Fabric on this FortiProxy.

```
config system csf
    Description: Add this FortiProxy to a Security Fabric or set up a new Security Fabric on
this FortiProxy.
    set status [enable|disable]
    set upstream {string}
    set upstream-port {integer}
    set group-name {string}
    set group-password {password}
    set accept-auth-by-cert [disable|enable]
    set log-unification [disable|enable]
    set authorization-request-type [serial|certificate]
    set certificate {string}
    set fabric-workers {integer}
    set downstream-access [enable|disable]
    set license-sharing [enable|disable]
    set downstream-accprofile {string}
    set configuration-sync [default|local]
    set fabric-object-unification [default|local]
    set saml-configuration-sync [default|local]
    config trusted-list
        Description: Pre-authorized and blocked security fabric nodes.
        edit <name>
            set authorization-type [serial|certificate]
            set serial {string}
            set certificate {var-string}
            set action [accept|deny]
            set ha-members {string}
            set downstream-authorization [enable|disable]
            set guaranteed-seats {integer}
        next
    end
```

```
    config fabric-connector
        Description: Fabric connector configuration.
        edit <serial>
            set accprofile {string}
            set configuration-write-access [enable|disable]
        next
    end
    set forticloud-account-enforcement [enable|disable]
    config fabric-device
        Description: Fabric device configuration.
        edit <name>
            set device-ip {ipv4-address}
            set https-port {integer}
            set access-token {varlen_password}
        next
    end
end
```

config system csf

Parameter	Description	Type	Size	Default
status	Enable/disable Security Fabric.	option	-	disable
	Option / **Description** *enable* — Enable Security Fabric. *disable* — Disable Security Fabric.			
upstream	IP/FQDN of the FortiProxy upstream from this FortiProxy in the Security Fabric.	string	Maximum length: 255	
upstream-port	The port number to use to communicate with the FortiProxy upstream from this FortiProxy in the Security Fabric .	integer	Minimum value: 1 Maximum value: 65535	8013
group-name	Security Fabric group name. All FortiProxys in a Security Fabric must have the same group name.	string	Maximum length: 35	
group-password	Security Fabric group password. All FortiProxys in a Security Fabric must have the same group password.	password	Not Specified	
accept-auth-by-cert	Accept connections with unknown certificates and ask admin for approval.	option	-	enable
	Option / **Description** *disable* — Do not accept SSL connections with unknown certificates. *enable* — Accept SSL connections without automatic certificate verification.			

Parameter	Description	Type	Size	Default
log-unification	Enable/disable broadcast of discovery messages for log unification.	option	-	enable

Option	Description
disable	Disable broadcast of discovery messages for log unification.
enable	Enable broadcast of discovery messages for log unification.

Parameter	Description	Type	Size	Default
authorization-request-type	Authorization request type.	option	-	serial

Option	Description
serial	Request verification by serial number.
certificate	Request verification by certificate.

Parameter	Description	Type	Size	Default
certificate	Certificate.	string	Maximum length: 35	
fabric-workers	Number of worker processes for Security Fabric daemon.	integer	Minimum value: 1 Maximum value: 4	2
downstream-access	Enable/disable downstream device access to this device's configuration and data.	option	-	disable

Option	Description
enable	Enable downstream device access to this device's configuration and data.
disable	Disable downstream device access to this device's configuration and data.

Parameter	Description	Type	Size	Default
license-sharing	Enable/disable license sharing between FortiProxy devices.	option	-	disable

Option	Description
enable	Enable license sharing.
disable	Disable license sharing.

Parameter	Description	Type	Size	Default
downstream-accprofile	Default access profile for requests from downstream devices.	string	Maximum length: 35	
configuration-sync	Configuration sync mode.	option	-	default

Parameter	Description	Type	Size	Default
	Option / **Description** *default* — Synchronize configuration for IPAM, FortiAnalyzer, FortiSandbox, and Central Management to root node. *local* — Do not synchronize configuration with root node.			
fabric-object-unification	Fabric CMDB Object Unification.	option	-	default
	Option / **Description** *default* — Global CMDB objects will be synchronized in Security Fabric. *local* — Global CMDB objects will not be synchronized to and from this device.			
saml-configuration-sync	SAML setting configuration synchronization.	option	-	default
	Option / **Description** *default* — SAML setting for fabric members is created by fabric root. *local* — Do not apply SAML configuration generated by root.			
forticloud-account-enforcement	Fabric FortiCloud account unification.	option	-	enable
	Option / **Description** *enable* — Enable FortiCloud account ID matching for Security Fabric. *disable* — Disable FortiCloud accound ID matching for Security Fabric.			

config trusted-list

Parameter	Description	Type	Size	Default
authorization-type	Authorization type.	option	-	serial
	Option / **Description** *serial* — Verify downstream by serial number. *certificate* — Verify downstream by certificate.			
serial	Serial.	string	Maximum length: 19	

Parameter	Description	Type	Size	Default
certificate	Certificate.	var-string	Maximum length: 32767	
action	Security fabric authorization action.	option	-	accept
	Option / **Description** *accept* — Accept authorization request. *deny* — Deny authorization request.			
ha-members	HA members.	string	Maximum length: 19	
downstream-authorization	Trust authorizations by this node's administrator.	option	-	disable
	Option / **Description** *enable* — Enable downstream authorization. *disable* — Disable downstream authorization.			
guaranteed-seats	The number of seats this FortiProxy device should be allocated with. This number is internally capped by 50%% of purchased seat.	integer	Minimum value: 0 Maximum value: 4294967295	0

config fabric-connector

Parameter	Description	Type	Size	Default
accprofile	Override access profile.	string	Maximum length: 35	
configuration-write-access	Enable/disable downstream device write access to configuration.	option	-	disable
	Option / **Description** *enable* — Enable downstream device write access to configuration. *disable* — Disable downstream device write access to configuration.			

config fabric-device

Parameter	Description	Type	Size	Default
device-ip	Device IP.	ipv4-address	Not Specified	0.0.0.0
https-port	HTTPS port for fabric device.	integer	Minimum value: 1 Maximum value: 65535	443
access-token	Device access token.	varlen_password	Not Specified	

config system custom-language

Configure custom languages.

```
config system custom-language
    Description: Configure custom languages.
    edit <name>
        set filename {string}
        set comments {var-string}
    next
end
```

config system custom-language

Parameter	Description	Type	Size	Default
filename	Custom language file path.	string	Maximum length: 63	
comments	Comment.	var-string	Maximum length: 255	

config system ddns

Configure DDNS.

```
config system ddns
    Description: Configure DDNS.
    edit <ddnsid>
        set ddns-server [dyndns.org|dyns.net|...]
        set server-type [ipv4|ipv6]
```

```
        set ddns-server-addr <addr1>, <addr2>, ...
        set ddns-zone {string}
        set ddns-ttl {integer}
        set ddns-auth [disable|tsig]
        set ddns-keyname {string}
        set ddns-key {password_aes256}
        set ddns-domain {string}
        set ddns-username {string}
        set ddns-sn {string}
        set ddns-password {password}
        set use-public-ip [disable|enable]
        set addr-type [ipv4|ipv6]
        set update-interval {integer}
        set clear-text [disable|enable]
        set ssl-certificate {string}
        set bound-ip {string}
        set monitor-interface <interface-name1>, <interface-name2>, ...
    next
end
```

config system ddns

Parameter	Description	Type	Size	Default
ddns-server	Select a DDNS service provider.	option	-	

Option	Description
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

server-type	Address type of the DDNS server.	option	-	ipv4

Option	Description
ipv4	Use IPv4 addressing.
ipv6	Use IPv6 addressing.

Parameter	Description	Type	Size	Default
ddns-server-addr <addr>	Generic DDNS server IP/FQDN list. IP address or FQDN of the server.	string	Maximum length: 256	
ddns-zone	Zone of your domain name (for example, DDNS.com).	string	Maximum length: 64	
ddns-ttl	Time-to-live for DDNS packets.	integer	Minimum value: 60 Maximum value: 86400	300
ddns-auth	Enable/disable TSIG authentication for your DDNS server.	option	-	disable
	Option / **Description** *disable* — Disable DDNS authentication. *tsig* — Enable TSIG authentication based on RFC2845.			
ddns-keyname	DDNS update key name.	string	Maximum length: 64	
ddns-key	DDNS update key (base 64 encoding).	password_aes256	Not Specified	
ddns-domain	Your fully qualified domain name. For example, yourname.ddns.com.	string	Maximum length: 64	
ddns-username	DDNS user name.	string	Maximum length: 64	
ddns-sn	DDNS Serial Number.	string	Maximum length: 64	
ddns-password	DDNS password.	password	Not Specified	
use-public-ip	Enable/disable use of public IP address.	option	-	disable
	Option / **Description** *disable* — Disable use of public IP address. *enable* — Enable use of public IP address.			
addr-type	Address type of interface address in DDNS update.	option	-	ipv4
	Option / **Description** *ipv4* — Use IPv4 address of the interface. *ipv6* — Use IPv6 address of the interface.			

Parameter	Description	Type	Size	Default
update-interval	DDNS update interval .	integer	Minimum value: 60 Maximum value: 2592000	0
clear-text	Enable/disable use of clear text connections.	option	-	disable
	Option / **Description** *disable* — Disable use of clear text connections. *enable* — Enable use of clear text connections.			
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory
bound-ip	Bound IP address.	string	Maximum length: 46	
monitor-interface <interface-name>	Monitored interface. Interface name.	string	Maximum length: 79	

config system dedicated-mgmt

Configure dedicated management.

```
config system dedicated-mgmt
    Description: Configure dedicated management.
    set status [enable|disable]
    set interface {string}
    set default-gateway {ipv4-address}
    set dhcp-server [enable|disable]
    set dhcp-netmask {ipv4-netmask}
    set dhcp-start-ip {ipv4-address}
    set dhcp-end-ip {ipv4-address}
end
```

config system dedicated-mgmt

Parameter	Description	Type	Size	Default
status	Enable/disable dedicated management.	option	-	disable

Parameter	Description	Type	Size	Default
	Option: *enable* — Enable setting. Option: *disable* — Disable setting.			
interface	Dedicated management interface.	string	Maximum length: 15	
default-gateway	Default gateway for dedicated management interface.	ipv4-address	Not Specified	0.0.0.0
dhcp-server	Enable/disable DHCP server on management interface. Option: *enable* — Enable DHCP server on management port. Option: *disable* — Disable DHCP server on management port.	option	-	disable
dhcp-netmask	DHCP netmask.	ipv4-netmask	Not Specified	0.0.0.0
dhcp-start-ip	DHCP start IP for dedicated management.	ipv4-address	Not Specified	0.0.0.0
dhcp-end-ip	DHCP end IP for dedicated management.	ipv4-address	Not Specified	0.0.0.0

config system dhcp6 server

Configure DHCPv6 servers.

```
config system dhcp6 server
    Description: Configure DHCPv6 servers.
    edit <id>
        set status [disable|enable]
        set rapid-commit [disable|enable]
        set lease-time {integer}
        set dns-service [delegated|default|...]
        set dns-search-list [delegated|specify]
        set dns-server1 {ipv6-address}
        set dns-server2 {ipv6-address}
        set dns-server3 {ipv6-address}
        set dns-server4 {ipv6-address}
        set domain {string}
        set subnet {ipv6-prefix}
        set interface {string}
        set option1 {user}
        set option2 {user}
        set option3 {user}
        set upstream-interface {string}
```

```
        set delegated-prefix-iaid {integer}
        set ip-mode [range|delegated]
        set prefix-mode [dhcp6|ra]
        config prefix-range
            Description: DHCP prefix configuration.
            edit <id>
                set start-prefix {ipv6-address}
                set end-prefix {ipv6-address}
                set prefix-length {integer}
            next
        end
        config ip-range
            Description: DHCP IP range configuration.
            edit <id>
                set start-ip {ipv6-address}
                set end-ip {ipv6-address}
            next
        end
    next
end
```

config system dhcp6 server

Parameter	Description	Type	Size	Default
status	Enable/disable this DHCPv6 configuration.	option	-	enable
	Option / **Description** *disable* — Enable this DHCPv6 server configuration. *enable* — Disable this DHCPv6 server configuration.			
rapid-commit	Enable/disable allow/disallow rapid commit.	option	-	disable
	Option / **Description** *disable* — Do not allow rapid commit. *enable* — Allow rapid commit.			
lease-time	Lease time in seconds, 0 means unlimited.	integer	Minimum value: 300 Maximum value: 8640000	604800
dns-service	Options for assigning DNS servers to DHCPv6 clients.	option	-	specify
	Option / **Description** *delegated* — Delegated DNS settings.			

Parameter	Description	Type	Size	Default
	Option / **Description** *default* — Clients are assigned the FortiProxy's configured DNS servers. *specify* — Specify up to 3 DNS servers in the DHCPv6 server configuration.			
dns-search-list	DNS search list options.	option	-	specify
	Option / **Description** *delegated* — Delegated the DNS search list. *specify* — Specify the DNS search list.			
dns-server1	DNS server 1.	ipv6-address	Not Specified	::
dns-server2	DNS server 2.	ipv6-address	Not Specified	::
dns-server3	DNS server 3.	ipv6-address	Not Specified	::
dns-server4	DNS server 4.	ipv6-address	Not Specified	::
domain	Domain name suffix for the IP addresses that the DHCP server assigns to clients.	string	Maximum length: 35	
subnet	Subnet or subnet-id if the IP mode is delegated.	ipv6-prefix	Not Specified	::/0
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15	
option1	Option 1.	user	Not Specified	
option2	Option 2.	user	Not Specified	
option3	Option 3.	user	Not Specified	
upstream-interface	Interface name from where delegated information is provided.	string	Maximum length: 15	
delegated-prefix-iaid	IAID of obtained delegated-prefix from the upstream interface.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip-mode	Method used to assign client IP.	option	-	range

Parameter	Description	Type	Size	Default
	Option / **Description** *range* / Use range defined by start IP/end IP to assign client IP. *delegated* / Use delegated prefix method to assign client IP.			
prefix-mode	Assigning a prefix from a DHCPv6 client or RA.	option	-	dhcp6
	Option / **Description** *dhcp6* / Use delegated prefix from a DHCPv6 client. *ra* / Use prefix from RA.			

config prefix-range

Parameter	Description	Type	Size	Default
start-prefix	Start of prefix range.	ipv6-address	Not Specified	::
end-prefix	End of prefix range.	ipv6-address	Not Specified	::
prefix-length	Prefix length.	integer	Minimum value: 1 Maximum value: 128	0

config ip-range

Parameter	Description	Type	Size	Default
start-ip	Start of IP range.	ipv6-address	Not Specified	::
end-ip	End of IP range.	ipv6-address	Not Specified	::

config system dhcp server

Configure DHCP servers.

```
config system dhcp server
    Description: Configure DHCP servers.
    edit <id>
        set status [disable|enable]
```

```
        set lease-time {integer}
        set mac-acl-default-action [assign|block]
        set forticlient-on-net-status [disable|enable]
        set dns-service [local|default|...]
        set dns-server1 {ipv4-address}
        set dns-server2 {ipv4-address}
        set dns-server3 {ipv4-address}
        set dns-server4 {ipv4-address}
        set wifi-ac-service [specify|local]
        set wifi-ac1 {ipv4-address}
        set wifi-ac2 {ipv4-address}
        set wifi-ac3 {ipv4-address}
        set ntp-service [local|default|...]
        set ntp-server1 {ipv4-address}
        set ntp-server2 {ipv4-address}
        set ntp-server3 {ipv4-address}
        set domain {string}
        set wins-server1 {ipv4-address}
        set wins-server2 {ipv4-address}
        set default-gateway {ipv4-address}
        set next-server {ipv4-address}
        set netmask {ipv4-netmask}
        set interface {string}
        config ip-range
            Description: DHCP IP range configuration.
            edit <id>
                set start-ip {ipv4-address}
                set end-ip {ipv4-address}
            next
        end
        set timezone-option [disable|default|...]
        set timezone [01|02|...]
        set tftp-server <tftp-server1>, <tftp-server2>, ...
        set filename {string}
        config options
            Description: DHCP options.
            edit <id>
                set code {integer}
                set type [hex|string|...]
                set value {string}
                set ip {user}
            next
        end
        set server-type [regular|ipsec]
        set ip-mode [range|usrgrp]
        set conflicted-ip-timeout {integer}
        set ipsec-lease-hold {integer}
        set auto-configuration [disable|enable]
        set dhcp-settings-from-fortiipam [disable|enable]
        set auto-managed-status [disable|enable]
        set ddns-update [disable|enable]
        set ddns-update-override [disable|enable]
        set ddns-server-ip {ipv4-address}
        set ddns-zone {string}
        set ddns-auth [disable|tsig]
        set ddns-keyname {string}
```

```
        set ddns-key {password_aes256}
        set ddns-ttl {integer}
        set vci-match [disable|enable]
        set vci-string <vci-string1>, <vci-string2>, ...
        config exclude-range
            Description: Exclude one or more ranges of IP addresses from being assigned to
clients.
            edit <id>
                set start-ip {ipv4-address}
                set end-ip {ipv4-address}
            next
        end
        config reserved-address
            Description: Options for the DHCP server to assign IP settings to specific MAC
addresses.
            edit <id>
                set type [mac|option82]
                set ip {ipv4-address}
                set mac {mac-address}
                set action [assign|block|...]
                set circuit-id-type [hex|string]
                set circuit-id {string}
                set remote-id-type [hex|string]
                set remote-id {string}
                set description {var-string}
            next
        end
    next
end
```

config system dhcp server

Parameter	Description	Type	Size	Default
status	Enable/disable this DHCP configuration.	option	-	enable
	Option / **Description** *disable* / Do not use this DHCP server configuration. *enable* / Use this DHCP server configuration.			
lease-time	Lease time in seconds, 0 means unlimited.	integer	Minimum value: 300 Maximum value: 8640000	604800
mac-acl-default-action	MAC access control default action (allow or block assigning IP settings).	option	-	assign

Parameter	Description	Type	Size	Default
	Option / **Description** *assign* — Allow the DHCP server to assign IP settings to clients on the MAC access control list. *block* — Block the DHCP server from assigning IP settings to clients on the MAC access control list.			
forticlient-on-net-status	Enable/disable FortiClient-On-Net service for this DHCP server.	option	-	enable
	Option / **Description** *disable* — Disable FortiClient On-Net Status. *enable* — Enable FortiClient On-Net Status.			
dns-service	Options for assigning DNS servers to DHCP clients.	option	-	specify
	Option / **Description** *local* — IP address of the interface the DHCP server is added to becomes the client's DNS server IP address. *default* — Clients are assigned the FortiProxy's configured DNS servers. *specify* — Specify up to 3 DNS servers in the DHCP server configuration.			
dns-server1	DNS server 1.	ipv4-address	Not Specified	0.0.0.0
dns-server2	DNS server 2.	ipv4-address	Not Specified	0.0.0.0
dns-server3	DNS server 3.	ipv4-address	Not Specified	0.0.0.0
dns-server4	DNS server 4.	ipv4-address	Not Specified	0.0.0.0
wifi-ac-service	Options for assigning WiFi access controllers to DHCP clients.	option	-	specify
	Option / **Description** *specify* — Specify up to 3 WiFi Access Controllers in the DHCP server configuration. *local* — IP address of the interface the DHCP server is added to becomes the client's WiFi Access Controller IP address.			
wifi-ac1	WiFi Access Controller 1 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
wifi-ac2	WiFi Access Controller 2 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified	0.0.0.0
wifi-ac3	WiFi Access Controller 3 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified	0.0.0.0
ntp-service	Options for assigning Network Time Protocol (NTP) servers to DHCP clients.	option	-	specify
	Option / **Description** *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 FortiProxy's configured NTP servers. *specify* — Specify up to 3 NTP servers in the DHCP server configuration.			
ntp-server1	NTP server 1.	ipv4-address	Not Specified	0.0.0.0
ntp-server2	NTP server 2.	ipv4-address	Not Specified	0.0.0.0
ntp-server3	NTP server 3.	ipv4-address	Not Specified	0.0.0.0
domain	Domain name suffix for the IP addresses that the DHCP server assigns to clients.	string	Maximum length: 35	
wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0
wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0
default-gateway	Default gateway IP address assigned by the DHCP server.	ipv4-address	Not Specified	0.0.0.0
next-server	IP address of a server (for example, a TFTP sever) that DHCP clients can download a boot file from.	ipv4-address	Not Specified	0.0.0.0
netmask	Netmask assigned by the DHCP server.	ipv4-netmask	Not Specified	0.0.0.0
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15	
timezone-option	Options for the DHCP server to set the client's time zone.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Do not set the client's time zone. *default* — Clients are assigned the FortiProxy's configured time zone. *specify* — Specify the time zone to be assigned to DHCP clients.			
timezone	Select the time zone to be assigned to DHCP clients.	option	-	00
	Option / **Description** *01* — (GMT-11:00) Midway Island, Samoa *02* — (GMT-10:00) Hawaii *03* — (GMT-9:00) Alaska *04* — (GMT-8:00) Pacific Time (US & Canada) *05* — (GMT-7:00) Arizona *81* — (GMT-7:00) Baja California Sur, Chihuahua *06* — (GMT-7:00) Mountain Time (US & Canada) *07* — (GMT-6:00) Central America *08* — (GMT-6:00) Central Time (US & Canada) *09* — (GMT-6:00) Mexico City *10* — (GMT-6:00) Saskatchewan *11* — (GMT-5:00) Bogota, Lima,Quito *12* — (GMT-5:00) Eastern Time (US & Canada) *13* — (GMT-5:00) Indiana (East) *74* — (GMT-4:00) Caracas *14* — (GMT-4:00) Atlantic Time (Canada) *77* — (GMT-4:00) Georgetown *15* — (GMT-4:00) La Paz *87* — (GMT-4:00) Paraguay *16* — (GMT-3:00) Santiago *17* — (GMT-3:30) Newfoundland *18* — (GMT-3:00) Brasilia *19* — (GMT-3:00) Buenos Aires			

Parameter	Description	Type	Size	Default

Option	Description
20	(GMT-3:00) Nuuk (Greenland)
75	(GMT-3:00) Uruguay
21	(GMT-2:00) Mid-Atlantic
22	(GMT-1:00) Azores
23	(GMT-1:00) Cape Verde Is.
24	(GMT) Monrovia
80	(GMT) Greenwich Mean Time
79	(GMT) Casablanca
25	(GMT) Dublin, Edinburgh, Lisbon, London, Canary Is.
26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris
78	(GMT+1:00) Namibia
29	(GMT+1:00) Sarajevo, Skopje, Warsaw, Zagreb
30	(GMT+1:00) West Central Africa
31	(GMT+2:00) Athens, Sofia, Vilnius
32	(GMT+2:00) Bucharest
33	(GMT+2:00) Cairo
34	(GMT+2:00) Harare, Pretoria
35	(GMT+2:00) Helsinki, Riga, Tallinn
36	(GMT+2:00) Jerusalem
37	(GMT+3:00) Baghdad
38	(GMT+3:00) Kuwait, Riyadh
83	(GMT+3:00) Moscow
84	(GMT+3:00) Minsk
40	(GMT+3:00) Nairobi
85	(GMT+3:00) Istanbul
41	(GMT+3:30) Tehran
42	(GMT+4:00) Abu Dhabi, Muscat

Parameter	Description	Type	Size	Default

Option	Description
43	(GMT+4:00) Baku
39	(GMT+3:00) St. Petersburg, Volgograd
44	(GMT+4:30) Kabul
46	(GMT+5:00) Islamabad, Karachi, Tashkent
47	(GMT+5:30) Kolkata, Chennai, Mumbai, New Delhi
51	(GMT+5:30) Sri 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

Parameter	Description	Type	Size	Default
	Option / **Description** *71* (GMT+12:00) Auckland, Wellington *72* (GMT+12:00) Fiji, Kamchatka, Marshall Is. *00* (GMT+12:00) Eniwetok, Kwajalein *82* (GMT+12:45) Chatham Islands *73* (GMT+13:00) Nuku'alofa *86* (GMT+13:00) Samoa *76* (GMT+14:00) Kiritimati			
tftp-server `<tftp-server>`	One or more hostnames or IP addresses of the TFTP servers in quotes separated by spaces. TFTP server.	string	Maximum length: 63	
filename	Name of the boot file on the TFTP server.	string	Maximum length: 127	
server-type	DHCP server can be a normal DHCP server or an IPsec DHCP server.	option	-	regular
	Option / **Description** *regular* Regular DHCP service. *ipsec* DHCP over IPsec service.			
ip-mode	Method used to assign client IP.	option	-	range
	Option / **Description** *range* Use range defined by start-ip/end-ip to assign client IP. *usrgrp* Use user-group defined method to assign client IP.			
conflicted-ip-timeout	Time in seconds to wait after a conflicted IP address is removed from the DHCP range before it can be reused.	integer	Minimum value: 60 Maximum value: 8640000	1800
ipsec-lease-hold	DHCP over IPsec leases expire this many seconds after tunnel down (0 to disable forced-expiry).	integer	Minimum value: 0 Maximum value: 8640000	60

Parameter	Description	Type	Size	Default
auto-configuration	Enable/disable auto configuration.	option	-	enable

Option	Description
disable	Disable auto configuration.
enable	Enable auto configuration.

Parameter	Description	Type	Size	Default
dhcp-settings-from-fortiipam	Enable/disable populating of DHCP server settings from FortiIPAM.	option	-	disable

Option	Description
disable	Disable populating of DHCP server settings from FortiIPAM.
enable	Enable populating of DHCP server settings from FortiIPAM.

Parameter	Description	Type	Size	Default
auto-managed-status	Enable/disable use of this DHCP server once this interface has been assigned an IP address from FortiIPAM.	option	-	enable

Option	Description
disable	Disable use of this DHCP server once this interface has been assigned an IP address from FortiIPAM.
enable	Enable use of this DHCP server once this interface has been assigned an IP address from FortiIPAM.

Parameter	Description	Type	Size	Default
ddns-update	Enable/disable DDNS update for DHCP.	option	-	disable

Option	Description
disable	Disable DDNS update for DHCP.
enable	Enable DDNS update for DHCP.

Parameter	Description	Type	Size	Default
ddns-update-override	Enable/disable DDNS update override for DHCP.	option	-	disable

Option	Description
disable	Disable DDNS update override for DHCP.
enable	Enable DDNS update override for DHCP.

Parameter	Description	Type	Size	Default
ddns-server-ip	DDNS server IP.	ipv4-address	Not Specified	0.0.0.0
ddns-zone	Zone of your domain name (ex. DDNS.com).	string	Maximum length: 64	

Parameter	Description	Type	Size	Default
ddns-auth	DDNS authentication mode.	option	-	disable
	Option / **Description** *disable* — Disable DDNS authentication. *tsig* — TSIG based on RFC2845.			
ddns-keyname	DDNS update key name.	string	Maximum length: 64	
ddns-key	DDNS update key (base 64 encoding).	password_aes256	Not Specified	
ddns-ttl	TTL.	integer	Minimum value: 60 Maximum value: 86400	300
vci-match	Enable/disable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI are served.	option	-	disable
	Option / **Description** *disable* — Disable VCI matching. *enable* — Enable VCI matching.			
vci-string `<vci-string>`	One or more VCI strings in quotes separated by spaces. VCI strings.	string	Maximum length: 255	

config ip-range

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

config options

Parameter	Description	Type	Size	Default
code	DHCP option code.	integer	Minimum value: 0 Maximum value: 255	0
type	DHCP option type.	option	-	hex

Option	Description
hex	DHCP option in hex.
string	DHCP option in string.
ip	DHCP option in IP.
fqdn	DHCP option in domain search option format.

value	DHCP option value.	string	Maximum length: 312	
ip	DHCP option IPs.	user	Not Specified	

config exclude-range

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

config reserved-address

Parameter	Description	Type	Size	Default
type	DHCP reserved-address type.	option	-	mac

Option	Description
mac	Match with MAC address.
option82	Match with DHCP option 82.

ip	IP address to be reserved for the MAC address.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
mac	MAC address of the client that will get the reserved IP address.	mac-address	Not Specified	00:00:00:00:00:00
action	Options for the DHCP server to configure the client with the reserved MAC address.	option	-	reserved
	Option / **Description** *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.			
circuit-id-type	DHCP option type.	option	-	string
	Option / **Description** *hex* — DHCP option in hex. *string* — DHCP option in string.			
circuit-id	Option 82 circuit-ID of the client that will get the reserved IP address.	string	Maximum length: 312	
remote-id-type	DHCP option type.	option	-	string
	Option / **Description** *hex* — DHCP option in hex. *string* — DHCP option in string.			
remote-id	Option 82 remote-ID of the client that will get the reserved IP address.	string	Maximum length: 312	
description	Description.	var-string	Maximum length: 255	

config system dns-database

Configure DNS databases.

```
config system dns-database
    Description: Configure DNS databases.
    edit <name>
        set status [enable|disable]
        set domain {string}
        set allow-transfer {user}
        set type [primary|secondary]
```

```
        set view [shadow|public]
        set ip-primary {ipv4-address-any}
        set primary-name {string}
        set contact {string}
        set ttl {integer}
        set authoritative [enable|disable]
        set forwarder {user}
        set source-ip {ipv4-address}
        set rr-max {integer}
        config dns-entry
            Description: DNS entry.
            edit <id>
                set status [enable|disable]
                set type [A|NS|...]
                set ttl {integer}
                set preference {integer}
                set ip {ipv4-address-any}
                set ipv6 {ipv6-address}
                set hostname {string}
                set canonical-name {string}
            next
        end
    next
end
```

config system dns-database

Parameter	Description	Type	Size	Default
status	Enable/disable this DNS zone.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
domain	Domain name.	string	Maximum length: 255	
allow-transfer	DNS zone transfer IP address list.	user	Not Specified	
type	Zone type (primary to manage entries directly, secondary to import entries from other zones).	option	-	primary
	Option / **Description** *primary* — Primary DNS zone, to manage entries directly. *secondary* — Secondary DNS zone, to import entries from other DNS zones.			
view	Zone view (public to serve public clients, shadow to serve internal clients).	option	-	shadow

Parameter	Description	Type	Size	Default
	Option / **Description** *shadow* — Shadow DNS zone to serve internal clients. *public* — Public DNS zone to serve public clients.			
ip-primary	IP address of primary DNS server. Entries in this primary DNS server and imported into the DNS zone.	ipv4-address-any	Not Specified	0.0.0.0
primary-name	Domain name of the default DNS server for this zone.	string	Maximum length: 255	dns
contact	Email address of the administrator for this zone. You can specify only the username, such as admin or the full email address, such as admin@test.com When using only a username, the domain of the email will be this zone.	string	Maximum length: 255	host
ttl	Default time-to-live value for the entries of this DNS zone .	integer	Minimum value: 0 Maximum value: 2147483647	86400
authoritative	Enable/disable authoritative zone.	option	-	enable
	Option / **Description** *enable* — Enable authoritative zone. *disable* — Disable authoritative zone.			
forwarder	DNS zone forwarder IP address list.	user	Not Specified	
source-ip	Source IP for forwarding to DNS server.	ipv4-address	Not Specified	0.0.0.0
rr-max	Maximum number of resource records .	integer	Minimum value: 10 Maximum value: 65536	16384

config dns-entry

Parameter	Description	Type	Size	Default
status	Enable/disable resource record status.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable resource record status. *disable* — Disable resource record status.			
type	Resource record type. **Option** / **Description** *A* — Host type. *NS* — Name server type. *CNAME* — Canonical name type. *MX* — Mail exchange type. *AAAA* — IPv6 host type. *PTR* — Pointer type. *PTR_V6* — IPv6 pointer type.	option	-	A
ttl	Time-to-live for this entry .	integer	Minimum value: 0 Maximum value: 2147483647	0
preference	DNS entry preference .	integer	Minimum value: 0 Maximum value: 65535	10
ip	IPv4 address of the host.	ipv4-address-any	Not Specified	0.0.0.0
ipv6	IPv6 address of the host.	ipv6-address	Not Specified	::
hostname	Name of the host.	string	Maximum length: 255	
canonical-name	Canonical name of the host.	string	Maximum length: 255	

config system dns-server

Configure DNS servers.

```
config system dns-server
    Description: Configure DNS servers.
    edit <name>
        set mode [recursive|non-recursive|...]
        set dnsfilter-profile {string}
        set doh [enable|disable]
    next
end
```

config system dns-server

Parameter	Description	Type	Size	Default
mode	DNS server mode.	option	-	recursive
	Option / **Description** *recursive* — Shadow DNS database and forward. *non-recursive* — Public DNS database only. *forward-only* — Forward only.			
dnsfilter-profile	DNS filter profile.	string	Maximum length: 35	
doh	DNS over HTTPS/443.	option	-	disable
	Option / **Description** *enable* — Enable DNS over HTTPS. *disable* — Disable DNS over HTTPS.			

config system dns

Configure DNS.

```
config system dns
    Description: Configure DNS.
    set primary {ipv4-address}
    set secondary {ipv4-address}
    set protocol {option1}, {option2}, ...
    set ssl-certificate {string}
    set server-hostname <hostname1>, <hostname2>, ...
    set domain <domain1>, <domain2>, ...
    set ip6-primary {ipv6-address}
    set ip6-secondary {ipv6-address}
    set timeout {integer}
    set retry {integer}
    set dns-cache-limit {integer}
    set dns-cache-ttl {integer}
```

```
    set cache-notfound-responses [disable|enable]
    set source-ip {ipv4-address}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
    set server-select-method [least-rtt|failover]
    set alt-primary {ipv4-address}
    set alt-secondary {ipv4-address}
    set log [disable|error|...]
end
```

config system dns

Parameter	Description	Type	Size	Default
primary	Primary DNS server IP address.	ipv4-address	Not Specified	0.0.0.0
secondary	Secondary DNS server IP address.	ipv4-address	Not Specified	0.0.0.0
protocol	DNS transport protocols.	option	-	cleartext
	Option / **Description** *cleartext* — DNS over UDP/53, DNS over TCP/53. *dot* — DNS over TLS/853. *doh* — DNS over HTTPS/443.			
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory
server-hostname <hostname>	DNS server host name list. DNS server host name list separated by space (maximum 4 domains).	string	Maximum length: 127	
domain <domain>	Search suffix list for hostname lookup. DNS search domain list separated by space (maximum 8 domains).	string	Maximum length: 127	
ip6-primary	Primary DNS server IPv6 address.	ipv6-address	Not Specified	::
ip6-secondary	Secondary DNS server IPv6 address.	ipv6-address	Not Specified	::
timeout	DNS query timeout interval in seconds .	integer	Minimum value: 1 Maximum value: 10	5

Parameter	Description	Type	Size	Default
retry	Number of times to retry .	integer	Minimum value: 0 Maximum value: 5	2
dns-cache-limit	Maximum number of records in the DNS cache.	integer	Minimum value: 0 Maximum value: 4294967295	5000
dns-cache-ttl	Duration in seconds that the DNS cache retains information.	integer	Minimum value: 60 Maximum value: 86400	1800
cache-notfound-responses	Enable/disable response from the DNS server when a record is not in cache.	option	-	disable
	Option / **Description** *disable* — Disable cache NOTFOUND responses from DNS server. *enable* — Enable cache NOTFOUND responses from DNS server.			
source-ip	IP address used by the DNS server as its source IP.	ipv4-address	Not Specified	0.0.0.0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
server-select-method	Specify how configured servers are prioritized.	option	-	least-rtt
	Option / **Description** *least-rtt* — Select servers based on least round trip time. *failover* — Select servers based on the order they are configured.			

Parameter	Description	Type	Size	Default
alt-primary	Alternate primary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0
alt-secondary	Alternate secondary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0
log	Local DNS log setting.	option	-	disable

Option	Description
disable	Disable.
error	Enable local DNS error log.
all	Enable local DNS log.

config system dscp-based-priority

Configure DSCP based priority table.

```
config system dscp-based-priority
    Description: Configure DSCP based priority table.
    edit <id>
        set ds {integer}
        set priority [low|medium|...]
    next
end
```

config system dscp-based-priority

Parameter	Description	Type	Size	Default
ds	DSCP.	integer	Minimum value: 0 Maximum value: 63	0
priority	DSCP based priority level.	option	-	high

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

config system email-server

Configure the email server used by the FortiProxy various things. For example, for sending email messages to users to support user authentication features.

```
config system email-server
    Description: Configure the email server used by the FortiProxy various things. For
example, for sending email messages to users to support user authentication features.
    set type {option}
    set reply-to {string}
    set server {string}
    set port {integer}
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set authenticate [enable|disable]
    set validate-server [enable|disable]
    set username {string}
    set password {password}
    set security [none|starttls|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config system email-server

Parameter	Description	Type	Size	Default
type	Use FortiGuard Message service or custom email server.	option	-	custom
	Option **Description** *custom* Use custom email server.			
reply-to	Reply-To email address.	string	Maximum length: 63	
server	SMTP server IP address or hostname.	string	Maximum length: 63	
port	SMTP server port.	integer	Minimum value: 1 Maximum value: 65535	25
source-ip	SMTP server IPv4 source IP.	ipv4-address	Not Specified	0.0.0.0
source-ip6	SMTP server IPv6 source IP.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default
authenticate	Enable/disable authentication.	option	-	disable
	Option / **Description** *enable* — Enable authentication. *disable* — Disable authentication.			
validate-server	Enable/disable validation of server certificate.	option	-	disable
	Option / **Description** *enable* — Enable validation of server certificate. *disable* — Disable validation of server certificate.			
username	SMTP server user name for authentication.	string	Maximum length: 63	
password	SMTP server user password for authentication.	password	Not Specified	
security	Connection security used by the email server.	option	-	none
	Option / **Description** *none* — None. *starttls* — STARTTLS. *smtps* — SSL/TLS.			
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically.			

Parameter	Description	Type	Size	Default
	Option: *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. Option: *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config system external-resource

Configure external resource.

```
config system external-resource
    Description: Configure external resource.
    edit <name>
        set uuid {uuid}
        set status [enable|disable]
        set type [category|address|...]
        set category {integer}
        set username {string}
        set password {password}
        set comments {var-string}
        set resource {string}
        set user-agent {var-string}
        set proxy {string}
        set proxy-port {integer}
        set proxy-username {string}
        set proxy-password {password}
        set server-identity-check [none|basic|...]
        set refresh-rate {integer}
        set source-ip {ipv4-address}
        set interface-select-method [auto|sdwan|...]
        set interface {string}
    next
end
```

config system external-resource

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
status	Enable/disable user resource.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable user resource. *disable* / Disable user resource.			
type	User resource type.	option	-	category
	Option / **Description** *category* / FortiGuard category. *address* / Firewall IP address. *domain* / Domain Name. *malware* / Malware hash. *url* / URL List.			
category	User resource category.	integer	Minimum value: 192 Maximum value: 221	0
username	HTTP basic authentication user name.	string	Maximum length: 64	
password	HTTP basic authentication password.	password	Not Specified	
comments	Comment.	var-string	Maximum length: 255	
resource	URI of external resource.	string	Maximum length: 511	
user-agent	HTTP User-Agent header .	var-string	Maximum length: 255	
proxy	Proxy server host(ip or domain name).	string	Maximum length: 255	
proxy-port	Port number that the proxy server expects to receive HTTP sessions on .	integer	Minimum value: 1 Maximum value: 65535	8080
proxy-username	HTTP proxy basic authentication user name.	string	Maximum length: 64	
proxy-password	HTTP proxy basic authentication password.	password	Not Specified	

Parameter	Description	Type	Size	Default
server-identity-check	Certificate verification option.	option	-	none
	Option / **Description** *none* — No certificate verification. *basic* — Check server certifcate only. *full* — Check server certificate and domain match server certificate.			
refresh-rate	Time interval to refresh external resource .	integer	Minimum value: 1 Maximum value: 43200	5
source-ip	Source IPv4 address used to communicate with server.	ipv4-address	Not Specified	0.0.0.0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config system federated-upgrade

Coordinate federated upgrades within the Security Fabric.

```
config system federated-upgrade
    Description: Coordinate federated upgrades within the Security Fabric.
    set status [disabled|initialized|...]
    set failure-reason [none|internal|...]
    set failure-device {string}
    set upgrade-id {integer}
    set next-path-index {integer}
    config node-list
        Description: Nodes which will be included in the upgrade.
        edit <serial>
            set timing [immediate|scheduled]
            set time {user}
            set setup-time {user}
```

```
            set upgrade-path {user}
            set device-type [fortiproxy|fortiswitch|...]
            set coordinating-fortiproxy {string}
        next
    end
end
```

config system federated-upgrade

Parameter	Description	Type	Size	Default
status	Current status of the upgrade.	option	-	disabled

Option	Description
disabled	No federated upgrade has been configured.
initialized	The upgrade has been configured.
downloading	The image is downloading in preparation for the upgrade.
device-disconnected	The image downloads are complete, but one or more devices have disconnected.
ready	The image download finished and the upgrade is pending.
staging	The upgrade is confirmed and images are being staged.
final-check	The upgrade is ready and final checks are in progress.
upgrade-devices	The upgrade is ready and devices are being rebooted.
cancelled	The upgrade was cancelled due to the tree not being ready.
confirmed	The upgrade was confirmed and reboots are running.
done	The upgrade completed successfully.
failed	The upgrade failed due to a local issue.

failure-reason	Reason for upgrade failure.	option	-	none

Option	Description
none	No failure.
internal	An internal error occurred.
timeout	The upgrade timed out.
device-type-unsupported	The device type was not supported by the FortiGate.
download-failed	The image could not be downloaded.
device-missing	The device was disconnected from the FortiGate.

Parameter	Description	Type	Size	Default
	Option / **Description** *version-unavailable* — An image matching the device and version could not be found. *staging-failed* — The image could not be pushed to the device. *reboot-failed* — The device could not be rebooted. *device-not-reconnected* — The device did not reconnect after rebooting. *node-not-ready* — A device in the CSF tree was not ready. *no-final-confirmation* — The coordinating FortiGate did not confirm the upgrade. *no-confirmation-query* — A downstream FortiGate did not initiate final confirmation.			
failure-device	Serial number of the node to include.	string	Maximum length: 79	
upgrade-id	Unique identifier for this upgrade.	integer	Minimum value: 0 Maximum value: 4294967295	0
next-path-index	The index of the next image to upgrade to.	integer	Minimum value: 0 Maximum value: 10	0

config node-list

Parameter	Description	Type	Size	Default
timing	Whether the upgrade should be run immediately, or at a scheduled time.	option	-	immediate
	Option / **Description** *immediate* — Begin the upgrade immediately. *scheduled* — Begin the upgrade at a configured time.			
time	Scheduled time for the upgrade. Format hh:mm yyyy/mm/dd UTC.	user	Not Specified	
setup-time	When the upgrade was configured. Format hh:mm yyyy/mm/dd UTC.	user	Not Specified	

Parameter	Description	Type	Size	Default
upgrade-path	Image IDs to upgrade through.	user	Not Specified	
device-type	What type of device this node represents.	option	-	fortiproxy

Option	Description
fortiproxy	This device is a FortiProxy.
fortiswitch	This device is a FortiSwitch.
fortiap	This device is a FortiAP.

coordinating-fortiproxy	Serial number of the FortiProxy that controls this device	string	Maximum length: 79	

config system fips-cc

Configure FIPS-CC mode.

```
config system fips-cc
    Description: Configure FIPS-CC mode.
    set entropy-token [enable|disable|...]
    set self-test-period {integer}
    set key-generation-self-test [enable|disable]
end
```

config system fips-cc

Parameter	Description	Type	Size	Default
entropy-token	Enable/disable/dynamic entropy token.	option	-	enable

Option	Description
enable	Enable entropy token to be present during boot process.
disable	Disable entropy token to be present during boot process.
dynamic	Dynamic detect entropy token to be present during boot process.

self-test-period	Self test period.	integer	Minimum value: 1 Maximum value: 1440	1440

Parameter	Description	Type	Size	Default
key-generation-self-test	Enable/disable self tests after key generation.	option	-	disable

Option	Description
enable	Enable self tests after key generation.
disable	Disable self tests after key generation.

config system fortianalyzer-connectivity

FortiAnalyzer Connectivity.

```
config system fortianalyzer-connectivity
    Description: FortiAnalyzer Connectivity.
end
```

config system fortiguard-log-service

Configuration of FortiCloud log service.

```
config system fortiguard-log-service
    Description: Configuration of FortiCloud log service.
end
```

config system fortiguard-service

Configuration of FortiGuard services.

```
config system fortiguard-service
    Description: Configuration of FortiGuard services.
end
```

config system fortiguard

Configure FortiGuard services.

```
config system fortiguard
    Description: Configure FortiGuard services.
    set fortiguard-anycast [enable|disable]
    set fortiguard-anycast-source [fortinet|aws|...]
```

```
    set protocol [udp|http|...]
    set port [8888|53|...]
    set load-balance-servers {integer}
    set auto-join-forticloud [enable|disable]
    set update-server-location [automatic|usa|...]
    set sandbox-region {string}
    set update-ffdb [enable|disable]
    set update-uwdb [enable|disable]
    set update-extdb [enable|disable]
    set update-build-proxy [enable|disable]
    set persistent-connection [enable|disable]
    set antispam-force-off [enable|disable]
    set antispam-cache [enable|disable]
    set antispam-cache-ttl {integer}
    set antispam-cache-mpercent {integer}
    set antispam-license {integer}
    set antispam-expiration {integer}
    set antispam-timeout {integer}
    set outbreak-prevention-force-off [enable|disable]
    set outbreak-prevention-cache [enable|disable]
    set outbreak-prevention-cache-ttl {integer}
    set outbreak-prevention-cache-mpercent {integer}
    set outbreak-prevention-license {integer}
    set outbreak-prevention-expiration {integer}
    set outbreak-prevention-timeout {integer}
    set ia-license {integer}
    set ia-expiration {integer}
    set fnbi-license {integer}
    set fnbi-expiration {integer}
    set webfilter-force-off [enable|disable]
    set webfilter-cache [enable|disable]
    set webfilter-cache-ttl {integer}
    set webfilter-license {integer}
    set webfilter-expiration {integer}
    set webfilter-timeout {integer}
    set sdns-server-ip {user}
    set sdns-server-port {integer}
    set anycast-sdns-server-ip {ipv4-address}
    set anycast-sdns-server-port {integer}
    set sdns-options {option1}, {option2}, ...
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set proxy-server-ip {ipv4-address}
    set proxy-server-port {integer}
    set proxy-username {string}
    set proxy-password {password}
    set videofilter-license {integer}
    set videofilter-expiration {integer}
    set ddns-server-ip {ipv4-address}
    set ddns-server-ip6 {ipv6-address}
    set ddns-server-port {integer}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config system fortiguard

Parameter	Description	Type	Size	Default
fortiguard-anycast	Enable/disable use of FortiGuard's Anycast network.	option	-	disable

Option	Description
enable	Enable use of FortiGuard's Anycast network.
disable	Disable use of FortiGuard's Anycast network.

Parameter	Description	Type	Size	Default
fortiguard-anycast-source	Configure which of Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network. Default is Fortinet.	option	-	fortinet

Option	Description
fortinet	Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network.
aws	Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network.
debug	Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.

Parameter	Description	Type	Size	Default
protocol	Protocol used to communicate with the FortiGuard servers.	option	-	https

Option	Description
udp	UDP for server communication (for use by FortiGuard or FortiManager).
http	HTTP for server communication (for use only by FortiManager).
https	HTTPS for server communication (for use by FortiGuard or FortiManager).

Parameter	Description	Type	Size	Default
port	Port used to communicate with the FortiGuard servers.	option	-	443

Option	Description
8888	port 8888 for server communication.
53	port 53 for server communication.
80	port 80 for server communication.
443	port 443 for server communication.

Parameter	Description	Type	Size	Default
load-balance-servers	Number of servers to alternate between as first FortiGuard option.	integer	Minimum value: 1 Maximum value: 266	1
auto-join-forticloud	Automatically connect to and login to FortiCloud.	option	-	disable

Option	Description
enable	Enable automatic connection and login to FortiCloud.
disable	Disable automatic connection and login to FortiCloud.

Parameter	Description	Type	Size	Default
update-server-location	Location from which to receive FortiGuard updates.	option	-	automatic

Option	Description
automatic	FortiGuard servers chosen based on closest proximity to FortiProxy unit.
usa	FortiGuard servers in United States.
eu	FortiGuard servers in the European Union.

Parameter	Description	Type	Size	Default
sandbox-region	Cloud sandbox region.	string	Maximum length: 63	
update-ffdb	Enable/disable Internet Service Database update.	option	-	enable

Option	Description
enable	Enable Internet Service Database update.
disable	Disable Internet Service Database update.

Parameter	Description	Type	Size	Default
update-uwdb	Enable/disable allowlist update.	option	-	enable

Option	Description
enable	Enable allowlist update.
disable	Disable allowlist update.

Parameter	Description	Type	Size	Default
update-extdb	Enable/disable external resource update.	option	-	enable

Option	Description
enable	Enable external resource update.
disable	Disable external resource update.

Parameter	Description	Type	Size	Default
update-build-proxy	Enable/disable proxy dictionary rebuild.	option	-	enable

Option	Description
enable	Enable proxy dictionary rebuild.
disable	Disable proxy dictionary rebuild.

Parameter	Description	Type	Size	Default
persistent-connection	Enable/disable use of persistent connection to receive update notification from FortiGuard.	option	-	disable

Option	Description
enable	Enable persistent connection to receive update notification from FortiGuard.
disable	Disable persistent connection to receive update notification from FortiGuard.

Parameter	Description	Type	Size	Default
antispam-force-off	Enable/disable turning off the FortiGuard antispam service.	option	-	disable

Option	Description
enable	Turn off the FortiGuard antispam service.
disable	Allow the FortiGuard antispam service.

Parameter	Description	Type	Size	Default
antispam-cache	Enable/disable FortiGuard antispam request caching. Uses a small amount of memory but improves performance.	option	-	enable

Option	Description
enable	Enable FortiGuard antispam request caching.
disable	Disable FortiGuard antispam request caching.

Parameter	Description	Type	Size	Default
antispam-cache-ttl	Time-to-live for antispam cache entries in seconds . Lower times reduce the cache size. Higher times may improve performance since the cache will have more entries.	integer	Minimum value: 300 Maximum value: 86400	1800
antispam-cache-mpercent	Maximum percent of FortiProxy memory the antispam cache is allowed to use .	integer	Minimum value: 1 Maximum value: 15	2
antispam-license	Interval of time between license checks for the FortiGuard antispam contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295

Parameter	Description	Type	Size	Default
antispam-expiration	Expiration date of the FortiGuard antispam contract.	integer	Minimum value: 0 Maximum value: 4294967295	0
antispam-timeout	Antispam query time out .	integer	Minimum value: 1 Maximum value: 30	7
outbreak-prevention-force-off	Turn off FortiGuard Virus Outbreak Prevention service.	option	-	disable

Option	Description
enable	Turn off FortiGuard antivirus service.
disable	Allow the FortiGuard antivirus service.

outbreak-prevention-cache	Enable/disable FortiGuard Virus Outbreak Prevention cache.	option	-	enable

Option	Description
enable	Enable FortiGuard antivirus caching.
disable	Disable FortiGuard antivirus caching.

outbreak-prevention-cache-ttl	Time-to-live for FortiGuard Virus Outbreak Prevention cache entries .	integer	Minimum value: 300 Maximum value: 86400	300
outbreak-prevention-cache-mpercent	Maximum percent of memory FortiGuard Virus Outbreak Prevention cache can use .	integer	Minimum value: 1 Maximum value: 15	2
outbreak-prevention-license	Interval of time between license checks for FortiGuard Virus Outbreak Prevention contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295

Parameter	Description	Type	Size	Default
outbreak-prevention-expiration	Expiration date of FortiGuard Virus Outbreak Prevention contract.	integer	Minimum value: 0 Maximum value: 4294967295	0
outbreak-prevention-timeout	FortiGuard Virus Outbreak Prevention time out .	integer	Minimum value: 1 Maximum value: 30	7
ia-license	License type.	integer	Minimum value: 0 Maximum value: 4294967295	0
ia-expiration	License expiration.	integer	Minimum value: 0 Maximum value: 4294967295	0
fnbi-license	License type.	integer	Minimum value: 0 Maximum value: 4294967295	0
fnbi-expiration	License expiration.	integer	Minimum value: 0 Maximum value: 4294967295	0
webfilter-force-off	Enable/disable turning off the FortiGuard web filtering service.	option	-	disable

Option	Description
enable	Turn off the FortiGuard web filtering service.
disable	Allow the FortiGuard web filtering service to operate.

webfilter-cache	Enable/disable FortiGuard web filter caching.	option	-	enable

Option	Description
enable	Enable FortiGuard web filter caching.

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* / Disable FortiGuard web filter caching.			
webfilter-cache-ttl	Time-to-live for web filter cache entries in seconds .	integer	Minimum value: 300 Maximum value: 86400	3600
webfilter-license	Interval of time between license checks for the FortiGuard web filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295
webfilter-expiration	Expiration date of the FortiGuard web filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	0
webfilter-timeout	Web filter query time out .	integer	Minimum value: 1 Maximum value: 30	15
sdns-server-ip	IP address of the FortiGuard DNS rating server.	user	Not Specified	
sdns-server-port	Port to connect to on the FortiGuard DNS rating server.	integer	Minimum value: 1 Maximum value: 65535	53
anycast-sdns-server-ip	IP address of the FortiGuard anycast DNS rating server.	ipv4-address	Not Specified	0.0.0.0
anycast-sdns-server-port	Port to connect to on the FortiGuard anycast DNS rating server.	integer	Minimum value: 1 Maximum value: 65535	853
sdns-options	Customization options for the FortiGuard DNS service.	option	-	
	Option / **Description** *include-question-section* / Include DNS question section in the FortiGuard DNS setup message.			

Parameter	Description	Type	Size	Default
source-ip	Source IPv4 address used to communicate with FortiGuard.	ipv4-address	Not Specified	0.0.0.0
source-ip6	Source IPv6 address used to communicate with FortiGuard.	ipv6-address	Not Specified	::
proxy-server-ip	IP address of the proxy server.	ipv4-address	Not Specified	0.0.0.0
proxy-server-port	Port used to communicate with the proxy server.	integer	Minimum value: 0 Maximum value: 65535	0
proxy-username	Proxy user name.	string	Maximum length: 64	
proxy-password	Proxy user password.	password	Not Specified	
videofilter-license	Interval of time between license checks for the FortiGuard video filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295
videofilter-expiration	Expiration date of the FortiGuard video filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	0
ddns-server-ip	IP address of the FortiDDNS server.	ipv4-address	Not Specified	0.0.0.0
ddns-server-ip6	IPv6 address of the FortiDDNS server.	ipv6-address	Not Specified	::
ddns-server-port	Port used to communicate with FortiDDNS servers.	integer	Minimum value: 1 Maximum value: 65535	443
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	Set outgoing interface manually.

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

config system fortindr

Configure FortiNDR.

```
config system fortindr
    Description: Configure FortiNDR.
    set status [disable|enable]
    set source-ip {string}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config system fortindr

Parameter	Description	Type	Size	Default
status	Enable/disable FortiNDR.	option	-	disable
	Option / **Description** *disable* — Disable FortiNDR. *enable* — Enable FortiNDR.			
source-ip	Source IP address for communications to FortiNDR.	string	Maximum length: 63	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config system fortisandbox

Configure FortiSandbox.

```
config system fortisandbox
    Description: Configure FortiSandbox.
    set status [enable|disable]
    set forticloud [enable|disable]
    set server {string}
    set source-ip {string}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
    set enc-algorithm [default|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set email {string}
end
```

config system fortisandbox

Parameter	Description	Type	Size	Default
status	Enable/disable FortiSandbox.	option	-	disable
	Option / **Description** *enable* — Enable FortiSandbox. *disable* — Disable FortiSandbox.			
forticloud	Enable/disable FortiSandbox Cloud.	option	-	disable
	Option / **Description** *enable* — Enable FortiSandbox Cloud. *disable* — Disable FortiSandbox Cloud.			
server	Server address of the remote FortiSandbox.	string	Maximum length: 63	
source-ip	Source IP address for communications to FortiSandbox.	string	Maximum length: 63	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			

Parameter	Description	Type	Size	Default
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
enc-algorithm	Configure the level of SSL protection for secure communication with FortiSandbox.	option	-	low

Option	Description
default	SSL communication with high and medium encryption algorithms.
high	SSL communication with high encryption algorithms.
low	SSL communication with low encryption algorithms.

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

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.

Parameter	Description	Type	Size	Default
email	Notifier email address.	string	Maximum length: 63	

config system fsso-polling

Configure Fortinet Single Sign On (FSSO) server.

```
config system fsso-polling
    Description: Configure Fortinet Single Sign On (FSSO) server.
    set status [enable|disable]
    set listening-port {integer}
    set authentication [enable|disable]
    set auth-password {password}
end
```

config system fsso-polling

Parameter	Description	Type	Size	Default
status	Enable/disable FSSO Polling Mode.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable FSSO Polling Mode. *disable* / Disable FSSO Polling Mode.			
listening-port	Listening port to accept clients .	integer	Minimum value: 1 Maximum value: 65535	8000
authentication	Enable/disable FSSO Agent Authentication.	option	-	disable
	Option / **Description** *enable* / Enable FSSO Agent Authentication. *disable* / Disable FSSO Agent Authentication.			
auth-password	Password to connect to FSSO Agent.	password	Not Specified	

config system ftm-push

Configure FortiToken Mobile push services.

```
config system ftm-push
    Description: Configure FortiToken Mobile push services.
    set server-port {integer}
    set server-cert {string}
    set server-ip {ipv4-address}
    set server {string}
    set status [enable|disable]
end
```

config system ftm-push

Parameter	Description	Type	Size	Default
server-port	Port to communicate with FortiToken Mobile push services server .	integer	Minimum value: 1 Maximum value: 65535	4433

Parameter	Description	Type	Size	Default
server-cert	Name of the server certificate to be used for SSL .	string	Maximum length: 35	self-sign
server-ip	IPv4 address of FortiToken Mobile push services server (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
server	IPv4 address or domain name of FortiToken Mobile push services server.	string	Maximum length: 127	
status	Enable/disable the use of FortiToken Mobile push services.	option	-	disable

Option	Description
enable	Enable FortiToken Mobile push services.
disable	Disable FortiToken Mobile push services.

config system geoip-country

Define geoip country name-ID table.

```
config system geoip-country
    Description: Define geoip country name-ID table.
    edit <id>
        set name {string}
    next
end
```

config system geoip-country

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

config system geoip-override

Configure geographical location mapping for IP address(es) to override mappings from FortiGuard.

```
config system geoip-override
    Description: Configure geographical location mapping for IP address(es) to override
mappings from FortiGuard.
    edit <name>
        set description {string}
        set country-id {string}
```

```
        config ip-range
            Description: Table of IP ranges assigned to country.
            edit <id>
                set start-ip {ipv4-address}
                set end-ip {ipv4-address}
            next
        end
        config ip6-range
            Description: Table of IPv6 ranges assigned to country.
            edit <id>
                set start-ip {ipv6-address}
                set end-ip {ipv6-address}
            next
        end
    next
end
```

config system geoip-override

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	
country-id	Two character Country ID code.	string	Maximum length: 2	

config ip-range

Parameter	Description	Type	Size	Default
start-ip	Starting IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
end-ip	Ending IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0

config ip6-range

Parameter	Description	Type	Size	Default
start-ip	Starting IP address, inclusive, of the address range (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::
end-ip	Ending IP address, inclusive, of the address range (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::

config system global

Configure global attributes.

```
config system global
    Description: Configure global attributes.
    set language [english|french|...]
    set gui-ipv6 [enable|disable]
    set gui-replacement-message-groups [enable|disable]
    set gui-local-out [enable|disable]
    set gui-certificates [enable|disable]
    set gui-custom-language [enable|disable]
    set gui-display-hostname [enable|disable]
    set gui-fortigate-cloud-sandbox [enable|disable]
    set gui-firmware-upgrade-warning [enable|disable]
    set gui-allow-default-hostname [enable|disable]
    set gui-forticare-registration-setup-warning [enable|disable]
    set gui-cdn-usage [enable|disable]
    set admin-https-ssl-versions {option1}, {option2}, ...
    set admin-https-ssl-ciphersuites {option1}, {option2}, ...
    set admin-https-ssl-banned-ciphers {option1}, {option2}, ...
    set admin-timeout {integer}
    set admin-console-timeout {integer}
    set ssd-trim-freq [never|hourly|...]
    set ssd-trim-hour {integer}
    set ssd-trim-min {integer}
    set ssd-trim-weekday [sunday|monday|...]
    set ssd-trim-date {integer}
    set admin-concurrent [enable|disable]
    set admin-lockout-threshold {integer}
    set admin-lockout-duration {integer}
    set refresh {integer}
    set interval {integer}
    set failtime {integer}
    set daily-restart [enable|disable]
    set restart-time {user}
    set radius-port {integer}
    set admin-login-max {integer}
    set remoteauthtimeout {integer}
    set ldapconntimeout {integer}
    set batch-cmdb [enable|disable]
    set multi-factor-authentication [optional|mandatory]
    set ssl-min-proto-version [SSLv3|TLSv1|...]
    set autorun-log-fsck [enable|disable]
    set dst [enable|disable]
    set timezone [01|02|...]
    set traffic-priority [tos|dscp]
    set traffic-priority-level [low|medium|...]
    set anti-replay [disable|loose|...]
    set pmtu-discovery [enable|disable]
    set revision-image-auto-backup [enable|disable]
    set revision-backup-on-logout [enable|disable]
    set management-vdom {string}
    set hostname {string}
    set alias {string}
```

```
set strong-crypto [enable|disable]
set ssl-static-key-ciphers [enable|disable]
set ssh-kex-algo {option1}, {option2}, ...
set ssh-enc-algo {option1}, {option2}, ...
set ssh-mac-algo {option1}, {option2}, ...
set snat-route-change [enable|disable]
set speedtest-server [enable|disable]
set cli-audit-log [enable|disable]
set dh-params [1024|1536|...]
set fds-statistics [enable|disable]
set fds-statistics-period {integer}
set tcp-option [enable|disable]
set lldp-transmission [enable|disable]
set lldp-reception [enable|disable]
set proxy-auth-timeout {integer}
set resigned-pkey-period {integer}
set proxy-keep-alive-mode [session|traffic|...]
set proxy-re-authentication-time {integer}
set proxy-auth-lifetime [enable|disable]
set proxy-auth-lifetime-timeout {integer}
set proxy-auth-machine-timeout {integer}
set proxy-resource-mode [enable|disable]
set proxy-cert-use-mgmt-vdom [enable|disable]
set update-tls-finger-print [enable|disable]
set sys-perf-log-interval {integer}
set check-protocol-header [loose|strict]
set vip-arp-range [unlimited|restricted]
set tcp-halfclose-timer {integer}
set tcp-halfopen-timer {integer}
set tcp-timewait-timer {integer}
set tcp-rst-timer {integer}
set udp-idle-timer {integer}
set block-session-timer {integer}
set ip-src-port-range {user}
set pre-login-banner [enable|disable]
set post-login-banner [disable|enable]
set tftp [enable|disable]
set av-failopen [pass|off|...]
set av-failopen-session [enable|disable]
set memory-use-threshold-extreme {integer}
set memory-use-threshold-red {integer}
set memory-use-threshold-green {integer}
set cpu-use-threshold {integer}
set check-reset-range [strict|disable]
set admin-port {integer}
set admin-sport {integer}
set admin-host {string}
set admin-ssh-password [enable|disable]
set admin-restrict-local [enable|disable]
set admin-ssh-port {integer}
set admin-ssh-grace-time {integer}
set admin-ssh-v1 [enable|disable]
set admin-telnet [enable|disable]
set admin-telnet-port {integer}
set admin-forticloud-sso-login [enable|disable]
set default-service-source-port {user}
```

```
    set admin-maintainer [enable|disable]
    set admin-server-cert {string}
    set user-server-cert {string}
    set admin-https-pki-required [enable|disable]
    set auth-http-port {integer}
    set auth-https-port {integer}
    set auth-keepalive [enable|disable]
    set policy-auth-concurrent {integer}
    set auth-session-limit [block-new|logout-inactive]
    set auth-cert {string}
    set clt-cert-req [enable|disable]
    set fortiservice-port {integer}
    set cfg-save [automatic|manual|...]
    set cfg-revert-timeout {integer}
    set reboot-upon-config-restore [enable|disable]
    set admin-scp [enable|disable]
    set security-rating-result-submission [enable|disable]
    set security-rating-run-on-schedule [enable|disable]
    set fortiextender-data-port {integer}
    set fortiextender [disable|enable]
    set extender-controller-reserved-network {ipv4-classnet-host}
    set fortiextender-discovery-lockdown [disable|enable]
    set dnsproxy-worker-count {integer}
    set url-filter-count {integer}
    set proxy-worker-count {integer}
    set scanunit-count {integer}
    set fgd-alert-subscription {option1}, {option2}, ...
    set ipv6-accept-dad {integer}
    set ipv6-allow-multicast-probe [enable|disable]
    set ipv6-allow-local-in-slient-drop [enable|disable]
    set csr-ca-attribute [enable|disable]
    set wimax-4g-usb [enable|disable]
    set cert-chain-max {integer}
    set sslvpn-max-worker-count {integer}
    set sslvpn-ems-sn-check [enable|disable]
    set sslvpn-plugin-version-check [enable|disable]
    set two-factor-ftk-expiry {integer}
    set two-factor-email-expiry {integer}
    set two-factor-sms-expiry {integer}
    set two-factor-fac-expiry {integer}
    set two-factor-ftm-expiry {integer}
    set max-img-cache-size {integer}
    set img-cache-mode [stop|rolling]
    set per-user-bal [enable|disable]
    set wad-worker-count {integer}
    set wad-csvc-cs-count {integer}
    set wad-csvc-db-count {integer}
    set http-view [enable|disable]
    set wad-source-affinity [disable|enable]
    set wad-memory-change-granularity {integer}
    set login-timestamp [enable|disable]
    set miglogd-children {integer}
    set special-file-23-support [disable|enable]
    set log-uuid-address [enable|disable]
    set log-ssl-connection [enable|disable]
    set gui-rest-api-cache [enable|disable]
```

```
    set gui-fortiguard-resource-fetch [enable|disable]
    set arp-max-entry {integer}
    set ha-affinity {string}
    set cmdbsvr-affinity {string}
    set av-affinity {string}
    set wad-affinity {string}
    set ips-affinity {string}
    set miglog-affinity {string}
    set url-filter-affinity {string}
    set ndp-max-entry {integer}
    set br-fdb-max-entry {integer}
    set max-route-cache-size {integer}
    set ipsec-round-robin [enable|disable]
    set ipsec-soft-dec-async [enable|disable]
    set device-idle-timeout {integer}
    set user-device-store-max-devices {integer}
    set user-device-store-max-users {integer}
    set user-device-store-max-unified-mem {integer}
    set gui-device-latitude {string}
    set gui-device-longitude {string}
    set private-data-encryption [disable|enable]
    set auto-auth-extension-device [enable|disable]
    set gui-theme [jade|neutrino|...]
    set gui-date-format [yyyy/MM/dd|dd/MM/yyyy|...]
    set gui-date-time-source [system|browser]
    set igmp-state-limit {integer}
    set cloud-communication [enable|disable]
    set ipsec-ha-seqjump-rate {integer}
    set fortitoken-cloud [enable|disable]
    set faz-disk-buffer-size {integer}
    set irq-time-accounting [auto|force]
    set management-ip {string}
    set management-port {integer}
    set management-port-use-admin-sport [enable|disable]
    set internet-service-database [mini|standard|...]
    set license-overlimit [bypass|block]
    set max-session-per-user {integer}
    set conntrack {integer}
    set established-timeout {integer}
    set time-wait-timeout {integer}
    set fin-wait-timeout {integer}
    set close-wait-timeout {integer}
    set syn-sent-timeout {integer}
    set syn-recv-timeout {integer}
    set last-ack-timeout {integer}
    set udp-timeout {integer}
    set udp-stream-timeout {integer}
end
```

config system global

Parameter	Description	Type	Size	Default
language	GUI display language.	option	-	english

Option	Description
english	English.
french	French.
spanish	Spanish.
portuguese	Portuguese.
japanese	Japanese.
trach	Traditional Chinese.
simch	Simplified Chinese.
korean	Korean.

Parameter	Description	Type	Size	Default
gui-ipv6	Enable/disable IPv6 settings on the GUI.	option	-	enable

Option	Description
enable	Display the feature in GUI.
disable	Do not display the feature in GUI.

Parameter	Description	Type	Size	Default
gui-replacement-message-groups	Enable/disable replacement message groups on the GUI.	option	-	disable

Option	Description
enable	Display the feature in GUI.
disable	Do not display the feature in GUI.

Parameter	Description	Type	Size	Default
gui-local-out	Enable/disable Local-out traffic on the GUI.	option	-	disable

Option	Description
enable	Display the feature in GUI.
disable	Do not display the feature in GUI.

Parameter	Description	Type	Size	Default
gui-certificates	Enable/disable the System > Certificate GUI page, allowing you to add and configure certificates from the GUI.	option	-	enable

Option	Description
enable	Display the feature in GUI.
disable	Do not display the feature in GUI.

Parameter	Description	Type	Size	Default
gui-custom-language	Enable/disable custom languages in GUI.	option	-	disable

Option	Description
enable	Display the feature in GUI.
disable	Do not display the feature in GUI.

Parameter	Description	Type	Size	Default
gui-display-hostname	Enable/disable displaying the FortiProxy's hostname on the GUI login page.	option	-	disable

Option	Description
enable	Display the feature in GUI.
disable	Do not display the feature in GUI.

Parameter	Description	Type	Size	Default
gui-fortigate-cloud-sandbox	Enable/disable displaying FortiProxy Cloud Sandbox on the GUI.	option	-	disable

Option	Description
enable	Display the feature in GUI.
disable	Do not display the feature in GUI.

Parameter	Description	Type	Size	Default
gui-firmware-upgrade-warning	Enable/disable the firmware upgrade warning on the GUI.	option	-	enable

Option	Description
enable	Display the feature in GUI.

Parameter	Description	Type	Size	Default
	Option **Description** *disable* Do not display the feature in GUI.			
gui-allow-default-hostname	Enable/disable the factory default hostname warning on the GUI setup wizard.	option	-	disable
	Option **Description** *enable* Display the feature in GUI. *disable* Do not display the feature in GUI.			
gui-forticare-registration-setup-warning	Enable/disable the FortiCare registration setup warning on the GUI.	option	-	enable
	Option **Description** *enable* Display the feature in GUI. *disable* Do not display the feature in GUI.			
gui-cdn-usage	Enable/disable Load GUI static files from a CDN.	option	-	enable
	Option **Description** *enable* Display the feature in GUI. *disable* Do not display the feature in GUI.			
admin-https-ssl-versions	Allowed TLS versions for web administration.	option	-	tlsv1-2
	Option **Description** *tlsv1-1* TLS 1.1. *tlsv1-2* TLS 1.2. *tlsv1-3* TLS 1.3.			

Parameter	Description	Type	Size	Default
admin-https-ssl-ciphersuites	Select one or more TLS 1.3 ciphersuites to enable. Does not affect ciphers in TLS 1.2 and below. At least one must be enabled. To disable all, remove TLS1.3 from admin-https-ssl-versions.	option	-	TLS-AES-128-GCM-SHA256 TLS-AES-256-GCM-SHA384 TLS-CHACHA20-POLY1305-SHA256

Option	Description
TLS-AES-128-GCM-SHA256	Enable TLS-AES-128-GCM-SHA256 in TLS 1.3.
TLS-AES-256-GCM-SHA384	Enable TLS-AES-256-GCM-SHA384 in TLS 1.3.
TLS-CHACHA20-POLY1305-SHA256	Enable TLS-CHACHA20-POLY1305-SHA256 in TLS 1.3.
TLS-AES-128-CCM-SHA256	Enable TLS-AES-128-CCM-SHA256 in TLS 1.3.
TLS-AES-128-CCM-8-SHA256	Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.

Parameter	Description	Type	Size	Default
admin-https-ssl-banned-ciphers	Select one or more cipher technologies that cannot be used in GUI HTTPS negotiations. Only applies to TLS 1.2 and below.	option	-	

Option	Description
RSA	Ban the use of cipher suites using RSA key.
DHE	Ban the use of cipher suites using authenticated ephemeral DH key agreement.
ECDHE	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.
DSS	Ban the use of cipher suites using DSS authentication.
ECDSA	Ban the use of cipher suites using ECDSA authentication.

Parameter	Description	Type	Size	Default
	Option / **Description** *AES* — Ban the use of cipher suites using either 128 or 256 bit AES. *AESGCM* — Ban the use of cipher suites using AES in Galois Counter Mode (GCM). *CAMELLIA* — Ban the use of cipher suites using either 128 or 256 bit CAMELLIA. *3DES* — Ban the use of cipher suites using triple DES. *SHA1* — Ban the use of cipher suites using HMAC-SHA1. *SHA256* — Ban the use of cipher suites using HMAC-SHA256. *SHA384* — Ban the use of cipher suites using HMAC-SHA384. *STATIC* — Ban the use of cipher suites using static keys. *CHACHA20* — Ban the use of cipher suites using ChaCha20. *ARIA* — Ban the use of cipher suites using ARIA. *AESCCM* — Ban the use of cipher suites using AESCCM.			
admin-timeout	Number of minutes before an idle administrator session times out . A shorter idle timeout is more secure.	integer	Minimum value: 1 Maximum value: 480	5
admin-console-timeout	Console login timeout that overrides the admin timeout value .	integer	Minimum value: 15 Maximum value: 300	0
ssd-trim-freq	How often to run SSD Trim . SSD Trim prevents SSD drive data loss by finding and isolating errors.	option	-	weekly
	Option / **Description** *never* — Never Run SSD Trim. *hourly* — Run SSD Trim Hourly. *daily* — Run SSD Trim Daily. *weekly* — Run SSD Trim Weekly. *monthly* — Run SSD Trim Monthly.			
ssd-trim-hour	Hour of the day on which to run SSD Trim .	integer	Minimum value: 0 Maximum value: 23	1

Parameter	Description	Type	Size	Default
ssd-trim-min	Minute of the hour on which to run SSD Trim .	integer	Minimum value: 0 Maximum value: 60	60
ssd-trim-weekday	Day of week to run SSD Trim.	option	-	sunday

Option	Description
sunday	Sunday
monday	Monday
tuesday	Tuesday
wednesday	Wednesday
thursday	Thursday
friday	Friday
saturday	Saturday

ssd-trim-date	Date within a month to run ssd trim.	integer	Minimum value: 1 Maximum value: 31	1
admin-concurrent	Enable/disable concurrent administrator logins. Use policy-auth-concurrent for firewall authenticated users.	option	-	enable

Option	Description
enable	Enable admin concurrent login.
disable	Disable admin concurrent login.

admin-lockout-threshold	Number of failed login attempts before an administrator account is locked out for the admin-lockout-duration.	integer	Minimum value: 1 Maximum value: 10	3
admin-lockout-duration	Amount of time in seconds that an administrator account is locked out after reaching the admin-lockout-threshold for repeated failed login attempts.	integer	Minimum value: 1 Maximum value: 2147483647	60

Parameter	Description	Type	Size	Default
refresh	Statistics refresh interval second(s) in GUI.	integer	Minimum value: 0 Maximum value: 4294967295	0
interval	Dead gateway detection interval.	integer	Minimum value: 0 Maximum value: 4294967295	5
failtime	Fail-time for server lost.	integer	Minimum value: 0 Maximum value: 4294967295	5
daily-restart	Enable/disable daily restart of FortiProxy unit. Use the restart-time option to set the time of day for the restart.	option	-	disable
	Option / **Description** *enable* — Enable daily reboot of the FortiProxy. *disable* — Disable daily reboot of the FortiProxy.			
restart-time	Daily restart time (hh:mm).	user	Not Specified	
radius-port	RADIUS service port number.	integer	Minimum value: 1 Maximum value: 65535	1812
admin-login-max	Maximum number of administrators who can be logged in at the same time .	integer	Minimum value: 1 Maximum value: 100	100
remoteauthtimeout	Number of seconds that the FortiProxy waits for responses from remote RADIUS, LDAP, or TACACS+ authentication servers. .	integer	Minimum value: 1 Maximum value: 300	5
ldapconntimeout	Global timeout for connections with remote LDAP servers in milliseconds .	integer	Minimum value: 1 Maximum value: 300000	500

Parameter	Description	Type	Size	Default
batch-cmdb	Enable/disable batch mode, allowing you to enter a series of CLI commands that will execute as a group once they are loaded.	option	-	enable

Option	Description
enable	Enable batch mode to execute in CMDB server.
disable	Disable batch mode to execute in CMDB server.

Parameter	Description	Type	Size	Default
multi-factor-authentication	Enforce all login methods to require an additional authentication factor .	option	-	optional

Option	Description
optional	Do not enforce all login methods to require an additional authentication factor (controlled by user settings).
mandatory	Enforce all login methods to require an additional authentication factor.

Parameter	Description	Type	Size	Default
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	SSLv3

Option	Description
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.
TLSv1-3	TLSv1.3.

Parameter	Description	Type	Size	Default
autorun-log-fsck	Enable/disable automatic log partition check after ungraceful shutdown.	option	-	disable

Option	Description
enable	Enable automatic log partition check after ungraceful shutdown.
disable	Disable automatic log partition check after ungraceful shutdown.

Parameter	Description	Type	Size	Default
dst	Enable/disable daylight saving time.	option	-	enable

Option	Description
enable	Enable daylight saving time.
disable	Disable daylight saving time.

Parameter	Description	Type	Size	Default
timezone	Number corresponding to your time zone from 00 to 86. Enter set timezone ? to view the list of time zones and the numbers that represent them.	option	-	00

Option	Description
01	(GMT-11:00) Midway Island, Samoa
02	(GMT-10:00) Hawaii
03	(GMT-9:00) Alaska
04	(GMT-8:00) Pacific Time (US & Canada)
05	(GMT-7:00) Arizona
81	(GMT-7:00) Baja California Sur, Chihuahua
06	(GMT-7:00) Mountain Time (US & Canada)
07	(GMT-6:00) Central America
08	(GMT-6:00) Central Time (US & Canada)
09	(GMT-6:00) Mexico City
10	(GMT-6:00) Saskatchewan
11	(GMT-5:00) Bogota, Lima,Quito
12	(GMT-5:00) Eastern Time (US & Canada)
13	(GMT-5:00) Indiana (East)
74	(GMT-4:00) Caracas
14	(GMT-4:00) Atlantic Time (Canada)
77	(GMT-4:00) Georgetown
15	(GMT-4:00) La Paz
87	(GMT-4:00) Paraguay

Parameter	Description	Type	Size	Default

Option	Description
16	(GMT-3:00) Santiago
17	(GMT-3:30) Newfoundland
18	(GMT-3:00) Brasilia
19	(GMT-3:00) Buenos Aires
20	(GMT-3:00) Nuuk (Greenland)
75	(GMT-3:00) Uruguay
21	(GMT-2:00) Mid-Atlantic
22	(GMT-1:00) Azores
23	(GMT-1:00) Cape Verde Is.
24	(GMT) Monrovia
80	(GMT) Greenwich Mean Time
79	(GMT) Casablanca
25	(GMT) Dublin, Edinburgh, Lisbon, London, Canary Is.
26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris
78	(GMT+1:00) Namibia
29	(GMT+1:00) Sarajevo, Skopje, Warsaw, Zagreb
30	(GMT+1:00) West Central Africa
31	(GMT+2:00) Athens, Sofia, Vilnius
32	(GMT+2:00) Bucharest
33	(GMT+2:00) Cairo
34	(GMT+2:00) Harare, Pretoria
35	(GMT+2:00) Helsinki, Riga, Tallinn
36	(GMT+2:00) Jerusalem
37	(GMT+3:00) Baghdad
38	(GMT+3:00) Kuwait, Riyadh
83	(GMT+3:00) Moscow
84	(GMT+3:00) Minsk

Parameter	Description	Type	Size	Default

Option	Description
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

Parameter	Description	Type	Size	Default
	Option / **Description** *67* (GMT+10:00) Hobart *68* (GMT+10:00) Vladivostok *69* (GMT+10:00) Magadan *70* (GMT+11:00) Solomon Is., New Caledonia *71* (GMT+12:00) Auckland, Wellington *72* (GMT+12:00) Fiji, Kamchatka, Marshall Is. *00* (GMT+12:00) Eniwetok, Kwajalein *82* (GMT+12:45) Chatham Islands *73* (GMT+13:00) Nuku'alofa *86* (GMT+13:00) Samoa *76* (GMT+14:00) Kiritimati			
traffic-priority	Choose Type of Service (ToS) or Differentiated Services Code Point (DSCP) for traffic prioritization in traffic shaping.	option	-	tos
	Option / **Description** *tos* IP TOS. *dscp* DSCP (DiffServ) DS.			
traffic-priority-level	Default system-wide level of priority for traffic prioritization.	option	-	medium
	Option / **Description** *low* Low priority. *medium* Medium priority. *high* High priority.			
anti-replay	Level of checking for packet replay and TCP sequence checking.	option	-	strict

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Disable anti-replay check. *loose* — Loose anti-replay check. *strict* — Strict anti-replay check.			
pmtu-discovery	Enable/disable path MTU discovery.	option	-	disable
	Option / **Description** *enable* — Enable path MTU discovery. *disable* — Disable path MTU discovery.			
revision-image-auto-backup	Enable/disable back-up of the latest image revision after the firmware is upgraded.	option	-	disable
	Option / **Description** *enable* — Enable revision image backup automatically when upgrading image. *disable* — Disable revision image backup automatically when upgrading image.			
revision-backup-on-logout	Enable/disable back-up of the latest configuration revision when an administrator logs out of the CLI or GUI.	option	-	disable
	Option / **Description** *enable* — Enable revision config backup automatically when logout. *disable* — Disable revision config backup automatically when logout.			
management-vdom	Management virtual domain name.	string	Maximum length: 31	root

Parameter	Description	Type	Size	Default
hostname	FortiProxy unit's hostname. Most models will truncate names longer than 24 characters. Some models support hostnames up to 35 characters.	string	Maximum length: 35	
alias	Alias for your FortiProxy unit.	string	Maximum length: 35	
strong-crypto	Enable to use strong encryption and only allow strong ciphers and digest for HTTPS/SSH/TLS/SSL functions.	option	-	disable

Option	Description
enable	Enable strong crypto for HTTPS/SSH/TLS/SSL.
disable	Disable strong crypto for HTTPS/SSH/TLS/SSL.

ssl-static-key-ciphers	Enable/disable static key ciphers in SSL/TLS connections (e.g. AES128-SHA, AES256-SHA, AES128-SHA256, AES256-SHA256).	option	-	enable

Option	Description
enable	Enable static key ciphers in SSL/TLS connections.
disable	Disable static key ciphers in SSL/TLS connections.

ssh-kex-algo	Select one or more SSH kex algorithms.	option	-	diffie-hellman-group14-sha1 diffie-hellman-group-exchange-sha1 diffie-hellman-group-exchange-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521

Parameter	Description	Type	Size	Default
	Option / **Description** *diffie-hellman-group1-sha1* / diffie-hellman-group1-sha1 *diffie-hellman-group14-sha1* / diffie-hellman-group14-sha1 *diffie-hellman-group-exchange-sha1* / diffie-hellman-group-exchange-sha1 *diffie-hellman-group-exchange-sha256* / diffie-hellman-group-exchange-sha256 *curve25519-sha256@libssh.org* / curve25519-sha256@libssh.org *ecdh-sha2-nistp256* / ecdh-sha2-nistp256 *ecdh-sha2-nistp384* / ecdh-sha2-nistp384 *ecdh-sha2-nistp521* / ecdh-sha2-nistp521			
ssh-enc-algo	Select one or more SSH ciphers.	option	-	chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr arcfour256 arcfour128 aes128-cbc 3des-cbc blowfish-cbc cast128-cbc aes192-cbc aes256-cbc arcfour rijndael-cbc@lysator.liu.se aes128-gcm@openssh.com aes256-gcm@openssh.com
	Option / **Description** *chacha20-poly1305@openssh.com* / chacha20-poly1305@openssh.com *aes128-ctr* / aes128-ctr *aes192-ctr* / aes192-ctr *aes256-ctr* / aes256-ctr *arcfour256* / arcfour256 *arcfour128* / arcfour128 *aes128-cbc* / aes128-cbc *3des-cbc* / 3des-cbc			

Parameter	Description	Type	Size	Default
	Option / **Description** *blowfish-cbc* / blowfish-cbc *cast128-cbc* / cast128-cbc *aes192-cbc* / aes192-cbc *aes256-cbc* / aes256-cbc *arcfour* / arcfour *rijndael-cbc@lysator.liu.se* / rijndael-cbc@lysator.liu.se *aes128-gcm@openssh.com* / aes128-gcm@openssh.com *aes256-gcm@openssh.com* / aes256-gcm@openssh.com			
ssh-mac-algo	Select one or more SSH MAC algorithms.	option	-	hmac-md5 hmac-md5-etm@openssh.com hmac-md5-96 hmac-md5-96-etm@openssh.com hmac-sha1 hmac-sha1-etm@openssh.com hmac-sha2-256 hmac-sha2-256-etm@openssh.com hmac-sha2-512 hmac-sha2-512-etm@openssh.com hmac-ripemd160 hmac-ripemd160@openssh.com hmac-ripemd160-etm@openssh.com umac-64@openssh.com umac-128@openssh.com umac-64-etm@openssh.com umac-128-etm@openssh.com
	Option / **Description** *hmac-md5* / hmac-md5 *hmac-md5-etm@openssh.com* / hmac-md5-etm@openssh.com *hmac-md5-96* / hmac-md5-96 *hmac-md5-96-etm@openssh.com* / hmac-md5-96-etm@openssh.com			

Parameter	Description	Type	Size	Default
	Option / **Description** *hmac-sha1* — hmac-sha1 *hmac-sha1-etm@openssh.com* — hmac-sha1-etm@openssh.com *hmac-sha2-256* — hmac-sha2-256 *hmac-sha2-256-etm@openssh.com* — hmac-sha2-256-etm@openssh.com *hmac-sha2-512* — hmac-sha2-512 *hmac-sha2-512-etm@openssh.com* — hmac-sha2-512-etm@openssh.com *hmac-ripemd160* — hmac-ripemd160 *hmac-ripemd160@openssh.com* — hmac-ripemd160@openssh.com *hmac-ripemd160-etm@openssh.com* — hmac-ripemd160-etm@openssh.com *umac-64@openssh.com* — umac-64@openssh.com *umac-128@openssh.com* — umac-128@openssh.com *umac-64-etm@openssh.com* — umac-64-etm@openssh.com *umac-128-etm@openssh.com* — umac-128-etm@openssh.com			
snat-route-change	Enable/disable the ability to change the static NAT route.	option	-	disable
	Option / **Description** *enable* — Enable SNAT route change. *disable* — Disable SNAT route change.			
speedtest-server	Enable/disable speed test server.	option	-	disable
	Option / **Description** *enable* — Enable speed test server service. *disable* — Disable speed test server service.			

Parameter	Description	Type	Size	Default
cli-audit-log	Enable/disable CLI audit log.	option	-	disable

Option	Description
enable	Enable CLI audit log.
disable	Disable CLI audit log.

Parameter	Description	Type	Size	Default
dh-params	Number of bits to use in the Diffie-Hellman exchange for HTTPS/SSH protocols.	option	-	2048

Option	Description
1024	1024 bits.
1536	1536 bits.
2048	2048 bits.
3072	3072 bits.
4096	4096 bits.
6144	6144 bits.
8192	8192 bits.

Parameter	Description	Type	Size	Default
fds-statistics	Enable/disable sending IPS, Application Control, and AntiVirus data to FortiGuard. This data is used to improve FortiGuard services and is not shared with external parties and is protected by Fortinet's privacy policy.	option	-	enable

Option	Description
enable	Enable FortiGuard statistics.
disable	Disable FortiGuard statistics.

Parameter	Description	Type	Size	Default
fds-statistics-period	FortiGuard statistics collection period in minutes. .	integer	Minimum value: 1 Maximum value: 1440	60

Parameter	Description	Type	Size	Default
tcp-option	Enable SACK, timestamp and MSS TCP options.	option	-	enable

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

Parameter	Description	Type	Size	Default
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission.	option	-	disable

Option	Description
enable	Enable transmission of Link Layer Discovery Protocol (LLDP).
disable	Disable transmission of Link Layer Discovery Protocol (LLDP).

Parameter	Description	Type	Size	Default
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception.	option	-	disable

Option	Description
enable	Enable reception of Link Layer Discovery Protocol (LLDP).
disable	Disable reception of Link Layer Discovery Protocol (LLDP).

Parameter	Description	Type	Size	Default
proxy-auth-timeout	Authentication timeout in minutes for authenticated users .	integer	Minimum value: 1 Maximum value: 600	10
resigned-pkey-period	Resigned cert private key regeration period in hours.	integer	Minimum value: 0 Maximum value: 600	0
proxy-keep-alive-mode	Control if users must re-authenticate after a session is closed, traffic has been idle, or from the point at which the user was first created.	option	-	session

Option	Description
session	Proxy keep-alive timeout begins at the closure of the session.

Parameter	Description	Type	Size	Default
	Option / **Description** *traffic* — Proxy keep-alive timeout begins after traffic has not been received. *re-authentication* — Proxy keep-alive timeout begins when the user was authenticated.			
proxy-re-authentication-time	The time limit that users must re-authenticate if proxy-keep-alive-mode is set to re-authenticate (1 - 86400 sec, default=30s.	integer	Minimum value: 1 Maximum value: 86400	30
proxy-auth-lifetime	Enable/disable authenticated users lifetime control. This is a cap on the total time a proxy user can be authenticated for after which re-authentication will take place.	option	-	disable
	Option / **Description** *enable* — Enable authenticated users lifetime control. *disable* — Disable authenticated users lifetime control.			
proxy-auth-lifetime-timeout	Lifetime timeout in minutes for authenticated users .	integer	Minimum value: 5 Maximum value: 65535	480
proxy-auth-machine-timeout	Machine account timeout in seconds for authenticated machines .	integer	Minimum value: 5 Maximum value: 30	15
proxy-resource-mode	Enable/disable use of the maximum memory usage on the FortiProxy unit's proxy processing of resources, such as block lists, allow lists, and external resources.	option	-	disable
	Option / **Description** *enable* — Enable use of the maximum memory usage. *disable* — Disable use of the maximum memory usage.			

Parameter	Description	Type	Size	Default
proxy-cert-use-mgmt-vdom	Enable/disable using management VDOM to send requests.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
update-tls-finger-print	Enable/disable update TLS fingerprint when deep-inspection is enabled.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
sys-perf-log-interval	Time in minutes between updates of performance statistics logging. .	integer	Minimum value: 0 Maximum value: 15	5
check-protocol-header	Level of checking performed on protocol headers. Strict checking is more thorough but may affect performance. Loose checking is OK in most cases.	option	-	loose

Option	Description
loose	Check protocol header loosely.
strict	Check protocol header strictly.

Parameter	Description	Type	Size	Default
vip-arp-range	Controls the number of ARPs that the FortiProxy sends for a Virtual IP (VIP) address range.	option	-	restricted

Option	Description
unlimited	Send ARPs for all addresses in VIP range.
restricted	Send ARPs for the first 8192 addresses in VIP range.

Parameter	Description	Type	Size	Default
tcp-halfclose-timer	Number of seconds the FortiProxy unit should wait to close a session after one peer has sent a FIN packet but the other has not responded .	integer	Minimum value: 1 Maximum value: 86400	120
tcp-halfopen-timer	Number of seconds the FortiProxy unit should wait to close a session after one peer has sent an open session packet but the other has not responded .	integer	Minimum value: 1 Maximum value: 86400	10
tcp-timewait-timer	Length of the TCP TIME-WAIT state in seconds .	integer	Minimum value: 0 Maximum value: 300	1
tcp-rst-timer	Length of the TCP CLOSE state in seconds .	integer	Minimum value: 5 Maximum value: 300	5
udp-idle-timer	UDP connection session timeout. This command can be useful in managing CPU and memory resources .	integer	Minimum value: 1 Maximum value: 86400	180
block-session-timer	Duration in seconds for blocked sessions .	integer	Minimum value: 1 Maximum value: 300	30
ip-src-port-range	IP source port range used for traffic originating from the FortiProxy unit.	user	Not Specified	1024-65001
pre-login-banner	Enable/disable displaying the administrator access disclaimer message on the login page before an administrator logs in.	option	-	disable

Option	Description
enable	Enable pre-login banner.
disable	Disable pre-login banner.

Parameter	Description	Type	Size	Default
post-login-banner	Enable/disable displaying the administrator access disclaimer message after an administrator successfully logs in.	option	-	disable

Option	Description
disable	Disable post-login banner.
enable	Enable post-login banner.

Parameter	Description	Type	Size	Default
tftp	Enable/disable TFTP.	option	-	enable

Option	Description
enable	Enable TFTP.
disable	Disable TFTP.

Parameter	Description	Type	Size	Default
av-failopen	Set the action to take if the FortiProxy is running low on memory or the proxy connection limit has been reached.	option	-	pass

Option	Description
pass	Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.
off	Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.
one-shot	Bypass the antivirus system when memory is low.

Parameter	Description	Type	Size	Default
av-failopen-session	When enabled and a proxy for a protocol runs out of room in its session table, that protocol goes into failopen mode and enacts the action specified by av-failopen.	option	-	disable

Option	Description
enable	Enable AV fail open session option.
disable	Disable AV fail open session option.

Parameter	Description	Type	Size	Default
memory-use-threshold-extreme	Threshold at which memory usage is considered extreme .	integer	Minimum value: 70 Maximum value: 97	95
memory-use-threshold-red	Threshold at which memory usage forces the FortiProxy to enter conserve mode .	integer	Minimum value: 70 Maximum value: 97	88
memory-use-threshold-green	Threshold at which memory usage forces the FortiProxy to exit conserve mode .	integer	Minimum value: 70 Maximum value: 97	82
cpu-use-threshold	Threshold at which CPU usage is reported .	integer	Minimum value: 50 Maximum value: 99	90
check-reset-range	Configure ICMP error message verification. You can either apply strict RST range checking or disable it.	option	-	disable

Option	Description
strict	Check RST range strictly.
disable	Disable RST range check.

admin-port	Administrative access port for HTTP. .	integer	Minimum value: 1 Maximum value: 65535	80
admin-sport	Administrative access port for HTTPS. .	integer	Minimum value: 1 Maximum value: 65535	443
admin-host	Administrative host for HTTP and HTTPS. When set, will be used in lieu of the client's Host header for any redirection.	string	Maximum length: 255	
admin-ssh-password	Enable/disable password authentication for SSH admin access.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable password authentication for SSH admin access. *disable* — Disable password authentication for SSH admin access.			
admin-restrict-local	Enable/disable local admin authentication restriction when remote authenticator is up and running .	option	-	disable
	Option / **Description** *enable* — Enable local admin authentication restriction. *disable* — Disable local admin authentication restriction.			
admin-ssh-port	Administrative access port for SSH. .	integer	Minimum value: 1 Maximum value: 65535	22
admin-ssh-grace-time	Maximum time in seconds permitted between making an SSH connection to the FortiProxy unit and authenticating .	integer	Minimum value: 10 Maximum value: 3600	120
admin-ssh-v1	Enable/disable SSH v1 compatibility.	option	-	disable
	Option / **Description** *enable* — Enable SSH v1 compatibility. *disable* — Disable SSH v1 compatibility.			
admin-telnet	Enable/disable TELNET service.	option	-	enable
	Option / **Description** *enable* — Enable TELNET service. *disable* — Disable TELNET service.			
admin-telnet-port	Administrative access port for TELNET. .	integer	Minimum value: 1 Maximum value: 65535	23

Parameter	Description	Type	Size	Default
admin-forticloud-sso-login	Enable/disable FortiCloud admin login via SSO.	option	-	disable
	Option / **Description** *enable* — Enable FortiCloud admin login via SSO. *disable* — Disable FortiCloud admin login via SSO.			
default-service-source-port	Default service source port range .	user	Not Specified	
admin-maintainer	Enable/disable maintainer administrator login. When enabled, the maintainer account can be used to log in from the console after a hard reboot. The password is "bcpb" followed by the FortiProxy unit serial number. You have limited time to complete this login.	option	-	enable
	Option / **Description** *enable* — Enable login for special user (maintainer). *disable* — Disable login for special user (maintainer).			
admin-server-cert	Server certificate that the FortiProxy uses for HTTPS administrative connections.	string	Maximum length: 35	self-sign
user-server-cert	Certificate to use for https user authentication.	string	Maximum length: 35	self-sign
admin-https-pki-required	Enable/disable admin login method. Enable to force administrators to provide a valid certificate to log in if PKI is enabled. Disable to allow administrators to log in with a certificate or password.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access. *disable* / Admin users can login by providing a valid certificate or password.			
auth-http-port	User authentication HTTP port. .	integer	Minimum value: 1 Maximum value: 65535	1000
auth-https-port	User authentication HTTPS port. .	integer	Minimum value: 1 Maximum value: 65535	1003
auth-keepalive	Enable to prevent user authentication sessions from timing out when idle.	option	-	disable
	Option / **Description** *enable* / Enable use of keep alive to extend authentication. *disable* / Disable use of keep alive to extend authentication.			
policy-auth-concurrent	Number of concurrent firewall use logins from the same user .	integer	Minimum value: 0 Maximum value: 100	0
auth-session-limit	Action to take when the number of allowed user authenticated sessions is reached.	option	-	block-new
	Option / **Description** *block-new* / Block new user authentication attempts. *logout-inactive* / Logout the most inactive user authenticated sessions.			
auth-cert	Server certificate that the FortiProxy uses for HTTPS firewall authentication connections.	string	Maximum length: 35	self-sign

Parameter	Description	Type	Size	Default
clt-cert-req	Enable/disable requiring administrators to have a client certificate to log into the GUI using HTTPS.	option	-	disable

Option	Description
enable	Enable require client certificate for GUI login.
disable	Disable require client certificate for GUI login.

fortiservice-port	FortiService port . Used by FortiClient endpoint compliance. Older versions of FortiClient used a different port.	integer	Minimum value: 1 Maximum value: 65535	8013
cfg-save	Configuration file save mode for CLI changes.	option	-	automatic

Option	Description
automatic	Automatically save config.
manual	Manually save config.
revert	Manually save config and revert the config when timeout.

cfg-revert-timeout	Time-out for reverting to the last saved configuration. .	integer	Minimum value: 10 Maximum value: 4294967295	600
reboot-upon-config-restore	Enable/disable reboot of system upon restoring configuration.	option	-	enable

Option	Description
enable	Enable reboot of system upon restoring configuration.
disable	Disable reboot of system upon restoring configuration.

admin-scp	Enable/disable using SCP to download the system configuration. You can use SCP as an alternative method for backing up the configuration.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable allow system configuration download by SCP. *disable* — Disable allow system configuration download by SCP.			
security-rating-result-submission	Enable/disable the submission of Security Rating results to FortiGuard.	option	-	enable
	Option / **Description** *enable* — Enable submission of Security Rating results to FortiGuard. *disable* — Disable submission of Security Rating results to FortiGuard.			
security-rating-run-on-schedule	Enable/disable scheduled runs of Security Rating.	option	-	enable
	Option / **Description** *enable* — Enable scheduled runs of Security Rating. *disable* — Disable scheduled runs of Security Rating.			
fortiextender-data-port	FortiExtender data port .	integer	Minimum value: 1024 Maximum value: 49150	25246
fortiextender	Enable/disable FortiExtender.	option	-	disable
	Option / **Description** *disable* — Disable FortiExtender controller. *enable* — Enable FortiExtender controller.			
extender-controller-reserved-network	Configure reserved network subnet for managed LAN extension FortiExtender units. This is available when the FortiExtender daemon is running.	ipv4-classnet-host	Not Specified	10.252.0.1 255.255.0.0
fortiextender-discovery-lockdown	Enable/disable FortiExtender CAPWAP lockdown.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Unlock down new FortiExtender device discovery. *enable* — Lock down new FortiExtender device discovery.			
dnsproxy-worker-count	DNS proxy worker count. For a FortiGate with multiple logical CPUs, you can set the DNS process number from 1 to the number of logical CPUs.	integer	Minimum value: 1 Maximum value: 2	1
url-filter-count	URL filter daemon count.	integer	Minimum value: 1 Maximum value: 1	1
proxy-worker-count	Proxy worker count.	integer	Minimum value: 1 Maximum value: 2	0
scanunit-count	Number of scanunits. The range and the default depend on the number of CPUs. Only available on FortiProxy units with multiple CPUs.	integer	Minimum value: 2 Maximum value: 2	0
fgd-alert-subscription	Type of alert to retrieve from FortiGuard.	option	-	
	Option / **Description** *advisory* — Retrieve FortiGuard advisories, report and news alerts. *latest-threat* — Retrieve latest FortiGuard threats alerts. *latest-virus* — Retrieve latest FortiGuard virus alerts. *latest-attack* — Retrieve latest FortiGuard attack alerts. *new-antivirus-db* — Retrieve FortiGuard AV database release alerts. *new-attack-db* — Retrieve FortiGuard IPS database release alerts.			
ipv6-accept-dad	Enable/disable acceptance of IPv6 Duplicate Address Detection (DAD).	integer	Minimum value: 0 Maximum value: 2	1

Parameter	Description	Type	Size	Default
ipv6-allow-multicast-probe	Enable/disable IPv6 address probe through Multicast.	option	-	disable

Option	Description
enable	Enable probing of IPv6 address space through Multicast.
disable	Disable probing of IPv6 address space through Multicast.

Parameter	Description	Type	Size	Default
ipv6-allow-local-in-slient-drop	Enable/disable silent drop of IPv6 local-in traffic.	option	-	enable

Option	Description
enable	Enable slient drop of IPv6 local-in traffic.
disable	Disable slient drop of IPv6 local-in traffic.

Parameter	Description	Type	Size	Default
csr-ca-attribute	Enable/disable the CA attribute in certificates. Some CA servers reject CSRs that have the CA attribute.	option	-	enable

Option	Description
enable	Enable CA attribute in CSR.
disable	Disable CA attribute in CSR.

Parameter	Description	Type	Size	Default
wimax-4g-usb	Enable/disable comparability with WiMAX 4G USB devices.	option	-	disable

Option	Description
enable	Enable WiMax 4G.
disable	Disable WiMax 4G.

Parameter	Description	Type	Size	Default
cert-chain-max	Maximum number of certificates that can be traversed in a certificate chain.	integer	Minimum value: 1 Maximum value: 2147483647	8

Parameter	Description	Type	Size	Default
sslvpn-max-worker-count	Maximum number of SSL-VPN processes. Upper limit for this value is the number of CPUs and depends on the model. Default value of zero means the SSLVPN daemon decides the number of worker processes.	integer	Minimum value: 0 Maximum value: 2	0
sslvpn-ems-sn-check	Enable/disable verification of EMS serial number in SSL-VPN connection.	option	-	disable
	Option / **Description** *enable* — Enable verification of EMS serial number in SSL-VPN connection. *disable* — Disable verification of EMS serial number in SSL-VPN connection.			
sslvpn-plugin-version-check	Enable/disable checking browser's plugin version by SSL-VPN.	option	-	enable
	Option / **Description** *enable* — Enable SSL-VPN automatic checking of browser plug-in version. *disable* — Disable SSL-VPN automatic checking of browser plug-in version.			
two-factor-ftk-expiry	FortiToken authentication session timeout .	integer	Minimum value: 60 Maximum value: 600	60
two-factor-email-expiry	Email-based two-factor authentication session timeout .	integer	Minimum value: 30 Maximum value: 300	60
two-factor-sms-expiry	SMS-based two-factor authentication session timeout .	integer	Minimum value: 30 Maximum value: 300	60
two-factor-fac-expiry	FortiAuthenticator token authentication session timeout .	integer	Minimum value: 10 Maximum value: 3600	60
two-factor-ftm-expiry	FortiToken Mobile session timeout .	integer	Minimum value: 1 Maximum value: 168	72

Parameter	Description	Type	Size	Default
max-img-cache-size	Maximum space (MB) can be used by image-analyzer to store blocked images into ram disk.	integer	Minimum value: 30 Maximum value: 300	60
img-cache-mode	Select image cache mode for image-analyzer	option	-	rolling

Option	Description
stop	Stop caching blocked images into ram disk when limit reaches.
rolling	Evict old cached images when limit reaches.

Parameter	Description	Type	Size	Default
per-user-bal	Enable/disable per-user block/allow list filter.	option	-	disable

Option	Description
enable	Enable per-user block/allow list filter.
disable	Disable per-user block/allow list filter.

Parameter	Description	Type	Size	Default
wad-worker-count	Number of explicit proxy WAN optimization daemon (WAD) processes. By default WAN optimization, explicit proxy, and web caching is handled by all of the CPU cores in a FortiProxy unit.	integer	Minimum value: 0 Maximum value: 2	0
wad-csvc-cs-count	Number of concurrent WAD-cache-service object-cache processes.	integer	Minimum value: 1 Maximum value: 1	1
wad-csvc-db-count	Number of concurrent WAD-cache-service byte-cache processes.	integer	Minimum value: 0 Maximum value: 2	0
http-view	Enable/disable logging and viewing of HTTP/S cache traffic.	option	-	disable

Option	Description
enable	Enable logging and viewing of HTTP/S cache traffic.
disable	Disable logging and viewing of HTTP/S cache traffic.

Parameter	Description	Type	Size	Default
wad-source-affinity	Enable/disable dispatching traffic to WAD workers based on source affinity.	option	-	enable

Option	Description
disable	Disable dispatching traffic to WAD workers based on source affinity.
enable	Enable dispatching traffic to WAD workers based on source affinity.

wad-memory-change-granularity	Minimum percentage change in system memory usage detected by the wad daemon prior to adjusting TCP window size for any active connection.	integer	Minimum value: 5 Maximum value: 25	10
login-timestamp	Enable/disable login time recording.	option	-	disable

Option	Description
enable	Enable login time recording.
disable	Disable login time recording.

miglogd-children	Number of logging (miglogd) processes to be allowed to run. Higher number can reduce performance; lower number can slow log processing time. No logs will be dropped or lost if the number is changed.	integer	Minimum value: 0 Maximum value: 15	0
special-file-23-support	Enable/disable detection of those special format files when using Data Leak Protection.	option	-	disable

Option	Description
disable	Disable detection of those special format files when using Data Leak Protection.
enable	Enable detection of those special format files when using Data Leak Protection.

Parameter	Description	Type	Size	Default
log-uuid-address	Enable/disable insertion of address UUIDs to traffic logs.	option	-	disable

Option	Description
enable	Enable insertion of address UUID to traffic logs.
disable	Disable insertion of address UUID to traffic logs.

Parameter	Description	Type	Size	Default
log-ssl-connection	Enable/disable logging of SSL connection events.	option	-	disable

Option	Description
enable	Enable logging of SSL connection events.
disable	Disable logging of SSL connection events.

Parameter	Description	Type	Size	Default
gui-rest-api-cache	Enable/disable REST API result caching on FortiProxy.	option	-	enable

Option	Description
enable	Enable REST API result caching on FortiProxy.
disable	Disable REST API result caching on FortiProxy.

Parameter	Description	Type	Size	Default
gui-fortiguard-resource-fetch	Enable/disable retrieving static GUI resources from FortiGuard. Disabling it will improve GUI load time for air-gapped environments.	option	-	enable

Option	Description
enable	Enable retrieving static GUI resources from FortiGuard.
disable	Disable retrieving static GUI resources from FortiGuard.

Parameter	Description	Type	Size	Default
arp-max-entry	Maximum number of dynamically learned MAC addresses that can be added to the ARP table .	integer	Minimum value: 131072 Maximum value: 2147483647	131072

Parameter	Description	Type	Size	Default
ha-affinity	Affinity setting for HA daemons (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxx).	string	Maximum length: 79	0
cmdbsvr-affinity	Affinity setting for cmdbsvr (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxx).	string	Maximum length: 79	0
av-affinity	Affinity setting for AV scanning (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxx).	string	Maximum length: 79	0
wad-affinity	Affinity setting for wad (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxx).	string	Maximum length: 79	0
ips-affinity	Affinity setting for IPS (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxx; allowed CPUs must be less than total number of IPS engine daemons).	string	Maximum length: 79	0
miglog-affinity	Affinity setting for logging (64-bit hexadecimal value in the format of xxxxxxxxxxxxxxxx).	string	Maximum length: 19	0
url-filter-affinity	URL filter CPU affinity.	string	Maximum length: 79	0
ndp-max-entry	Maximum number of NDP table entries (set to 65,536 or higher; if set to 0, kernel holds 65,536 entries).	integer	Minimum value: 65536 Maximum value: 2147483647	0
br-fdb-max-entry	Maximum number of bridge forwarding database (FDB) entries.	integer	Minimum value: 8192 Maximum value: 2147483647	8192

Parameter	Description	Type	Size	Default
max-route-cache-size	Maximum number of IP route cache entries .	integer	Minimum value: 0 Maximum value: 2147483647	0
ipsec-round-robin	Enable/disable round-robin redistribution to multiple CPUs for IPsec VPN traffic.	option	-	disable

Option	Description
enable	Enable round-robin redistribution for IPsec VPN.
disable	Disable round-robin redistribution for IPsec VPN.

ipsec-soft-dec-async	Enable/disable software decryption asynchronization (using multiple CPUs to do decryption) for IPsec VPN traffic.	option	-	disable

Option	Description
enable	Enable software decryption asynchronization for IPsec VPN.
disable	Disable software decryption asynchronization for IPsec VPN.

device-idle-timeout	Time in seconds that a device must be idle to automatically log the device user out. .	integer	Minimum value: 30 Maximum value: 31536000	300
user-device-store-max-devices	Maximum number of devices allowed in user device store.	integer	Minimum value: 5172 Maximum value: 14779	10345
user-device-store-max-users	Maximum number of users allowed in user device store.	integer	Minimum value: 5172 Maximum value: 14779	10345
user-device-store-max-unified-mem	Maximum unified memory allowed in user device store.	integer	Minimum value: 10345676 Maximum value: 103456768	51728384

Parameter	Description	Type	Size	Default
gui-device-latitude	Add the latitude of the location of this FortiProxy to position it on the Threat Map.	string	Maximum length: 19	
gui-device-longitude	Add the longitude of the location of this FortiProxy to position it on the Threat Map.	string	Maximum length: 19	
private-data-encryption	Enable/disable private data encryption using an AES 128-bit key or passpharse.	option	-	disable

Option	Description
disable	Disable private data encryption using an AES 128-bit key.
enable	Enable private data encryption using an AES 128-bit key.

Parameter	Description	Type	Size	Default
auto-auth-extension-device	Enable/disable automatic authorization of dedicated Fortinet extension devices.	option	-	enable

Option	Description
enable	Enable automatic authorization of dedicated Fortinet extension device globally.
disable	Disable automatic authorization of dedicated Fortinet extension device globally.

Parameter	Description	Type	Size	Default
gui-theme	Color scheme for the administration GUI.	option	-	jade

Option	Description
jade	Jade theme.
neutrino	Neutrino theme.
mariner	Mariner theme.
graphite	Graphite theme.
melongene	Melongene theme.
retro	FortiProxy v3 Retro theme.
dark-matter	Dark Matter theme.

Parameter	Description	Type	Size	Default
	Option / **Description** *onyx* — Onyx theme. *eclipse* — Eclipse theme.			
gui-date-format	Default date format used throughout GUI.	option	-	yyyy/MM/dd
	Option / **Description** *yyyy/MM/dd* — Year/Month/Day. *dd/MM/yyyy* — Day/Month/Year. *MM/dd/yyyy* — Month/Day/Year. *yyyy-MM-dd* — Year-Month-Day. *dd-MM-yyyy* — Day-Month-Year. *MM-dd-yyyy* — Month-Day-Year.			
gui-date-time-source	Source from which the FortiProxy GUI uses to display date and time entries.	option	-	system
	Option / **Description** *system* — Use this FortiProxy unit's configured timezone. *browser* — Use the web browser's timezone.			
igmp-state-limit	Maximum number of IGMP memberships .	integer	Minimum value: 96 Maximum value: 128000	3200
cloud-communication	Enable/disable all cloud communication.	option	-	enable
	Option / **Description** *enable* — Allow cloud communication. *disable* — Disable all cloud-related settings.			
ipsec-ha-seqjump-rate	ESP jump ahead rate (1G - 10G pps equivalent).	integer	Minimum value: 1 Maximum value: 10	10

Parameter	Description	Type	Size	Default
fortitoken-cloud	Enable/disable FortiToken Cloud service.	option	-	enable

Option	Description
enable	Enable FortiToken Cloud service.
disable	Disable FortiToken Cloud service.

faz-disk-buffer-size	Maximum disk buffer size to temporarily store logs destined for FortiAnalyzer. To be used in the event that FortiAnalyzer is unavailable.	integer	Minimum value: 0 Maximum value: 214748364	0
irq-time-accounting	Configure CPU IRQ time accounting mode.	option	-	auto

Option	Description
auto	Automatically switch CPU accounting mode.
force	Force the use of CPU IRQ time accounting mode.

management-ip	Management IP address of this FortiProxy. Used to log into this FortiProxy from another FortiProxy in the Security Fabric.	string	Maximum length: 255	
management-port	Overriding port for management connection (Overrides admin port).	integer	Minimum value: 1 Maximum value: 65535	443
management-port-use-admin-sport	Enable/disable use of the admin-sport setting for the management port. If disabled, FortiGate will allow user to specify management-port.	option	-	enable

Option	Description
enable	Enable use of the admin-sport setting for the management port.
disable	Disable use of the admin-sport setting for the management port.

Parameter	Description	Type	Size	Default
internet-service-database	Configure which Internet Service database size to download from FortiGuard and use.	option	-	full
	Option / **Description** *mini* — Small sized Internet Service database with very limited IP addresses. *standard* — Medium sized Internet Service database with most IP addresses. *full* — Full sized Internet Service database with all IP addresses.			
license-overlimit	System behaviour when max licensed proxy user is reached.	option	-	bypass
	Option / **Description** *bypass* — Bypass further traffic when licensed user is reached. *block* — Block further traffic when licensed user is reached.			
max-session-per-user	Max UTM sessions per user.	integer	Minimum value: 0 Maximum value: 4294967295	0
conntrack	Max numbers of conntrack.	integer	Minimum value: 60000 Maximum value: 10000000	2560000
established-timeout	Default established session timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	1800
time-wait-timeout	Default time-wait timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	60
fin-wait-timeout	Default fin-wait timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	60
close-wait-timeout	Default close-wait timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	30

Parameter	Description	Type	Size	Default
syn-sent-timeout	Default syn-sent timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	60
syn-recv-timeout	Default syn-recv timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	30
last-ack-timeout	Default last-ack timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	15
udp-timeout	Default last-ack timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	30
udp-stream-timeout	Default last-ack timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	180

config system gre-tunnel

Configure GRE tunnel.

```
config system gre-tunnel
    Description: Configure GRE tunnel.
    edit <name>
        set interface {string}
        set remote-gw {ipv4-address}
        set local-gw {ipv4-address-any}
        set sequence-number-transmission [disable|enable]
        set sequence-number-reception [disable|enable]
        set checksum-transmission [disable|enable]
        set checksum-reception [disable|enable]
        set key-outbound {integer}
        set key-inbound {integer}
        set keepalive-interval {integer}
        set keepalive-failtimes {integer}
    next
end
```

config system gre-tunnel

Parameter	Description	Type	Size	Default
interface	Interface name.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default
remote-gw	IP address of the remote gateway.	ipv4-address	Not Specified	0.0.0.0
local-gw	IP address of the local gateway.	ipv4-address-any	Not Specified	0.0.0.0
sequence-number-transmission	Enable/disable including of sequence numbers in transmitted GRE packets.	option	-	disable
	Option / **Description** *disable* — Include sequence numbers in transmitted GRE packets. *enable* — Do not include sequence numbers in transmitted GRE packets.			
sequence-number-reception	Enable/disable validating sequence numbers in received GRE packets.	option	-	disable
	Option / **Description** *disable* — Do not validate sequence number in received GRE packets. *enable* — Validate sequence numbers in received GRE packets.			
checksum-transmission	Enable/disable including checksums in transmitted GRE packets.	option	-	disable
	Option / **Description** *disable* — Do not include checksums in transmitted GRE packets. *enable* — Include checksums in transmitted GRE packets.			
checksum-reception	Enable/disable validating checksums in received GRE packets.	option	-	disable
	Option / **Description** *disable* — Do not validate checksums in received GRE packets. *enable* — Validate checksums in received GRE packets.			
key-outbound	Include this key in transmitted GRE packets .	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
key-inbound	Require received GRE packets contain this key .	integer	Minimum value: 0 Maximum value: 4294967295	0
keepalive-interval	Keepalive message interval .	integer	Minimum value: 0 Maximum value: 32767	0
keepalive-failtimes	Number of consecutive unreturned keepalive messages before a GRE connection is considered down .	integer	Minimum value: 1 Maximum value: 255	10

config system ha-monitor

Configure HA monitor.

```
config system ha-monitor
    Description: Configure HA monitor.
    set monitor-vlan [enable|disable]
    set vlan-hb-interval {integer}
    set vlan-hb-lost-threshold {integer}
end
```

config system ha-monitor

Parameter	Description	Type	Size	Default
monitor-vlan	Enable/disable monitor VLAN interfaces.	option	-	disable
	Option / **Description** *enable* — Enable monitor VLAN interfaces. *disable* — Disable monitor VLAN interfaces.			
vlan-hb-interval	Configure heartbeat interval (seconds).	integer	Minimum value: 1 Maximum value: 30	5
vlan-hb-lost-threshold	VLAN lost heartbeat threshold .	integer	Minimum value: 1 Maximum value: 60	3

config system ha-nonsync-csum

System checksum for FortiManager use only.

```
config system ha-nonsync-csum
    Description: System checksum for FortiManager use only.
end
```

config system ha

Configure HA.

```
config system ha
    Description: Configure HA.
    set group-id {integer}
    set group-name {string}
    set mode [standalone|config-sync-only|...]
    set sync-packet-balance [enable|disable]
    set password {password}
    set key {password}
    set hbdev {user}
    set unicast-hb [enable|disable]
    set unicast-hb-peerip {ipv4-address}
    set unicast-hb-netmask {ipv4-netmask}
    set session-sync-dev {user}
    set route-ttl {integer}
    set route-wait {integer}
    set route-hold {integer}
    set multicast-ttl {integer}
    set load-balance-all [enable|disable]
    set encryption [enable|disable]
    set authentication [enable|disable]
    set hb-interval {integer}
    set hb-interval-in-milliseconds [100ms|10ms]
    set hb-lost-threshold {integer}
    set hello-holddown {integer}
    set gratuitous-arps [enable|disable]
    set arps {integer}
    set arps-interval {integer}
    set link-failed-signal [enable|disable]
    set uninterruptible-upgrade [enable|disable]
    set sequential-upgrade [enable|disable]
    set uninterruptible-primary-wait {integer}
    set ha-mgmt-status [enable|disable]
    config ha-mgmt-interfaces
        Description: Reserve interfaces to manage individual cluster units.
        edit <id>
            set interface {string}
            set dst {ipv4-classnet}
            set gateway {ipv4-address}
            set gateway6 {ipv6-address}
        next
```

```
    end
    set ha-uptime-diff-margin {integer}
    set unicast-status [enable|disable]
    set unicast-gateway {ipv4-address}
    config unicast-peers
        Description: Number of unicast peers.
        edit <id>
            set peer-ip {ipv4-address}
        next
    end
    set logical-sn [enable|disable]
    set vcluster-id {integer}
    set override [enable|disable]
    set priority {integer}
    set override-wait-time {integer}
    set schedule [none|hub|...]
    set weight {user}
    set cpu-threshold {user}
    set memory-threshold {user}
    set http-proxy-threshold {user}
    set ftp-proxy-threshold {user}
    set imap-proxy-threshold {user}
    set nntp-proxy-threshold {user}
    set pop3-proxy-threshold {user}
    set smtp-proxy-threshold {user}
    set monitor {user}
    set pingserver-monitor-interface {user}
    set pingserver-failover-threshold {integer}
    set pingserver-secondary-force-reset [enable|disable]
    set pingserver-flip-timeout {integer}
    set vdom {user}
    set vcluster2 [enable|disable]
    config secondary-vcluster
        Description: Configure virtual cluster 2.
        set vcluster-id {integer}
        set override [enable|disable]
        set priority {integer}
        set override-wait-time {integer}
        set monitor {user}
        set pingserver-monitor-interface {user}
        set pingserver-failover-threshold {integer}
        set pingserver-secondary-force-reset [enable|disable]
        set vdom {user}
    end
    set ha-direct [enable|disable]
    set ssd-failover [enable|disable]
    set memory-compatible-mode [enable|disable]
    set memory-based-failover [enable|disable]
    set memory-failover-threshold {integer}
    set memory-failover-monitor-period {integer}
    set memory-failover-sample-rate {integer}
    set memory-failover-flip-timeout {integer}
    set failover-hold-time {integer}
end
```

config system ha

Parameter	Description	Type	Size	Default
group-id	HA group ID . Must be the same for all members.	integer	Minimum value: 0 Maximum value: 1023	0
group-name	Cluster group name. Must be the same for all members.	string	Maximum length: 32	
mode	HA mode. Must be the same for all members. FGSP requires standalone.	option	-	standalone
	Option / **Description** *standalone* — Disable HA feature. *config-sync-only* — Enable Config sync only *active-passive* — Enable Active-passive mode.			
sync-packet-balance	Enable/disable HA packet distribution to multiple CPUs.	option	-	disable
	Option / **Description** *enable* — Enable HA packet distribution to multiple CPUs. *disable* — Disable HA packet distribution to multiple CPUs.			
password	Cluster password. Must be the same for all members.	password	Not Specified	
key	Key.	password	Not Specified	
hbdev	Heartbeat interfaces. Must be the same for all members.	user	Not Specified	
unicast-hb	Enable/disable unicast heartbeat.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
unicast-hb-peerip	Unicast heartbeat peer IP.	ipv4-address	Not Specified	0.0.0.0
unicast-hb-netmask	Unicast heartbeat netmask.	ipv4-netmask	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
session-sync-dev	Offload session-sync process to kernel and sync sessions using connected interface(s) directly.	user	Not Specified	
route-ttl	TTL for primary unit routes . Increase to maintain active routes during failover.	integer	Minimum value: 5 Maximum value: 3600	10
route-wait	Time to wait before sending new routes to the cluster .	integer	Minimum value: 0 Maximum value: 3600	0
route-hold	Time to wait between routing table updates to the cluster .	integer	Minimum value: 0 Maximum value: 3600	10
multicast-ttl	HA multicast TTL on primary .	integer	Minimum value: 5 Maximum value: 3600	600
load-balance-all	Enable to load balance TCP sessions. Disable to load balance proxy sessions only.	option	-	disable

Option	Description
enable	Enable load balance.
disable	Disable load balance.

Parameter	Description	Type	Size	Default
encryption	Enable/disable heartbeat message encryption.	option	-	disable

Option	Description
enable	Enable heartbeat message encryption.
disable	Disable heartbeat message encryption.

Parameter	Description	Type	Size	Default
authentication	Enable/disable heartbeat message authentication.	option	-	disable

Option	Description
enable	Enable heartbeat message authentication.
disable	Disable heartbeat message authentication.

Parameter	Description	Type	Size	Default
hb-interval	Time between sending heartbeat packets . Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 20	2
hb-interval-in-milliseconds	Number of milliseconds for each heartbeat interval: 100ms or 10ms.	option	-	100ms
	Option / **Description** *100ms* — Each heartbeat interval is 100ms. *10ms* — Each heartbeat interval is 10ms.			
hb-lost-threshold	Number of lost heartbeats to signal a failure . Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 60	20
hello-holddown	Time to wait before changing from hello to work state .	integer	Minimum value: 5 Maximum value: 300	20
gratuitous-arps	Enable/disable gratuitous ARPs. Disable if link-failed-signal enabled.	option	-	enable
	Option / **Description** *enable* — Enable gratuitous ARPs. *disable* — Disable gratuitous ARPs.			
arps	Number of gratuitous ARPs . Lower to reduce traffic. Higher to reduce failover time.	integer	Minimum value: 1 Maximum value: 60	5
arps-interval	Time between gratuitous ARPs . Lower to reduce failover time. Higher to reduce traffic.	integer	Minimum value: 1 Maximum value: 20	8
link-failed-signal	Enable to shut down all interfaces for 1 sec after a failover. Use if gratuitous ARPs do not update network.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			

Parameter	Description	Type	Size	Default
uninterruptible-upgrade	Enable to upgrade a cluster without blocking network traffic.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
sequential-upgrade	Enable to upgrade secondaries one by one.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
uninterruptible-primary-wait	Number of minutes the primary HA unit waits before the secondary HA unit is considered upgraded and the system is started before starting its own upgrade .	integer	Minimum value: 15 Maximum value: 300	30
ha-mgmt-status	Enable to reserve interfaces to manage individual cluster units.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
ha-uptime-diff-margin	Normally you would only reduce this value for failover testing.	integer	Minimum value: 1 Maximum value: 65535	300
unicast-status	Enable/disable unicast connection.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
unicast-gateway	Default route gateway for unicast interface.	ipv4-address	Not Specified	0.0.0.0
logical-sn	Enable/disable usage of the logical serial number.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable usage of the logical serial number. *disable* — Disable usage of the logical serial number.			
vcluster-id	Cluster ID.	integer	Minimum value: 0 Maximum value: 255	0
override	Enable and increase the priority of the unit that should always be primary.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
priority	Increase the priority to select the primary unit .	integer	Minimum value: 0 Maximum value: 255	128
override-wait-time	Delay negotiating if override is enabled . Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600	0
schedule	Type of A-A load balancing. Use none if you have external load balancers.	option	-	round-robin
	Option / **Description** *none* — None. *hub* — Hub. *leastconnection* — Least connection. *round-robin* — Round robin. *weight-round-robin* — Weight round robin. *random* — Random. *ip* — IP. *ipport* — IP port.			
weight	Weighted round robin weight for each cluster unit. Syntax <priority> <weight>.	user	Not Specified	0 40

Parameter	Description	Type	Size	Default
cpu-threshold	Dynamic weighted load balancing CPU usage weight and high and low thresholds.	user	Not Specified	
memory-threshold	Dynamic weighted load balancing memory usage weight and high and low thresholds.	user	Not Specified	
http-proxy-threshold	Dynamic weighted load balancing weight and high and low number of HTTP proxy sessions.	user	Not Specified	
ftp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of FTP proxy sessions.	user	Not Specified	
imap-proxy-threshold	Dynamic weighted load balancing weight and high and low number of IMAP proxy sessions.	user	Not Specified	
nntp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of NNTP proxy sessions.	user	Not Specified	
pop3-proxy-threshold	Dynamic weighted load balancing weight and high and low number of POP3 proxy sessions.	user	Not Specified	
smtp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of SMTP proxy sessions.	user	Not Specified	
monitor	Interfaces to check for port monitoring (or link failure).	user	Not Specified	
pingserver-monitor-interface	Interfaces to check for remote IP monitoring.	user	Not Specified	
pingserver-failover-threshold	Remote IP monitoring failover threshold .	integer	Minimum value: 0 Maximum value: 50	0
pingserver-secondary-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-	enable
	Option / **Description** *enable* — Enable force reset of secondary after PING server failure. *disable* — Disable force reset of secondary after PING server failure.			
pingserver-flip-timeout	Time to wait in minutes before renegotiating after a remote IP monitoring failover.	integer	Minimum value: 6 Maximum value: 2147483647	60
vdom	VDOMs in virtual cluster 1.	user	Not Specified	

Parameter	Description	Type	Size	Default
vcluster2	Enable/disable virtual cluster 2 for virtual clustering.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
ha-direct	Enable/disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, and FortiSandbox.	option	-	disable
	Option / **Description** *enable* — Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, and FortiSandbox. *disable* — Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, and FortiSandbox.			
ssd-failover	Enable/disable automatic HA failover on SSD disk failure.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
memory-compatible-mode	Enable/disable memory compatible mode.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
memory-based-failover	Enable/disable memory based failover.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
memory-failover-threshold	Memory usage threshold to trigger memory based failover (0 means using conserve mode threshold in system.global).	integer	Minimum value: 0 Maximum value: 95	0

Parameter	Description	Type	Size	Default
memory-failover-monitor-period	Duration of high memory usage before memory based failover is triggered in seconds .	integer	Minimum value: 1 Maximum value: 300	60
memory-failover-sample-rate	Rate at which memory usage is sampled in order to measure memory usage in seconds .	integer	Minimum value: 1 Maximum value: 60	1
memory-failover-flip-timeout	Time to wait between subsequent memory based failovers in minutes .	integer	Minimum value: 6 Maximum value: 2147483647	6
failover-hold-time	Time to wait before failover , to avoid flip.	integer	Minimum value: 0 Maximum value: 300	0

config ha-mgmt-interfaces

Parameter	Description	Type	Size	Default
interface	Interface to reserve for HA management.	string	Maximum length: 15	
dst	Default route destination for reserved HA management interface.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
gateway	Default route gateway for reserved HA management interface.	ipv4-address	Not Specified	0.0.0.0
gateway6	Default IPv6 gateway for reserved HA management interface.	ipv6-address	Not Specified	::

config unicast-peers

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

config secondary-vcluster

Parameter	Description	Type	Size	Default
vcluster-id	Cluster ID.	integer	Minimum value: 0 Maximum value: 255	1
override	Enable and increase the priority of the unit that should always be primary.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

priority	Increase the priority to select the primary unit .	integer	Minimum value: 0 Maximum value: 255	128
override-wait-time	Delay negotiating if override is enabled . Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600	0
monitor	Interfaces to check for port monitoring (or link failure).	user	Not Specified	
pingserver-monitor-interface	Interfaces to check for remote IP monitoring.	user	Not Specified	
pingserver-failover-threshold	Remote IP monitoring failover threshold .	integer	Minimum value: 0 Maximum value: 50	0
pingserver-secondary-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-	enable

Option	Description
enable	Enable force reset of secondary after PING server failure.
disable	Disable force reset of secondary after PING server failure.

vdom	VDOMs in virtual cluster 2.	user	Not Specified	

config system info admin ssh

Show SSH status.

```
config system info admin ssh
    Description: Show SSH status.
end
```

config system info admin status

Show logged in administrators.

```
config system info admin status
    Description: Show logged in administrators.
end
```

config system interface

Configure interfaces.

```
config system interface
    Description: Configure interfaces.
    edit <name>
        set vdom {string}
        set cli-conn-status {integer}
        set mode [static|dhcp|...]
        config client-options
            Description: DHCP client options.
            edit <id>
                set code {integer}
                set type [hex|string|...]
                set value {string}
                set ip {user}
            next
        end
        set distance {integer}
        set priority {integer}
        set dhcp-relay-interface-select-method [auto|sdwan|...]
        set dhcp-relay-interface {string}
        set dhcp-relay-service [disable|enable]
        set dhcp-relay-ip {user}
        set dhcp-relay-link-selection {ipv4-address}
        set dhcp-relay-request-all-server [disable|enable]
        set dhcp-relay-type [regular|ipsec]
        set dhcp-relay-agent-option [enable|disable]
        set dhcp-classless-route-addition [enable|disable]
        set management-ip {ipv4-classnet-host}
        set ip {ipv4-classnet-host}
        set allowaccess {option1}, {option2}, ...
```

```
set gwdetect [enable|disable]
set ping-serv-status {integer}
set detectserver {user}
set detectprotocol {option1}, {option2}, ...
set ha-priority {integer}
set fail-detect [enable|disable]
set fail-detect-option {option1}, {option2}, ...
set fail-alert-method [link-failed-signal|link-down]
set fail-action-on-extender [soft-restart|hard-restart|...]
set fail-alert-interfaces <name1>, <name2>, ...
set dhcp-client-identifier {string}
set dhcp-renew-time {integer}
set ipunnumbered {ipv4-address}
set username {string}
set pppoe-unnumbered-negotiate [enable|disable]
set password {password}
set idle-timeout {integer}
set detected-peer-mtu {integer}
set disc-retry-timeout {integer}
set padt-retry-timeout {integer}
set service-name {string}
set ac-name {string}
set lcp-echo-interval {integer}
set lcp-max-echo-fails {integer}
set defaultgw [enable|disable]
set dns-server-override [enable|disable]
set dns-server-protocol {option1}, {option2}, ...
set auth-type [auto|pap|...]
set pptp-client [enable|disable]
set pptp-user {string}
set pptp-password {password}
set pptp-server-ip {ipv4-address}
set pptp-auth-type [auto|pap|...]
set pptp-timeout {integer}
set arpforward [enable|disable]
set broadcast-forward [enable|disable]
set bfd [global|enable|...]
set bfd-desired-min-tx {integer}
set bfd-detect-mult {integer}
set bfd-required-min-rx {integer}
set l2forward [enable|disable]
set icmp-send-redirect [enable|disable]
set icmp-accept-redirect [enable|disable]
set vlanforward [enable|disable]
set stpforward [enable|disable]
set stpforward-mode [rpl-all-ext-id|rpl-bridge-ext-id|...]
set macaddr {mac-address}
set substitute-dst-mac {mac-address}
set speed [auto|10full|...]
set status [up|down]
set netbios-forward [disable|enable]
set wins-ip {ipv4-address}
set type [physical|vlan|...]
set dedicated-to [none|management]
set trust-ip-1 {ipv4-classnet-any}
set trust-ip-2 {ipv4-classnet-any}
```

```
set trust-ip-3 {ipv4-classnet-any}
set trust-ip6-1 {ipv6-prefix}
set trust-ip6-2 {ipv6-prefix}
set trust-ip6-3 {ipv6-prefix}
set mtu-override [enable|disable]
set mtu {integer}
set ring-rx {integer}
set ring-tx {integer}
set wccp [enable|disable]
set drop-overlapped-fragment [enable|disable]
set drop-fragment [enable|disable]
set src-check [enable|disable]
set explicit-web-proxy [enable|disable]
set explicit-ftp-proxy [enable|disable]
set proxy-captive-portal [enable|disable]
set tcp-mss {integer}
set inbandwidth {integer}
set outbandwidth {integer}
set egress-shaping-profile {string}
set ingress-shaping-profile {string}
set disconnect-threshold {integer}
set spillover-threshold {integer}
set ingress-spillover-threshold {integer}
set weight {integer}
set interface {string}
set external [enable|disable]
set vlan-protocol [8021q|8021ad]
set vlanid {integer}
set forward-domain {integer}
set remote-ip {ipv4-classnet-host}
set member <interface-name1>, <interface-name2>, ...
set lacp-mode [static|passive|...]
set lacp-ha-secondary [enable|disable]
set system-id-type [auto|user]
set system-id {mac-address}
set lacp-speed [slow|fast]
set min-links {integer}
set min-links-down [operational|administrative]
set algorithm [L2|L3|...]
set link-up-delay {integer}
set priority-override [enable|disable]
set aggregate {string}
set redundant-interface {string}
set devindex {integer}
set switch {string}
set description {var-string}
set alias {string}
set security-mode [none|captive-portal|...]
set security-mac-auth-bypass [mac-auth-only|enable|...]
set security-external-web {var-string}
set security-external-logout {string}
set replacemsg-override-group {string}
set security-redirect-url {var-string}
set auth-cert {string}
set auth-portal-addr {string}
set security-exempt-list {string}
```

```
        set security-groups <name1>, <name2>, ...
        set role [lan|wan|...]
        set snmp-index {integer}
        set secondary-IP [enable|disable]
        config secondaryip
            Description: Second IP address of interface.
            edit <id>
                set ip {ipv4-classnet-host}
                set allowaccess {option1}, {option2}, ...
                set gwdetect [enable|disable]
                set ping-serv-status {integer}
                set detectserver {user}
                set detectprotocol {option1}, {option2}, ...
                set ha-priority {integer}
            next
        end
        set color {integer}
        config tagging
            Description: Config object tagging.
            edit <name>
                set category {string}
                set tags <name1>, <name2>, ...
            next
        end
        config ipv6
            Description: IPv6 of interface.
            set ip6-mode [static|dhcp|...]
            set nd-mode [basic|SEND-compatible]
            set nd-cert {string}
            set nd-security-level {integer}
            set nd-timestamp-delta {integer}
            set nd-timestamp-fuzz {integer}
            set nd-cga-modifier {user}
            set ip6-dns-server-override [enable|disable]
            set ip6-address {ipv6-prefix}
            config ip6-extra-addr
                Description: Extra IPv6 address prefixes of interface.
                edit <prefix>
                next
            end
            set ip6-allowaccess {option1}, {option2}, ...
            set ip6-send-adv [enable|disable]
            set icmp6-send-redirect [enable|disable]
            set ip6-manage-flag [enable|disable]
            set ip6-other-flag [enable|disable]
            set ip6-max-interval {integer}
            set ip6-min-interval {integer}
            set ip6-link-mtu {integer}
            set ra-send-mtu [enable|disable]
            set ip6-reachable-time {integer}
            set ip6-retrans-time {integer}
            set ip6-default-life {integer}
            set ip6-hop-limit {integer}
            set autoconf [enable|disable]
            set unique-autoconf-addr [enable|disable]
            set interface-identifier {ipv6-address}
```

```
            set ip6-prefix-mode [dhcp6|ra]
            set ip6-upstream-interface {string}
            set ip6-delegated-prefix-iaid {integer}
            set ip6-subnet {ipv6-prefix}
            config ip6-prefix-list
                Description: Advertised prefix list.
                edit <prefix>
                    set autonomous-flag [enable|disable]
                    set onlink-flag [enable|disable]
                    set valid-life-time {integer}
                    set preferred-life-time {integer}
                    set rdnss {user}
                    set dnssl <domain1>, <domain2>, ...
                next
            end
            config ip6-delegated-prefix-list
                Description: Advertised IPv6 delegated prefix list.
                edit <prefix-id>
                    set upstream-interface {string}
                    set delegated-prefix-iaid {integer}
                    set autonomous-flag [enable|disable]
                    set onlink-flag [enable|disable]
                    set subnet {ipv6-network}
                    set rdnss-service [delegated|default|...]
                    set rdnss {user}
                next
            end
            set dhcp6-relay-service [disable|enable]
            set dhcp6-relay-type {option}
            set dhcp6-relay-ip {user}
            set dhcp6-client-options {option1}, {option2}, ...
            set dhcp6-prefix-delegation [enable|disable]
            set dhcp6-information-request [enable|disable]
            config dhcp6-iapd-list
                Description: DHCPv6 IA-PD list.
                edit <iaid>
                    set prefix-hint {ipv6-network}
                    set prefix-hint-plt {integer}
                    set prefix-hint-vlt {integer}
                next
            end
            set cli-conn6-status {integer}
        end
    next
end
```

config system interface

Parameter	Description	Type	Size	Default
vdom	Interface is in this virtual domain (VDOM).	string	Maximum length: 31	

Parameter	Description	Type	Size	Default
cli-conn-status	CLI connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0
mode	Addressing mode (static, DHCP, PPPoE).	option	-	static

Option	Description
static	Static setting.
dhcp	External DHCP client mode.
pppoe	External PPPoE mode.

distance	Distance for routes learned through PPPoE or DHCP, lower distance indicates preferred route.	integer	Minimum value: 1 Maximum value: 255	5
priority	Priority of learned routes.	integer	Minimum value: 1 Maximum value: 65535	0
dhcp-relay-interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	Set outgoing interface manually.

dhcp-relay-interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
dhcp-relay-service	Enable/disable allowing this interface to act as a DHCP relay.	option	-	disable

Option	Description
disable	None.
enable	DHCP relay agent.

dhcp-relay-ip	DHCP relay IP address.	user	Not Specified	

Parameter	Description	Type	Size	Default
dhcp-relay-link-selection	DHCP relay link selection.	ipv4-address	Not Specified	0.0.0.0
dhcp-relay-request-all-server	Enable/disable sending of DHCP requests to all servers.	option	-	disable
	Option / **Description** *disable* — Send DHCP requests only to a matching server. *enable* — Send DHCP requests to all servers.			
dhcp-relay-type	DHCP relay type (regular or IPsec).	option	-	regular
	Option / **Description** *regular* — Regular DHCP relay. *ipsec* — DHCP relay for IPsec.			
dhcp-relay-agent-option	Enable/disable DHCP relay agent option.	option	-	enable
	Option / **Description** *enable* — Enable DHCP relay agent option. *disable* — Disable DHCP relay agent option.			
dhcp-classless-route-addition	Enable/disable addition of classless static routes retrieved from DHCP server.	option	-	enable
	Option / **Description** *enable* — Enable addition of classless static routes retrieved from DHCP server. *disable* — Disable addition of classless static routes retrieved from DHCP server.			
management-ip	High Availability in-band management IP address of this interface.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
ip	Interface IPv4 address and subnet mask, syntax: X.X.X.X/24.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
allowaccess	Permitted types of management access to this interface.	option	-	

Parameter	Description	Type	Size	Default
	Option / **Description** *ping* — PING access. *https* — HTTPS access. *ssh* — SSH access. *snmp* — SNMP access. *http* — HTTP access. *telnet* — TELNET access. *fgfm* — FortiManager access. *radius-acct* — RADIUS accounting access. *probe-response* — Probe access. *fabric* — Security Fabric access. *ftm* — FTM access. *speed-test* — Speed test access.			
gwdetect	Enable/disable detect gateway alive for first.	option	-	disable
	Option / **Description** *enable* — Enable detect gateway alive for first. *disable* — Disable detect gateway alive for first.			
ping-serv-status	PING server status.	integer	Minimum value: 0 Maximum value: 255	0
detectserver	Gateway's ping server for this IP.	user	Not Specified	
detectprotocol	Protocols used to detect the server.	option	-	ping
	Option / **Description** *ping* — PING. *tcp-echo* — TCP echo. *udp-echo* — UDP echo.			

Parameter	Description	Type	Size	Default
ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50	1
fail-detect	Enable/disable fail detection features for this interface.	option	-	disable
	Option / **Description** *enable* — Enable interface failed option status. *disable* — Disable interface failed option status.			
fail-detect-option	Options for detecting that this interface has failed.	option	-	link-down
	Option / **Description** *detectserver* — Use a ping server to determine if the interface has failed. *link-down* — Use port detection to determine if the interface has failed.			
fail-alert-method	Select link-failed-signal or link-down method to alert about a failed link.	option	-	link-down
	Option / **Description** *link-failed-signal* — Link-failed-signal. *link-down* — Link-down.			
fail-action-on-extender	Action on FortiExtender when interface fail.	option	-	soft-restart
	Option / **Description** *soft-restart* — Soft-restart-on-extender. *hard-restart* — Hard-restart-on-extender. *reboot* — Reboot-on-extender.			
fail-alert-interfaces <name>	Names of the FortiProxy interfaces to which the link failure alert is sent. Names of the non-virtual interface.	string	Maximum length: 79	
dhcp-client-identifier	DHCP client identifier.	string	Maximum length: 48	

Parameter	Description	Type	Size	Default
dhcp-renew-time	DHCP renew time in seconds , 0 means use the renew time provided by the server.	integer	Minimum value: 300 Maximum value: 604800	0
ipunnumbered	Unnumbered IP used for PPPoE interfaces for which no unique local address is provided.	ipv4-address	Not Specified	0.0.0.0
username	Username of the PPPoE account, provided by your ISP.	string	Maximum length: 64	
pppoe-unnumbered-negotiate	Enable/disable PPPoE unnumbered negotiation.	option	-	enable
	Option / **Description** *enable* — Enable IP address negotiating for unnumbered. *disable* — Disable IP address negotiating for unnumbered.			
password	PPPoE account's password.	password	Not Specified	
idle-timeout	PPPoE auto disconnect after idle timeout seconds, 0 means no timeout.	integer	Minimum value: 0 Maximum value: 32767	0
detected-peer-mtu	MTU of detected peer .	integer	Minimum value: 0 Maximum value: 4294967295	0
disc-retry-timeout	Time in seconds to wait before retrying to start a PPPoE discovery, 0 means no timeout.	integer	Minimum value: 0 Maximum value: 4294967295	1
padt-retry-timeout	PPPoE Active Discovery Terminate (PADT) used to terminate sessions after an idle time.	integer	Minimum value: 0 Maximum value: 4294967295	1
service-name	PPPoE service name.	string	Maximum length: 63	
ac-name	PPPoE server name.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
lcp-echo-interval	Time in seconds between PPPoE Link Control Protocol (LCP) echo requests.	integer	Minimum value: 0 Maximum value: 32767	5
lcp-max-echo-fails	Maximum missed LCP echo messages before disconnect.	integer	Minimum value: 0 Maximum value: 32767	3
defaultgw	Enable to get the gateway IP from the DHCP or PPPoE server.	option	-	enable

Option	Description
enable	Enable default gateway.
disable	Disable default gateway.

Parameter	Description	Type	Size	Default
dns-server-override	Enable/disable use DNS acquired by DHCP or PPPoE.	option	-	enable

Option	Description
enable	Use DNS acquired by DHCP or PPPoE.
disable	No not use DNS acquired by DHCP or PPPoE.

Parameter	Description	Type	Size	Default
dns-server-protocol	DNS transport protocols.	option	-	cleartext

Option	Description
cleartext	DNS over UDP/53, DNS over TCP/53.
dot	DNS over TLS/853.
doh	DNS over HTTPS/443.

Parameter	Description	Type	Size	Default
auth-type	PPP authentication type to use.	option	-	auto

Option	Description
auto	Automatically choose authentication.
pap	PAP authentication.
chap	CHAP authentication.
mschapv1	MS-CHAPv1 authentication.
mschapv2	MS-CHAPv2 authentication.

Parameter	Description	Type	Size	Default
pptp-client	Enable/disable PPTP client.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable PPTP client. *disable* / Disable PPTP client.			
pptp-user	PPTP user name.	string	Maximum length: 64	
pptp-password	PPTP password.	password	Not Specified	
pptp-server-ip	PPTP server IP address.	ipv4-address	Not Specified	0.0.0.0
pptp-auth-type	PPTP authentication type.	option	-	auto
	Option / **Description** *auto* / Automatically choose authentication. *pap* / PAP authentication. *chap* / CHAP authentication. *mschapv1* / MS-CHAPv1 authentication. *mschapv2* / MS-CHAPv2 authentication.			
pptp-timeout	Idle timer in minutes (0 for disabled).	integer	Minimum value: 0 Maximum value: 65535	0
arpforward	Enable/disable ARP forwarding.	option	-	enable
	Option / **Description** *enable* / Enable ARP forwarding. *disable* / Disable ARP forwarding.			
broadcast-forward	Enable/disable broadcast forwarding.	option	-	disable
	Option / **Description** *enable* / Enable broadcast forwarding. *disable* / Disable broadcast forwarding.			
bfd	Bidirectional Forwarding Detection (BFD) settings.	option	-	global

Parameter	Description	Type	Size	Default
	Option / **Description** *global* — BFD behavior of this interface will be based on global configuration. *enable* — Enable BFD on this interface and ignore global configuration. *disable* — Disable BFD on this interface and ignore global configuration.			
bfd-desired-min-tx	BFD desired minimal transmit interval.	integer	Minimum value: 1 Maximum value: 100000	250
bfd-detect-mult	BFD detection multiplier.	integer	Minimum value: 1 Maximum value: 50	3
bfd-required-min-rx	BFD required minimal receive interval.	integer	Minimum value: 1 Maximum value: 100000	250
l2forward	Enable/disable l2 forwarding.	option	-	disable
	Option / **Description** *enable* — Enable L2 forwarding. *disable* — Disable L2 forwarding.			
icmp-send-redirect	Enable/disable sending of ICMP redirects.	option	-	enable
	Option / **Description** *enable* — Enable sending of ICMP redirects. *disable* — Disable sending of ICMP redirects.			
icmp-accept-redirect	Enable/disable ICMP accept redirect.	option	-	enable
	Option / **Description** *enable* — Enable ICMP accept redirect. *disable* — Disable ICMP accept redirect.			
vlanforward	Enable/disable traffic forwarding between VLANs on this interface.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable traffic forwarding. *disable* — Disable traffic forwarding.			
stpforward	Enable/disable STP forwarding.	option	-	disable
	Option / **Description** *enable* — Enable STP forwarding. *disable* — Disable STP forwarding.			
stpforward-mode	Configure STP forwarding mode.	option	-	rpl-all-ext-id
	Option / **Description** *rpl-all-ext-id* — Replace all extension IDs (root, bridge). *rpl-bridge-ext-id* — Replace the bridge extension ID only. *rpl-nothing* — Replace nothing.			
macaddr	Change the interface's MAC address.	mac-address	Not Specified	00:00:00:00:00:00
substitute-dst-mac	Destination MAC address that all packets are sent to from this interface.	mac-address	Not Specified	00:00:00:00:00:00
speed	Interface speed. The default setting and the options available depend on the interface hardware.	option	-	auto
	Option / **Description** *auto* — Automatically adjust speed. *10full* — 10M full-duplex. *10half* — 10M half-duplex. *100full* — 100M full-duplex. *100half* — 100M half-duplex. *1000full* — 1000M full-duplex. *1000auto* — 1000M auto adjust.			
status	Bring the interface up or shut the interface down.	option	-	up

Parameter	Description	Type	Size	Default
	Option / **Description** *up* — Bring the interface up. *down* — Shut the interface down.			
netbios-forward	Enable/disable NETBIOS forwarding.	option	-	disable
	Option / **Description** *disable* — Disable NETBIOS forwarding. *enable* — Enable NETBIOS forwarding.			
wins-ip	WINS server IP.	ipv4-address	Not Specified	0.0.0.0
type	Interface type.	option	-	vlan
	Option / **Description** *physical* — Physical interface. *vlan* — VLAN interface. *aggregate* — Aggregate interface. *redundant* — Redundant interface. *tunnel* — Tunnel interface. *loopback* — Loopback interface. *vdom-link* — VDOM link interface. *vxlan* — VXLAN interface.			
dedicated-to	Configure interface for single purpose.	option	-	none
	Option / **Description** *none* — Interface not dedicated for any purpose. *management* — Dedicate this interface for management purposes only.			
trust-ip-1	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
trust-ip-2	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0

Parameter	Description	Type	Size	Default
trust-ip-3	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
trust-ip6-1	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified	::/0
trust-ip6-2	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified	::/0
trust-ip6-3	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified	::/0
mtu-override	Enable to set a custom MTU for this interface.	option	-	disable
	Option / **Description** *enable* — Override default MTU. *disable* — Use default MTU.			
mtu	MTU value for this interface.	integer	Minimum value: 0 Maximum value: 4294967295	1500
ring-rx	RX ring size.	integer	Minimum value: 0 Maximum value: 4294967295	0
ring-tx	TX ring size.	integer	Minimum value: 0 Maximum value: 4294967295	0
wccp	Enable/disable WCCP on this interface. Used for encapsulated WCCP communication between WCCP clients and servers.	option	-	disable
	Option / **Description** *enable* — Enable WCCP protocol on this interface. *disable* — Disable WCCP protocol on this interface.			

Parameter	Description	Type	Size	Default
drop-overlapped-fragment	Enable/disable drop overlapped fragment packets.	option	-	disable

Option	Description
enable	Enable drop of overlapped fragment packets.
disable	Disable drop of overlapped fragment packets.

Parameter	Description	Type	Size	Default
drop-fragment	Enable/disable drop fragment packets.	option	-	disable

Option	Description
enable	Enable/disable drop fragment packets.
disable	Do not drop fragment packets.

Parameter	Description	Type	Size	Default
src-check	Enable/disable source IP check.	option	-	enable

Option	Description
enable	Enable source IP check.
disable	Disable source IP check.

Parameter	Description	Type	Size	Default
explicit-web-proxy	Enable/disable the explicit web proxy on this interface.	option	-	disable

Option	Description
enable	Enable explicit Web proxy on this interface.
disable	Disable explicit Web proxy on this interface.

Parameter	Description	Type	Size	Default
explicit-ftp-proxy	Enable/disable the explicit FTP proxy on this interface.	option	-	disable

Option	Description
enable	Enable explicit FTP proxy on this interface.
disable	Disable explicit FTP proxy on this interface.

Parameter	Description	Type	Size	Default
proxy-captive-portal	Enable/disable proxy captive portal on this interface.	option	-	disable

Option	Description
enable	Enable proxy captive portal on this interface.
disable	Disable proxy captive portal on this interface.

Parameter	Description	Type	Size	Default
tcp-mss	TCP maximum segment size. 0 means do not change segment size.	integer	Minimum value: 48 Maximum value: 65535	0
inbandwidth	Bandwidth limit for incoming traffic , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 80000000	0
outbandwidth	Bandwidth limit for outgoing traffic .	integer	Minimum value: 0 Maximum value: 80000000	0
egress-shaping-profile	Outgoing traffic shaping profile.	string	Maximum length: 35	
ingress-shaping-profile	Incoming traffic shaping profile.	string	Maximum length: 35	
disconnect-threshold	Time in milliseconds to wait before sending a notification that this interface is down or disconnected.	integer	Minimum value: 0 Maximum value: 10000	0
spillover-threshold	Egress Spillover threshold , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000	0
ingress-spillover-threshold	Ingress Spillover threshold , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000	0
weight	Default weight for static routes (if route has no weight configured).	integer	Minimum value: 0 Maximum value: 255	0
interface	Interface name.	string	Maximum length: 15	
external	Enable/disable identifying the interface as an external interface (which usually means it's connected to the Internet).	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable identifying the interface as an external interface. *disable* — Disable identifying the interface as an external interface.			
vlan-protocol	Ethernet protocol of VLAN.	option	-	8021q
	Option / **Description** *8021q* — IEEE 802.1Q. *8021ad* — IEEE 802.1AD.			
vlanid	VLAN ID .	integer	Minimum value: 1 Maximum value: 4094	0
forward-domain	Transparent mode forward domain.	integer	Minimum value: 0 Maximum value: 2147483647	0
remote-ip	Remote IP address of tunnel.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
member `<interface-name>`	Physical interfaces that belong to the aggregate or redundant interface. Physical interface name.	string	Maximum length: 79	
lacp-mode	LACP mode.	option	-	active
	Option / **Description** *static* — Use static aggregation, do not send and ignore any LACP messages. *passive* — Passively use LACP to negotiate 802.3ad aggregation. *active* — Actively use LACP to negotiate 802.3ad aggregation.			
lacp-ha-secondary	LACP HA slave.	option	-	enable
	Option / **Description** *enable* — Allow HA slave to send/receive LACP messages. *disable* — Block HA slave from sending/receiving LACP messages.			
system-id-type	Method in which system ID is generated.	option	-	auto

Parameter	Description	Type	Size	Default
	Option / **Description** *auto* — Use the MAC address of the first member. *user* — User-defined system ID.			
system-id	Define a system ID for the aggregate interface.	mac-address	Not Specified	00:00:00:00:00:00
lacp-speed	How often the interface sends LACP messages.	option	-	slow
	Option / **Description** *slow* — Send LACP message every 30 seconds. *fast* — Send LACP message every second.			
min-links	Minimum number of aggregated ports that must be up.	integer	Minimum value: 1 Maximum value: 32	1
min-links-down	Action to take when less than the configured minimum number of links are active.	option	-	operational
	Option / **Description** *operational* — Set the aggregate operationally down. *administrative* — Set the aggregate administratively down.			
algorithm	Frame distribution algorithm.	option	-	L4
	Option / **Description** *L2* — Use layer 2 address for distribution. *L3* — Use layer 3 address for distribution. *L4* — Use layer 4 information for distribution.			
link-up-delay	Number of milliseconds to wait before considering a link is up.	integer	Minimum value: 50 Maximum value: 3600000	50
priority-override	Enable/disable fail back to higher priority port once recovered.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable fail back to higher priority port once recovered. *disable* / Disable fail back to higher priority port once recovered.			
aggregate	Aggregate interface.	string	Maximum length: 15	
redundant-interface	Redundant interface.	string	Maximum length: 15	
devindex	Device Index.	integer	Minimum value: 0 Maximum value: 4294967295	0
switch	Contained in switch.	string	Maximum length: 15	
description	Description.	var-string	Maximum length: 255	
alias	Alias will be displayed with the interface name to make it easier to distinguish.	string	Maximum length: 25	
security-mode	Turn on captive portal authentication for this interface.	option	-	none
	Option / **Description** *none* / No security option. *captive-portal* / Captive portal authentication. *802.1X* / 802.1X port-based authentication.			
security-mac-auth-bypass	Enable/disable MAC authentication bypass.	option	-	disable
	Option / **Description** *mac-auth-only* / Enable MAC authentication bypass without EAP. *enable* / Enable MAC authentication bypass. *disable* / Disable MAC authentication bypass.			
security-external-web	URL of external authentication web server.	var-string	Maximum length: 1023	

Parameter	Description	Type	Size	Default
security-external-logout	URL of external authentication logout server.	string	Maximum length: 127	
replacemsg-override-group	Replacement message override group.	string	Maximum length: 35	
security-redirect-url	URL redirection after disclaimer/authentication.	var-string	Maximum length: 1023	
auth-cert	HTTPS server certificate.	string	Maximum length: 35	
auth-portal-addr	Address of captive portal.	string	Maximum length: 63	
security-exempt-list	Name of security-exempt-list.	string	Maximum length: 35	
security-groups <name>	User groups that can authenticate with the captive portal. Names of user groups that can authenticate with the captive portal.	string	Maximum length: 79	
role	Interface role.	option	-	undefined

Option	Description
lan	Connected to local network of endpoints.
wan	Connected to Internet.
dmz	Connected to server zone.
undefined	Interface has no specific role.

Parameter	Description	Type	Size	Default
snmp-index	Permanent SNMP Index of the interface.	integer	Minimum value: 1 Maximum value: 2147483647	0
secondary-IP	Enable/disable adding a secondary IP to this interface.	option	-	disable

Option	Description
enable	Enable secondary IP.
disable	Disable secondary IP.

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

config client-options

Parameter	Description	Type	Size	Default
code	DHCP client option code.	integer	Minimum value: 0 Maximum value: 255	0
type	DHCP client option type.	option	-	hex

Option	Description
hex	DHCP option in hex.
string	DHCP option in string.
ip	DHCP option in IP.
fqdn	DHCP option in domain search option format.

value	DHCP client option value.	string	Maximum length: 312	
ip	DHCP option IPs.	user	Not Specified	

config secondaryip

Parameter	Description	Type	Size	Default
ip	Secondary IP address of the interface.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
allowaccess	Management access settings for the secondary IP address.	option	-	

Option	Description
ping	PING access.
https	HTTPS access.
ssh	SSH access.
snmp	SNMP access.
http	HTTP access.
telnet	TELNET access.
fgfm	FortiManager access.

Parameter	Description	Type	Size	Default
	Option / **Description** *radius-acct* / RADIUS accounting access. *probe-response* / Probe access. *fabric* / Security Fabric access. *ftm* / FTM access. *speed-test* / Speed test access.			
gwdetect	Enable/disable detect gateway alive for first.	option	-	disable
	Option / **Description** *enable* / Enable detect gateway alive for first. *disable* / Disable detect gateway alive for first.			
ping-serv-status	PING server status.	integer	Minimum value: 0 Maximum value: 255	0
detectserver	Gateway's ping server for this IP.	user	Not Specified	
detectprotocol	Protocols used to detect the server.	option	-	ping
	Option / **Description** *ping* / PING. *tcp-echo* / TCP echo. *udp-echo* / UDP echo.			
ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50	1

config tagging

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

config ipv6

Parameter	Description	Type	Size	Default
ip6-mode	Addressing mode (static, DHCP, delegated).	option	-	static
	Option / **Description** *static* — Static setting. *dhcp* — DHCPv6 client mode. *pppoe* — IPv6 over PPPoE mode. *delegated* — IPv6 address with delegated prefix.			
nd-mode	Neighbor discovery mode.	option	-	basic
	Option / **Description** *basic* — Do not support SEND. *SEND-compatible* — Support SEND.			
nd-cert	Neighbor discovery certificate.	string	Maximum length: 35	
nd-security-level	Neighbor discovery security level .	integer	Minimum value: 0 Maximum value: 7	0
nd-timestamp-delta	Neighbor discovery timestamp delta value .	integer	Minimum value: 1 Maximum value: 3600	300
nd-timestamp-fuzz	Neighbor discovery timestamp fuzz factor .	integer	Minimum value: 1 Maximum value: 60	1
nd-cga-modifier	Neighbor discovery CGA modifier.	user	Not Specified	
ip6-dns-server-override	Enable/disable using the DNS server acquired by DHCP.	option	-	enable
	Option / **Description** *enable* — Enable using the DNS server acquired by DHCP. *disable* — Disable using the DNS server acquired by DHCP.			

Parameter	Description	Type	Size	Default
ip6-address	Primary IPv6 address prefix. Syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx.	ipv6-prefix	Not Specified	::/0
ip6-allowaccess	Allow management access to the interface.	option	-	

Option	Description
ping	PING access.
https	HTTPS access.
ssh	SSH access.
snmp	SNMP access.
http	HTTP access.
telnet	TELNET access.
fgfm	FortiManager access.
fabric	Fabric access.

Parameter	Description	Type	Size	Default
ip6-send-adv	Enable/disable sending advertisements about the interface.	option	-	disable

Option	Description
enable	Enable sending advertisements about this interface.
disable	Disable sending advertisements about this interface.

Parameter	Description	Type	Size	Default
icmp6-send-redirect	Enable/disable sending of ICMPv6 redirects.	option	-	enable

Option	Description
enable	Enable sending of ICMPv6 redirects.
disable	Disable sending of ICMPv6 redirects.

Parameter	Description	Type	Size	Default
ip6-manage-flag	Enable/disable the managed flag.	option	-	disable

Option	Description
enable	Enable the managed IPv6 flag.
disable	Disable the managed IPv6 flag.

Parameter	Description	Type	Size	Default
ip6-other-flag	Enable/disable the other IPv6 flag.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable the other IPv6 flag. *disable* — Disable the other IPv6 flag.			
ip6-max-interval	IPv6 maximum interval (4 to 1800 sec).	integer	Minimum value: 4 Maximum value: 1800	600
ip6-min-interval	IPv6 minimum interval (3 to 1350 sec).	integer	Minimum value: 3 Maximum value: 1350	198
ip6-link-mtu	IPv6 link MTU.	integer	Minimum value: 1280 Maximum value: 16000	0
ra-send-mtu	Enable/disable sending link MTU in RA packet.	option	-	enable
	Option / **Description** *enable* — Enable sending link MTU in RA packet. *disable* — Disable sending link MTU in RA packet.			
ip6-reachable-time	IPv6 reachable time (milliseconds; 0 means unspecified).	integer	Minimum value: 0 Maximum value: 3600000	0
ip6-retrans-time	IPv6 retransmit time (milliseconds; 0 means unspecified).	integer	Minimum value: 0 Maximum value: 4294967295	0
ip6-default-life	Default life (sec).	integer	Minimum value: 0 Maximum value: 9000	1800
ip6-hop-limit	Hop limit (0 means unspecified).	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default
autoconf	Enable/disable address auto config.	option	-	disable
	Option / **Description** *enable* / Enable auto-configuration. *disable* / Disable auto-configuration.			
unique-autoconf-addr	Enable/disable unique auto config address.	option	-	disable
	Option / **Description** *enable* / Enable unique auto-configuration address. *disable* / Disable unique auto-configuration address.			
interface-identifier	IPv6 interface identifier.	ipv6-address	Not Specified	::
ip6-prefix-mode	Assigning a prefix from DHCP or RA.	option	-	dhcp6
	Option / **Description** *dhcp6* / Use delegated prefix from a DHCPv6 client to form a delegated IPv6 address. *ra* / Use prefix from RA to form a delegated IPv6 address.			
ip6-upstream-interface	Interface name providing delegated information.	string	Maximum length: 15	
ip6-delegated-prefix-iaid	IAID of obtained delegated-prefix from the upstream interface.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip6-subnet	Subnet to routing prefix. Syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx.	ipv6-prefix	Not Specified	::/0
dhcp6-relay-service	Enable/disable DHCPv6 relay.	option	-	disable
	Option / **Description** *disable* / Disable DHCPv6 relay *enable* / Enable DHCPv6 relay.			
dhcp6-relay-type	DHCPv6 relay type.	option	-	regular

Parameter	Description	Type	Size	Default
	Option / **Description** *regular* / Regular DHCP relay.			
dhcp6-relay-ip	DHCPv6 relay IP address.	user	Not Specified	
dhcp6-client-options	DHCPv6 client options.	option	-	
	Option / **Description** *rapid* / Send rapid commit option. *iapd* / Send including IA-PD option. *iana* / Send including IA-NA option.			
dhcp6-prefix-delegation	Enable/disable DHCPv6 prefix delegation.	option	-	disable
	Option / **Description** *enable* / Enable DHCPv6 prefix delegation. *disable* / Disable DHCPv6 prefix delegation.			
dhcp6-information-request	Enable/disable DHCPv6 information request.	option	-	disable
	Option / **Description** *enable* / Enable DHCPv6 information request. *disable* / Disable DHCPv6 information request.			
cli-conn6-status	CLI IPv6 connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0

config ip6-prefix-list

Parameter	Description	Type	Size	Default
autonomous-flag	Enable/disable the autonomous flag.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable the autonomous flag. *disable* / Disable the autonomous flag.			
onlink-flag	Enable/disable the onlink flag.	option	-	enable
	Option / **Description** *enable* / Enable the onlink flag. *disable* / Disable the onlink flag.			
valid-life-time	Valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	2592000
preferred-life-time	Preferred life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	604800
rdnss	Recursive DNS server option.	user	Not Specified	
dnssl <domain>	DNS search list option. Domain name.	string	Maximum length: 79	

config ip6-delegated-prefix-list

Parameter	Description	Type	Size	Default
upstream-interface	Name of the interface that provides delegated information.	string	Maximum length: 15	
delegated-prefix-iaid	IAID of obtained delegated-prefix from the upstream interface.	integer	Minimum value: 0 Maximum value: 4294967295	0
autonomous-flag	Enable/disable the autonomous flag.	option	-	enable
	Option / **Description** *enable* / Enable the autonomous flag. *disable* / Disable the autonomous flag.			

Parameter	Description	Type	Size	Default
onlink-flag	Enable/disable the onlink flag.	option	-	enable
	Option / **Description** *enable* — Enable the onlink flag. *disable* — Disable the onlink flag.			
subnet	Add subnet ID to routing prefix.	ipv6-network	Not Specified	::/0
rdnss-service	Recursive DNS service option.	option	-	specify
	Option / **Description** *delegated* — Delegated RDNSS settings. *default* — System RDNSS settings. *specify* — Specify recursive DNS servers.			
rdnss	Recursive DNS server option.	user	Not Specified	

config dhcp6-iapd-list

Parameter	Description	Type	Size	Default
prefix-hint	DHCPv6 prefix that will be used as a hint to the upstream DHCPv6 server.	ipv6-network	Not Specified	::/0
prefix-hint-plt	DHCPv6 prefix hint preferred life time (sec), 0 means unlimited lease time.	integer	Minimum value: 0 Maximum value: 4294967295	604800
prefix-hint-vlt	DHCPv6 prefix hint valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	2592000

config system ip-conflict status

List interface names and IP addresses in conflict.

```
config system ip-conflict status
    Description: List interface names and IP addresses in conflict.
end
```

config system ipam

Configure IP address management services.

```
config system ipam
    Description: Configure IP address management services.
    set status [enable|disable]
    set server-type [cloud|fabric-root]
    set pool-subnet {ipv4-classnet}
end
```

config system ipam

Parameter	Description	Type	Size	Default
status	Enable/disable IP address management services.	option	-	disable
	Option / **Description** *enable* — Enable integration with IP address management services. *disable* — Disable integration with IP address management services.			
server-type	Configure the type of IPAM server to use.	option	-	fabric-root
	Option / **Description** *cloud* — Use the FortiIPAM cloud server. *fabric-root* — Use the IPAM server running on the Security Fabric root.			
pool-subnet	Configure IPAM pool subnet, Class A - Class B subnet.	ipv4-classnet	Not Specified	172.31.0.0 255.255.0.0

config system ips-urlfilter-dns

Configure IPS URL filter DNS servers.

```
config system ips-urlfilter-dns
    Description: Configure IPS URL filter DNS servers.
    edit <address>
        set status [enable|disable]
        set ipv6-capability [enable|disable]
    next
end
```

config system ips-urlfilter-dns

Parameter	Description	Type	Size	Default
status	Enable/disable using this DNS server for IPS URL filter DNS queries.	option	-	enable

Option	Description
enable	Enable this DNS server for IPS URL filter DNS queries.
disable	Disable this DNS server for IPS URL filter DNS queries.

Parameter	Description	Type	Size	Default
ipv6-capability	Enable/disable this server for IPv6 queries.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

config system ips-urlfilter-dns6

Configure IPS URL filter IPv6 DNS servers.

```
config system ips-urlfilter-dns6
    Description: Configure IPS URL filter IPv6 DNS servers.
    edit <address6>
        set status [enable|disable]
    next
end
```

config system ips-urlfilter-dns6

Parameter	Description	Type	Size	Default
status	Enable/disable this server for IPv6 DNS queries.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

config system ips

Configure IPS system settings.

```
config system ips
    Description: Configure IPS system settings.
    set signature-hold-time {user}
    set override-signature-hold-by-id [enable|disable]
end
```

config system ips

Parameter	Description	Type	Size	Default
signature-hold-time	Time to hold and monitor IPS signatures. Format <#d##h> .	user	Not Specified	0h
override-signature-hold-by-id	Enable/disable override of hold of triggering signatures that are specified by IDs regardless of hold.	option	-	enable

Option	Description
enable	Allow the signatures specified by IDs to be triggered even if they are on hold.
disable	Do not trigger the signatures that are on hold.

config system ipv6-neighbor-cache

Configure IPv6 neighbor cache table.

```
config system ipv6-neighbor-cache
    Description: Configure IPv6 neighbor cache table.
    edit <id>
        set interface {string}
        set ipv6 {ipv6-address}
        set mac {mac-address}
    next
end
```

config system ipv6-neighbor-cache

Parameter	Description	Type	Size	Default
interface	Select the associated interface name from available options.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default
ipv6	IPv6 address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::
mac	MAC address (format: xx:xx:xx:xx:xx:xx).	mac-address	Not Specified	00:00:00:00:00:00

config system link-monitor

Configure Link Health Monitor.

```
config system link-monitor
    Description: Configure Link Health Monitor.
    edit <name>
        set addr-mode [ipv4|ipv6]
        set srcintf {string}
        set server-config [default|individual]
        set server <address1>, <address2>, ...
        set protocol {option1}, {option2}, ...
        set port {integer}
        set gateway-ip {ipv4-address-any}
        set gateway-ip6 {ipv6-address}
        set route <subnet1>, <subnet2>, ...
        set source-ip {ipv4-address-any}
        set source-ip6 {ipv6-address}
        set http-get {string}
        set http-agent {string}
        set http-match {string}
        set interval {integer}
        set probe-timeout {integer}
        set failtime {integer}
        set recoverytime {integer}
        set probe-count {integer}
        set security-mode [none|authentication]
        set password {password}
        set packet-size {integer}
        set ha-priority {integer}
        set fail-weight {integer}
        set update-cascade-interface [enable|disable]
        set update-static-route [enable|disable]
        set update-policy-route [enable|disable]
        set status [enable|disable]
        set diffservcode {user}
        set class-id {integer}
        set service-detection [enable|disable]
        config server-list
            Description: Servers for link-monitor to monitor.
            edit <id>
                set dst {string}
                set protocol {option1}, {option2}, ...
                set port {integer}
                set weight {integer}
```

```
            next
        end
    next
end
```

config system link-monitor

Parameter	Description	Type	Size	Default
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4
	Option / **Description** *ipv4* — IPv4 mode. *ipv6* — IPv6 mode.			
srcintf	Interface that receives the traffic to be monitored.	string	Maximum length: 15	
server-config	Mode of server configuration.	option	-	default
	Option / **Description** *default* — All servers share the same attributes. *individual* — Some attributes can be specified for individual servers.			
server <address>	IP address of the server(s) to be monitored. Server address.	string	Maximum length: 79	
protocol	Protocols used to monitor the server.	option	-	ping
	Option / **Description** *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.			
port	Port number of the traffic to be used to monitor the server.	integer	Minimum value: 1 Maximum value: 65535	0
gateway-ip	Gateway IP address used to probe the server.	ipv4-address-any	Not Specified	0.0.0.0
gateway-ip6	Gateway IPv6 address used to probe the server.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default
route <subnet>	Subnet to monitor. IP and netmask (x.x.x.x/y).	string	Maximum length: 79	
source-ip	Source IP address used in packet to the server.	ipv4-address-any	Not Specified	0.0.0.0
source-ip6	Source IPv6 address used in packet to the server.	ipv6-address	Not Specified	::
http-get	If you are monitoring an HTML server you can send an HTTP-GET request with a custom string. Use this option to define the string.	string	Maximum length: 1024	/
http-agent	String in the http-agent field in the HTTP header.	string	Maximum length: 1024	Chrome/ Safari/
http-match	String that you expect to see in the HTTP-GET requests of the traffic to be monitored.	string	Maximum length: 1024	
interval	Detection interval in milliseconds .	integer	Minimum value: 500 Maximum value: 3600000	500
probe-timeout	Time to wait before a probe packet is considered lost .	integer	Minimum value: 500 Maximum value: 5000	500
failtime	Number of retry attempts before the server is considered down .	integer	Minimum value: 1 Maximum value: 3600	5
recoverytime	Number of successful responses received before server is considered recovered .	integer	Minimum value: 1 Maximum value: 3600	5
probe-count	Number of most recent probes that should be used to calculate latency and jitter .	integer	Minimum value: 5 Maximum value: 30	30
security-mode	Twamp controller security mode.	option	-	none

Option	Description
none	Unauthenticated mode.

Parameter	Description	Type	Size	Default
	Option **Description** *authentication* Authenticated mode.			
password	TWAMP controller password in authentication mode.	password	Not Specified	
packet-size	Packet size of a TWAMP test session.	integer	Minimum value: 64 Maximum value: 1024	64
ha-priority	HA election priority .	integer	Minimum value: 1 Maximum value: 50	1
fail-weight	Threshold weight to trigger link failure alert.	integer	Minimum value: 0 Maximum value: 255	0
update-cascade-interface	Enable/disable update cascade interface.	option	-	enable
	Option **Description** *enable* Enable update cascade interface. *disable* Disable update cascade interface.			
update-static-route	Enable/disable updating the static route.	option	-	enable
	Option **Description** *enable* Enable updating the static route. *disable* Disable updating the static route.			
update-policy-route	Enable/disable updating the policy route.	option	-	enable
	Option **Description** *enable* Enable updating the policy route. *disable* Disable updating the policy route.			
status	Enable/disable this link monitor.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable this link monitor. *disable* / Disable this link monitor.			
diffservcode	Differentiated services code point (DSCP) in the IP header of the probe packet.	user	Not Specified	
class-id	Traffic class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
service-detection	Only use monitor to read quality values. If enabled, static routes and cascade interfaces will not be updated.	option	-	disable
	Option / **Description** *enable* / Only use monitor for service-detection. *disable* / Monitor will update routes/interfaces on link failure.			

config server-list

Parameter	Description	Type	Size	Default
dst	IP address of the server to be monitored.	string	Maximum length: 64	
protocol	Protocols used to monitor the server.	option	-	ping
	Option / **Description** *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.			
port	Port number of the traffic to be used to monitor the server.	integer	Minimum value: 1 Maximum value: 65535	0

Parameter	Description	Type	Size	Default
weight	Weight of the monitor to this dst .	integer	Minimum value: 0 Maximum value: 255	0

config system mac-address-table

Configure MAC address tables.

```
config system mac-address-table
    Description: Configure MAC address tables.
    edit <mac>
        set interface {string}
        set reply-substitute {mac-address}
    next
end
```

config system mac-address-table

Parameter	Description	Type	Size	Default
interface	Interface name.	string	Maximum length: 35	
reply-substitute	New MAC for reply traffic.	mac-address	Not Specified	00:00:00:00:00:00

config system management-tunnel

Management tunnel configuration.

```
config system management-tunnel
    Description: Management tunnel configuration.
    set status [enable|disable]
    set allow-config-restore [enable|disable]
    set allow-push-configuration [enable|disable]
    set allow-push-firmware [enable|disable]
    set allow-collect-statistics [enable|disable]
    set authorized-manager-only [enable|disable]
    set serial-number {user}
end
```

config system management-tunnel

Parameter	Description	Type	Size	Default
status	Enable/disable FGFM tunnel.	option	-	enable

Option	Description
enable	Enable management tunnel.
disable	Disable management tunnel.

Parameter	Description	Type	Size	Default
allow-config-restore	Enable/disable allow config restore.	option	-	enable

Option	Description
enable	Enable allow config restore.
disable	Disable allow config restore.

Parameter	Description	Type	Size	Default
allow-push-configuration	Enable/disable push configuration.	option	-	enable

Option	Description
enable	Enable push configuration.
disable	Disable push configuration.

Parameter	Description	Type	Size	Default
allow-push-firmware	Enable/disable push firmware.	option	-	enable

Option	Description
enable	Enable push firmware.
disable	Disable push firmware.

Parameter	Description	Type	Size	Default
allow-collect-statistics	Enable/disable collection of run time statistics.	option	-	enable

Option	Description
enable	Enable collection of run time statistics.
disable	Disable collection of run time statistics.

Parameter	Description	Type	Size	Default
authorized-manager-only	Enable/disable restriction of authorized manager only.	option	-	enable

Option	Description
enable	Enable restriction of authorized manager only.
disable	Disable restriction of authorized manager only.

Parameter	Description	Type	Size	Default
serial-number	Serial number.	user	Not Specified	

config system mgmt-csum

System checksum for FortiManager use only.

```
config system mgmt-csum
    Description: System checksum for FortiManager use only.
end
```

config system nethsm

Configure system nethsm.

```
config system nethsm
    Description: Configure system nethsm.
    set status [enable|disable]
    set vendor {option}
    set interface {string}
    set receivetimeout {integer}
    config servers
        Description: NetHSM server list.
        edit <name>
            set server {string}
            set port {integer}
            set server-cert {user}
            set htl [enable|disable]
        next
    end
    config slots
        Description: NetHSM slot list.
        edit <name>
            set id {integer}
            set password {password}
            set for-ha [yes|no]
        next
    end
    set ha [enable|disable]
    set ha-status-pulling-interval {integer}
    config hagroups
        Description: NetHSM HA group list.
        edit <name>
            set member <name1>, <name2>, ...
        next
    end
    set rsa-mech-remap [enable|disable]
end
```

config system nethsm

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	Option / **Description** *enable* / Enable system network HSM. *disable* / Disable system network HSM.			
vendor	Vendor.	option	-	SafeNet
	Option / **Description** *SafeNet* / SafeNet			
interface	Outgoing interface	string	Maximum length: 15	
receivetimeout	Receive timeout, specified in ms .	integer	Minimum value: 0 Maximum value: 4294967295	20000
ha	HA option .	option	-	disable
	Option / **Description** *enable* / Enable HA. *disable* / Disable HA.			
ha-status-pulling-interval	Interval to pull HA status in minutes .	integer	Minimum value: 0 Maximum value: 60	1
rsa-mech-remap	RSA Mechanism Remap option . Enable it if Luna server is running in FIPS mode and firmware version is 6.22.* or greater.	option	-	disable
	Option / **Description** *enable* / Enable RSA Mechanism Remap. *disable* / Disable RSA Mechanism Remap.			

config servers

Parameter	Description	Type	Size	Default
server	{<name_str|ip_str>} NetHSM server domain name or IP.	string	Maximum length: 63	
port	NetHSM server port .	integer	Minimum value: 1 Maximum value: 65535	1792
server-cert	NetHSM server certificate.	user	Not Specified	
htl	HTL option .	option	-	disable

Option	Description
enable	Enable HTL.
disable	Disable HTL.

config slots

Parameter	Description	Type	Size	Default
id	NetHSM slot ID .	integer	Minimum value: 0 Maximum value: 4294967295	0
password	NetHSM slot access password.	password	Not Specified	
for-ha	HA option.	option	-	no

Option	Description
yes	HA slot.
no	Regular slot.

config hagroups

Parameter	Description	Type	Size	Default
member <name>	HA group members. NetHSM HA group member (slot names).	string	Maximum length: 79	

config system network-visibility

Configure network visibility settings.

```
config system network-visibility
    Description: Configure network visibility settings.
    set destination-visibility [disable|enable]
    set source-location [disable|enable]
    set destination-hostname-visibility [disable|enable]
    set hostname-ttl {integer}
    set hostname-limit {integer}
    set destination-location [disable|enable]
end
```

config system network-visibility

Parameter	Description	Type	Size	Default
destination-visibility	Enable/disable logging of destination visibility.	option	-	enable
	Option / **Description** *disable* — Disable logging of destination visibility. *enable* — Enable logging of destination visibility.			
source-location	Enable/disable logging of source geographical location visibility.	option	-	enable
	Option / **Description** *disable* — Disable logging of source geographical location visibility. *enable* — Enable logging of source geographical location visibility.			
destination-hostname-visibility	Enable/disable logging of destination hostname visibility.	option	-	enable
	Option / **Description** *disable* — Disable logging of destination hostname visibility. *enable* — Enable logging of destination hostname visibility.			
hostname-ttl	TTL of hostname table entries .	integer	Minimum value: 60 Maximum value: 86400	86400

Parameter	Description	Type	Size	Default
hostname-limit	Limit of the number of hostname table entries .	integer	Minimum value: 0 Maximum value: 50000	5000
destination-location	Enable/disable logging of destination geographical location visibility.	option	-	enable

Option	Description
disable	Disable logging of destination geographical location visibility.
enable	Enable logging of destination geographical location visibility.

config system ntp

Configure system NTP information.

```
config system ntp
    Description: Configure system NTP information.
    set ntpsync [enable|disable]
    set type [fortiguard|custom]
    set syncinterval {integer}
    config ntpserver
        Description: Configure the FortiProxy to connect to any available third-party NTP
server.
        edit <id>
            set server {string}
            set ntpv3 [enable|disable]
            set authentication [enable|disable]
            set key {password}
            set key-id {integer}
            set interface-select-method [auto|sdwan|...]
            set interface {string}
        next
    end
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set server-mode [enable|disable]
    set authentication [enable|disable]
    set key-type [MD5|SHA1]
    set key {password}
    set key-id {integer}
    set interface <interface-name1>, <interface-name2>, ...
end
```

config system ntp

Parameter	Description	Type	Size	Default
ntpsync	Enable/disable setting the FortiProxy system time by synchronizing with an NTP Server.	option	-	disable
	Option / **Description** *enable* — Enable synchronization with NTP Server. *disable* — Disable synchronization with NTP Server.			
type	Use the FortiGuard NTP server or any other available NTP Server.	option	-	fortiguard
	Option / **Description** *fortiguard* — Use the FortiGuard NTP server. *custom* — Use any other available NTP server.			
syncinterval	NTP synchronization interval .	integer	Minimum value: 1 Maximum value: 1440	60
source-ip	Source IP address for communication to the NTP server.	ipv4-address	Not Specified	0.0.0.0
source-ip6	Source IPv6 address for communication to the NTP server.	ipv6-address	Not Specified	::
server-mode	Enable/disable FortiProxy NTP Server Mode. Your FortiProxy becomes an NTP server for other devices on your network. The FortiProxy relays NTP requests to its configured NTP server.	option	-	disable
	Option / **Description** *enable* — Enable FortiProxy NTP Server Mode. *disable* — Disable FortiProxy NTP Server Mode.			
authentication	Enable/disable authentication.	option	-	disable
	Option / **Description** *enable* — Enable authentication. *disable* — Disable authentication.			
key-type	Key type for authentication (MD5, SHA1).	option	-	MD5

Parameter	Description	Type	Size	Default
	Option / **Description** *MD5* / Use MD5 to authenticate the message. *SHA1* / Use SHA1 to authenticate the message.			
key	Key for authentication.	password	Not Specified	
key-id	Key ID for authentication.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface <interface-name>	FortiProxy interface(s) with NTP server mode enabled. Devices on your network can contact these interfaces for NTP services. Interface name.	string	Maximum length: 79	

config ntpserver

Parameter	Description	Type	Size	Default
server	IP address or hostname of the NTP Server.	string	Maximum length: 63	
ntpv3	Enable to use NTPv3 instead of NTPv4.	option	-	disable
	Option / **Description** *enable* / Enable NTPv3. *disable* / Disable NTPv3 (use NTPv4).			
authentication	Enable/disable MD5(NTPv3)/SHA1(NTPv4) authentication.	option	-	disable
	Option / **Description** *enable* / Enable MD5(NTPv3)/SHA1(NTPv4) authentication. *disable* / Disable MD5(NTPv3)/SHA1(NTPv4) authentication.			
key	Key for MD5(NTPv3)/SHA1(NTPv4) authentication.	password	Not Specified	
key-id	Key ID for authentication.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config system object-tagging

Configure object tagging.

```
config system object-tagging
    Description: Configure object tagging.
    edit <category>
        set address [disable|mandatory|...]
        set device [disable|mandatory|...]
        set interface [disable|mandatory|...]
        set multiple [enable|disable]
        set color {integer}
        set tags <name1>, <name2>, ...
    next
end
```

config system object-tagging

Parameter	Description	Type	Size	Default
address	Address.	option	-	optional
	Option / **Description** *disable* — Disable. *mandatory* — Mandatory. *optional* — Optional.			
device	Device.	option	-	optional

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* / Disable. *mandatory* / Mandatory. *optional* / Optional.			
interface	Interface.	option	-	optional
	Option / **Description** *disable* / Disable. *mandatory* / Mandatory. *optional* / Optional.			
multiple	Allow multiple tag selection.	option	-	enable
	Option / **Description** *enable* / Enable multi-tagging. *disable* / Disable multi-tagging.			
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config system password-policy-guest-admin

Configure the password policy for guest administrators.

```
config system password-policy-guest-admin
    Description: Configure the password policy for guest administrators.
    set status [enable|disable]
    set apply-to {option1}, {option2}, ...
    set minimum-length {integer}
    set min-lower-case-letter {integer}
    set min-upper-case-letter {integer}
    set min-non-alphanumeric {integer}
    set min-number {integer}
    set min-change-characters {integer}
    set expire-status [enable|disable]
    set expire-day {integer}
    set reuse-password [enable|disable]
```

```
    set password-history {integer}
end
```

config system password-policy-guest-admin

Parameter	Description	Type	Size	Default
status	Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.	option	-	disable
	Option / **Description** *enable* — Enable password policy. *disable* — Disable password policy.			
apply-to	Guest administrator to which this password policy applies.	option	-	guest-admin-password
	Option / **Description** *guest-admin-password* — Apply to guest administrator password.			
minimum-length	Minimum password length .	integer	Minimum value: 8 Maximum value: 128	8
min-lower-case-letter	Minimum number of lowercase characters in password .	integer	Minimum value: 0 Maximum value: 128	0
min-upper-case-letter	Minimum number of uppercase characters in password .	integer	Minimum value: 0 Maximum value: 128	0
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password .	integer	Minimum value: 0 Maximum value: 128	0
min-number	Minimum number of numeric characters in password .	integer	Minimum value: 0 Maximum value: 128	0

Parameter	Description	Type	Size	Default
min-change-characters	Minimum number of unique characters in new password which do not exist in old password .	integer	Minimum value: 0 Maximum value: 128	0
expire-status	Enable/disable password expiration.	option	-	disable
	Option / **Description** *enable* — Passwords expire after expire-day days. *disable* — Passwords do not expire.			
expire-day	Number of days after which passwords expire .	integer	Minimum value: 1 Maximum value: 999	90
reuse-password	Enable/disable reuse of password. If both reuse-password and min-change-characters are enabled, min-change-characters overrides.	option	-	enable
	Option / **Description** *enable* — Administrators are allowed to reuse the same password. *disable* — Administrators must create a new password.			
password-history	Number of previous passwords that cannot be reused.	integer	Minimum value: 2 Maximum value: 20	2

config system password-policy

Configure password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.

```
config system password-policy
    Description: Configure password policy for locally defined administrator passwords and
IPsec VPN pre-shared keys.
    set status [enable|disable]
    set apply-to {option1}, {option2}, ...
    set minimum-length {integer}
    set min-lower-case-letter {integer}
    set min-upper-case-letter {integer}
    set min-non-alphanumeric {integer}
    set min-number {integer}
    set min-change-characters {integer}
    set expire-status [enable|disable]
    set expire-day {integer}
```

```
    set reuse-password [enable|disable]
    set password-history {integer}
end
```

config system password-policy

Parameter	Description	Type	Size	Default
status	Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.	option	-	disable
	Option / **Description** *enable* — Enable password policy. *disable* — Disable password policy.			
apply-to	Apply password policy to administrator passwords or IPsec pre-shared keys or both. Separate entries with a space.	option	-	admin-password
	Option / **Description** *admin-password* — Apply to administrator passwords. *ipsec-preshared-key* — Apply to IPsec pre-shared keys.			
minimum-length	Minimum password length .	integer	Minimum value: 8 Maximum value: 128	8
min-lower-case-letter	Minimum number of lowercase characters in password .	integer	Minimum value: 0 Maximum value: 128	0
min-upper-case-letter	Minimum number of uppercase characters in password .	integer	Minimum value: 0 Maximum value: 128	0
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password .	integer	Minimum value: 0 Maximum value: 128	0

Parameter	Description	Type	Size	Default
min-number	Minimum number of numeric characters in password .	integer	Minimum value: 0 Maximum value: 128	0
min-change-characters	Minimum number of unique characters in new password which do not exist in old password .	integer	Minimum value: 0 Maximum value: 128	0
expire-status	Enable/disable password expiration.	option	-	disable
	Option / **Description** *enable* — Passwords expire after expire-day days. *disable* — Passwords do not expire.			
expire-day	Number of days after which passwords expire .	integer	Minimum value: 1 Maximum value: 999	90
reuse-password	Enable/disable reuse of password. If both reuse-password and min-change-characters are enabled, min-change-characters overrides.	option	-	enable
	Option / **Description** *enable* — Administrators are allowed to reuse the same password. *disable* — Administrators must create a new password.			
password-history	Number of previous passwords that cannot be reused.	integer	Minimum value: 2 Maximum value: 20	2

config system performance status

System performance status.

```
config system performance status
    Description: System performance status.
end
```

config system performance top

Display information about the top CPU processes.

```
config system performance top
    Description: Display information about the top CPU processes.
    set <delay> {string}
end
```

config system performance top

Parameter	Description	Type	Size	Default
<delay>	Delay in seconds .	string	Maximum length: -1	

config system probe-response

Configure system probe response.

```
config system probe-response
    Description: Configure system probe response.
    set port {integer}
    set http-probe-value {string}
    set ttl-mode [reinit|decrease|...]
    set mode [none|http-probe|...]
    set security-mode [none|authentication]
    set password {password}
    set timeout {integer}
end
```

config system probe-response

Parameter	Description	Type	Size	Default
port	Port number to response.	integer	Minimum value: 1 Maximum value: 65535	8008
http-probe-value	Value to respond to the monitoring server.	string	Maximum length: 1024	OK
ttl-mode	Mode for TWAMP packet TTL modification.	option	-	retain

Parameter	Description	Type	Size	Default
	Option / **Description** *reinit* / Reinitialize TTL. *decrease* / Decrease TTL. *retain* / Retain TTL.			
mode	SLA response mode.	option	-	none
	Option / **Description** *none* / Disable probe. *http-probe* / HTTP probe. *twamp* / Two way active measurement protocol.			
security-mode	TWAMP responder security mode.	option	-	none
	Option / **Description** *none* / Unauthenticated mode. *authentication* / Authenticated mode.			
password	TWAMP responder password in authentication mode.	password	Not Specified	
timeout	An inactivity timer for a twamp test session.	integer	Minimum value: 10 Maximum value: 3600	300

config system proxy-arp

Configure proxy-ARP.

```
config system proxy-arp
    Description: Configure proxy-ARP.
    edit <id>
        set interface {string}
        set ip {ipv4-address}
        set end-ip {ipv4-address}
    next
end
```

config system proxy-arp

Parameter	Description	Type	Size	Default
interface	Interface acting proxy-ARP.	string	Maximum length: 15	
ip	IP address or start IP to be proxied.	ipv4-address	Not Specified	0.0.0.0
end-ip	End IP of IP range to be proxied.	ipv4-address	Not Specified	0.0.0.0

config system ptp

Configure system PTP information.

```
config system ptp
    Description: Configure system PTP information.
    set status [enable|disable]
    set mode [multicast|hybrid]
    set delay-mechanism [E2E|P2P]
    set request-interval {integer}
    set interface {string}
    set server-mode [enable|disable]
    config server-interface
        Description: FortiGate interface(s) with PTP server mode enabled. Devices on your
network can contact these interfaces for PTP services.
        edit <id>
            set server-interface-name {string}
            set delay-mechanism [E2E|P2P]
        next
    end
end
```

config system ptp

Parameter	Description	Type	Size	Default
status	Enable/disable setting the FortiProxy system time by synchronizing with an PTP Server.	option	-	disable
	Option / **Description** *enable* — Enable synchronization with PTP Server. *disable* — Disable synchronization with PTP Server.			
mode	Multicast transmission or hybrid transmission.	option	-	multicast

Parameter	Description	Type	Size	Default
	Option / **Description** *multicast* / Send PTP packets with multicast. *hybrid* / Send PTP packets with unicast and multicast.			
delay-mechanism	End to end delay detection or peer to peer delay detection.	option	-	E2E
	Option / **Description** *E2E* / End to end delay detection. *P2P* / Peer to peer delay detection.			
request-interval	The delay request value is the logarithmic mean interval in seconds between the delay request messages sent by the slave to the master.	integer	Minimum value: 1 Maximum value: 6	1
interface	PTP client will reply through this interface.	string	Maximum length: 15	
server-mode	Enable/disable FortiGate PTP server mode. Your FortiGate becomes an PTP server for other devices on your network.	option	-	disable
	Option / **Description** *enable* / Enable FortiGate PTP server mode. *disable* / Disable FortiGate PTP server mode.			

config server-interface

Parameter	Description	Type	Size	Default
server-interface-name	Interface name.	string	Maximum length: 15	
delay-mechanism	End to end delay detection or peer to peer delay detection.	option	-	E2E
	Option / **Description** *E2E* / End to end delay detection. *P2P* / Peer to peer delay detection.			

config system replacemsg-group

Configure replacement message groups.

```
config system replacemsg-group
    Description: Configure replacement message groups.
    edit <name>
        set comment {var-string}
        set group-type [default|utm|...]
        config mail
            Description: Replacement message table entries.
            edit <msg-type>
                set buffer {var-string}
                set header [none|http|...]
                set format [none|text|...]
            next
        end
        config http
            Description: Replacement message table entries.
            edit <msg-type>
                set buffer {var-string}
                set header [none|http|...]
                set format [none|text|...]
            next
        end
        config webproxy
            Description: Replacement message table entries.
            edit <msg-type>
                set buffer {var-string}
                set header [none|http|...]
                set format [none|text|...]
            next
        end
        config ftp
            Description: Replacement message table entries.
            edit <msg-type>
                set buffer {var-string}
                set header [none|http|...]
                set format [none|text|...]
            next
        end
        config fortiguard-wf
            Description: Replacement message table entries.
            edit <msg-type>
                set buffer {var-string}
                set header [none|http|...]
                set format [none|text|...]
            next
        end
        config spam
            Description: Replacement message table entries.
            edit <msg-type>
                set buffer {var-string}
                set header [none|http|...]
                set format [none|text|...]
```

```
    next
end
config alertmail
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config admin
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config auth
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config sslvpn
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config nac-quar
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config traffic-quota
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config utm
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
```

```
            next
        end
        config custom-message
            Description: Replacement message table entries.
            edit <msg-type>
                set buffer {var-string}
                set header [none|http|...]
                set format [none|text|...]
            next
        end
        config icap
            Description: Replacement message table entries.
            edit <msg-type>
                set buffer {var-string}
                set header [none|http|...]
                set format [none|text|...]
            next
        end
        config automation
            Description: Replacement message table entries.
            edit <msg-type>
                set buffer {var-string}
                set header [none|http|...]
                set format [none|text|...]
            next
        end
    next
end
```

config system replacemsg-group

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
group-type	Group type.	option	-	default

Option	Description
default	Per-vdom replacement messages.
utm	For use with UTM settings in firewall policies.
auth	For use with authentication pages in firewall policies.

config mail

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config http

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config webproxy

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config ftp

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config fortiguard-wf

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config spam

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config alertmail

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config admin

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config auth

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config sslvpn

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config nac-quar

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config traffic-quota

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config utm

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config custom-message

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config icap

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config automation

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg-image

Configure replacement message images.

```
config system replacemsg-image
    Description: Configure replacement message images.
    edit <name>
        set image-type [gif|jpg|...]
        set image-base64 {var-string}
    next
end
```

config system replacemsg-image

Parameter	Description	Type	Size	Default
image-type	Image type.	option	-	png
	Option / **Description** *gif* — GIF image. *jpg* — JPEG image. *tiff* — TIFF image. *png* — PNG image.			
image-base64	Image data.	var-string	Maximum length: 32768	

config system replacemsg admin

Replacement messages.

```
config system replacemsg admin
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg admin

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg alertmail

Replacement messages.

```
config system replacemsg alertmail
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg alertmail

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	

Parameter	Description	Type	Size	Default
	Option / **Description** *none* — No header type. *http* — HTTP *8bit* — 8 bit.			
format	Format flag.	option	-	
	Option / **Description** *none* — No format type. *text* — Text format. *html* — HTML format.			

config system replacemsg auth

Replacement messages.

```
config system replacemsg auth
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg auth

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
	Option / **Description** *none* — No header type. *http* — HTTP *8bit* — 8 bit.			
format	Format flag.	option	-	

Parameter	Description	Type	Size	Default
	Option — **Description** *none* — No format type. *text* — Text format. *html* — HTML format.			

config system replacemsg automation

Replacement messages.

```
config system replacemsg automation
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg automation

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
	Option — **Description** *none* — No header type. *http* — HTTP *8bit* — 8 bit.			
format	Format flag.	option	-	
	Option — **Description** *none* — No format type. *text* — Text format. *html* — HTML format.			

config system replacemsg fortiguard-wf

Replacement messages.

```
config system replacemsg fortiguard-wf
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg fortiguard-wf

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg ftp

Replacement messages.

```
config system replacemsg ftp
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
```

```
    next
end
```

config system replacemsg ftp

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg http

Replacement messages.

```
config system replacemsg http
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg http

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg icap

Replacement messages.

```
config system replacemsg icap
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg icap

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	

Parameter	Description	Type	Size	Default
	Option / **Description** *none* — No header type. *http* — HTTP *8bit* — 8 bit.			
format	Format flag.	option	-	
	Option / **Description** *none* — No format type. *text* — Text format. *html* — HTML format.			

config system replacemsg mail

Replacement messages.

```
config system replacemsg mail
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg mail

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
	Option / **Description** *none* — No header type. *http* — HTTP *8bit* — 8 bit.			
format	Format flag.	option	-	

Parameter	Description	Type	Size	Default
	Option / **Description** *none* — No format type. *text* — Text format. *html* — HTML format.			

config system replacemsg nac-quar

Replacement messages.

```
config system replacemsg nac-quar
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg nac-quar

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
	Option / **Description** *none* — No header type. *http* — HTTP *8bit* — 8 bit.			
format	Format flag.	option	-	
	Option / **Description** *none* — No format type. *text* — Text format. *html* — HTML format.			

config system replacemsg spam

Replacement messages.

```
config system replacemsg spam
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg spam

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg sslvpn

Replacement messages.

```
config system replacemsg sslvpn
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
```

```
    next
end
```

config system replacemsg sslvpn

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg traffic-quota

Replacement messages.

```
config system replacemsg traffic-quota
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg traffic-quota

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg utm

Replacement messages.

```
config system replacemsg utm
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg utm

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	

Parameter	Description	Type	Size	Default
	Option / **Description** *none* — No header type. *http* — HTTP *8bit* — 8 bit.			
format	Format flag.	option	-	
	Option / **Description** *none* — No format type. *text* — Text format. *html* — HTML format.			

config system replacemsg webproxy

Replacement messages.

```
config system replacemsg webproxy
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg webproxy

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
	Option / **Description** *none* — No header type. *http* — HTTP *8bit* — 8 bit.			
format	Format flag.	option	-	

Parameter	Description	Type	Size	Default
	Option — **Description** *none* — No format type. *text* — Text format. *html* — HTML format.			

config system resource-limits

Configure resource limits.

```
config system resource-limits
    Description: Configure resource limits.
    set session {integer}
    set ipsec-phase1-interface {integer}
    set ipsec-phase2-interface {integer}
    set firewall-policy {integer}
    set firewall-address {integer}
    set firewall-addrgrp {integer}
    set custom-service {integer}
    set service-group {integer}
    set onetime-schedule {integer}
    set recurring-schedule {integer}
    set user {integer}
    set user-group {integer}
    set sslvpn {integer}
    set proxy {integer}
    set log-disk-quota {integer}
end
```

config system resource-limits

Parameter	Description	Type	Size	Default
session	Maximum number of sessions.	integer	Minimum value: 0 Maximum value: 4294967295	
ipsec-phase1-interface	Maximum number of VPN IPsec phase1 interface tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
ipsec-phase2-interface	Maximum number of VPN IPsec phase2 interface tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
firewall-policy	Maximum number of firewall policies (policy, DoS-policy4, DoS-policy6, multicast).	integer	Minimum value: 0 Maximum value: 4294967295	
firewall-address	Maximum number of firewall addresses (IPv4, IPv6, multicast).	integer	Minimum value: 0 Maximum value: 4294967295	
firewall-addrgrp	Maximum number of firewall address groups (IPv4, IPv6).	integer	Minimum value: 0 Maximum value: 4294967295	
custom-service	Maximum number of firewall custom services.	integer	Minimum value: 0 Maximum value: 4294967295	
service-group	Maximum number of firewall service groups.	integer	Minimum value: 0 Maximum value: 4294967295	
onetime-schedule	Maximum number of firewall one-time schedules.	integer	Minimum value: 0 Maximum value: 4294967295	
recurring-schedule	Maximum number of firewall recurring schedules.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
user	Maximum number of local users.	integer	Minimum value: 0 Maximum value: 4294967295	
user-group	Maximum number of user groups.	integer	Minimum value: 0 Maximum value: 4294967295	
sslvpn	Maximum number of SSL-VPN.	integer	Minimum value: 0 Maximum value: 4294967295	
proxy	Maximum number of concurrent proxy users.	integer	Minimum value: 0 Maximum value: 4294967295	
log-disk-quota	Log disk quota in megabytes (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0

config system saml

Global settings for SAML authentication.

```
config system saml
    Description: Global settings for SAML authentication.
    set status [enable|disable]
    set role [identity-provider|service-provider]
    set default-login-page [normal|sso]
    set default-profile {string}
    set cert {string}
    set binding-protocol [post|redirect]
    set portal-url {string}
    set entity-id {string}
    set single-sign-on-url {string}
    set single-logout-url {string}
    set idp-entity-id {string}
    set idp-single-sign-on-url {string}
    set idp-single-logout-url {string}
```

```
        set idp-cert {string}
        set server-address {string}
        set tolerance {integer}
        set life {integer}
        config service-providers
            Description: Authorized service providers.
            edit <name>
                set prefix {string}
                set sp-binding-protocol [post|redirect]
                set sp-cert {string}
                set sp-entity-id {string}
                set sp-single-sign-on-url {string}
                set sp-single-logout-url {string}
                set sp-portal-url {string}
                set idp-entity-id {string}
                set idp-single-sign-on-url {string}
                set idp-single-logout-url {string}
                config assertion-attributes
                    Description: Customized SAML attributes to send along with assertion.
                    edit <name>
                        set type [username|email|...]
                    next
                end
            next
        end
    end
```

config system saml

Parameter	Description	Type	Size	Default
status	Enable/disable SAML authentication .	option	-	disable
	Option / **Description** *enable* — Enable SAML authentication. *disable* — Disable SAML authentication.			
role	SAML role.	option	-	service-provider
	Option / **Description** *identity-provider* — Identity Provider. *service-provider* — Service Provider.			
default-login-page	Choose default login page.	option	-	normal
	Option / **Description** *normal* — Use local login page as default.			

Parameter	Description	Type	Size	Default
	Option / **Description** *sso* / Use IdP's Single Sign-On page as default.			
default-profile	Default profile for new SSO admin.	string	Maximum length: 35	
cert	Certificate to sign SAML messages.	string	Maximum length: 35	
binding-protocol	IdP Binding protocol.	option	-	redirect
	Option / **Description** *post* / HTTP POST binding. *redirect* / HTTP Redirect binding.			
portal-url	SP portal URL.	string	Maximum length: 255	
entity-id	SP entity ID.	string	Maximum length: 255	
single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255	
single-logout-url	SP single logout URL.	string	Maximum length: 255	
idp-entity-id	IDP entity ID.	string	Maximum length: 255	
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255	
idp-single-logout-url	IDP single logout URL.	string	Maximum length: 255	
idp-cert	IDP certificate name.	string	Maximum length: 35	
server-address	Server address.	string	Maximum length: 63	
tolerance	Tolerance to the range of time when the assertion is valid (in minutes).	integer	Minimum value: 0 Maximum value: 4294967295	5

Parameter	Description	Type	Size	Default
life	Length of the range of time when the assertion is valid (in minutes).	integer	Minimum value: 0 Maximum value: 4294967295	30

config service-providers

Parameter	Description	Type	Size	Default
prefix	Prefix.	string	Maximum length: 35	
sp-binding-protocol	SP binding protocol.	option	-	post

Option	Description
post	HTTP POST binding.
redirect	HTTP Redirect binding.

Parameter	Description	Type	Size	Default
sp-cert	SP certificate name.	string	Maximum length: 35	
sp-entity-id	SP entity ID.	string	Maximum length: 255	
sp-single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255	
sp-single-logout-url	SP single logout URL.	string	Maximum length: 255	
sp-portal-url	SP portal URL.	string	Maximum length: 255	
idp-entity-id	IDP entity ID.	string	Maximum length: 255	
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255	
idp-single-logout-url	IDP single logout URL.	string	Maximum length: 255	

config assertion-attributes

Parameter	Description	Type	Size	Default
type	Type.	option	-	username

Parameter	Description	Type	Size	Default

Option	Description
username	User Name.
email	Email Address.
profile-name	Profile Name.

config system sdn-connector

Configure connection to SDN Connector.

```
config system sdn-connector
    Description: Configure connection to SDN Connector.
    edit <name>
        set status [disable|enable]
        set type [aci|alicloud|...]
        set use-metadata-iam [disable|enable]
        set ha-status [disable|enable]
        set verify-certificate [disable|enable]
        set server {string}
        set server-list <ip1>, <ip2>, ...
        set server-port {integer}
        set username {string}
        set password {password_aes256}
        set vcenter-server {string}
        set vcenter-username {string}
        set vcenter-password {password_aes256}
        set access-key {string}
        set secret-key {password}
        set region {string}
        set vpc-id {string}
        config external-account-list
            Description: Configure AWS external account list.
            edit <role-arn>
                set region-list <region1>, <region2>, ...
            next
        end
        set tenant-id {string}
        set client-id {string}
        set client-secret {password}
        set subscription-id {string}
        set resource-group {string}
        set login-endpoint {string}
        set resource-url {string}
        set azure-region [global|china|...]
        config nic
            Description: Configure Azure network interface.
            edit <name>
                config ip
                    Description: Configure IP configuration.
```

```
            edit <name>
                set public-ip {string}
                set resource-group {string}
            next
        end
    next
end
config route-table
    Description: Configure Azure route table.
    edit <name>
        set subscription-id {string}
        set resource-group {string}
        config route
            Description: Configure Azure route.
            edit <name>
                set next-hop {string}
            next
        end
    next
end
set user-id {string}
set compartment-id {string}
set oci-region {string}
set oci-region-type [commercial|government]
set oci-cert {string}
set oci-fingerprint {string}
config external-ip
    Description: Configure GCP external IP.
    edit <name>
    next
end
config route
    Description: Configure GCP route.
    edit <name>
    next
end
config gcp-project-list
    Description: Configure GCP project list.
    edit <id>
        set gcp-zone-list <name1>, <name2>, ...
    next
end
config forwarding-rule
    Description: Configure GCP forwarding rule.
    edit <rule-name>
        set target {string}
    next
end
set service-account {string}
set private-key {user}
set secret-token {user}
set domain {string}
set group-name {string}
set api-key {password}
set compute-generation {integer}
set ibm-region [dallas|washington-dc|...]
```

```
        set update-interval {integer}
    next
end
```

config system sdn-connector

Parameter	Description	Type	Size	Default
status	Enable/disable connection to the remote SDN connector.	option	-	enable

Option	Description
disable	Disable connection to this SDN Connector.
enable	Enable connection to this SDN Connector.

Parameter	Description	Type	Size	Default
type	Type of SDN connector.	option	-	aws

Option	Description
aci	Application Centric Infrastructure (ACI).
alicloud	AliCloud Service (ACS).
aws	Amazon Web Services (AWS).
azure	Microsoft Azure.
gcp	Google Cloud Platform (GCP).
nsx	VMware NSX.
nuage	Nuage VSP.
oci	Oracle Cloud Infrastructure.
openstack	OpenStack.
kubernetes	Kubernetes.
vmware	VMware vSphere (vCenter & ESXi).
sepm	Symantec Endpoint Protection Manager.
aci-direct	Application Centric Infrastructure (ACI Direct Connection).
ibm	IBM Cloud Infrastructure.
nutanix	Nutanix Prism Central.

Parameter	Description	Type	Size	Default
use-metadata-iam	Enable/disable use of IAM role from metadata to call API.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* — Disable using IAM role to call API. *enable* — Enable using IAM role to call API.			
ha-status	Enable/disable use for FortiProxy HA service.	option	-	disable
	Option / **Description** *disable* — Disable use for FortiProxy HA service. *enable* — Enable use for FortiProxy HA service.			
verify-certificate	Enable/disable server certificate verification.	option	-	enable
	Option / **Description** *disable* — Disable server certificate verification. *enable* — Enable server certificate verification.			
server	Server address of the remote SDN connector.	string	Maximum length: 127	
server-list <ip>	Server address list of the remote SDN connector. IPv4 address.	string	Maximum length: 15	
server-port	Port number of the remote SDN connector.	integer	Minimum value: 0 Maximum value: 65535	0
username	Username of the remote SDN connector as login credentials.	string	Maximum length: 64	
password	Password of the remote SDN connector as login credentials.	password_aes256	Not Specified	
vcenter-server	vCenter server address for NSX quarantine.	string	Maximum length: 127	
vcenter-username	vCenter server username for NSX quarantine.	string	Maximum length: 64	
vcenter-password	vCenter server password for NSX quarantine.	password_aes256	Not Specified	
access-key	AWS / ACS access key ID.	string	Maximum length: 31	

Parameter	Description	Type	Size	Default
secret-key	AWS / ACS secret access key.	password	Not Specified	
region	AWS / ACS region name.	string	Maximum length: 31	
vpc-id	AWS VPC ID.	string	Maximum length: 31	
tenant-id	Tenant ID (directory ID).	string	Maximum length: 127	
client-id	Azure client ID (application ID).	string	Maximum length: 63	
client-secret	Azure client secret (application key).	password	Not Specified	
subscription-id	Azure subscription ID.	string	Maximum length: 63	
resource-group	Azure resource group.	string	Maximum length: 63	
login-endpoint	Azure Stack login endpoint.	string	Maximum length: 127	
resource-url	Azure Stack resource URL.	string	Maximum length: 127	
azure-region	Azure server region.	option	-	global

Option	Description
global	Global Azure Server.
china	China Azure Server.
germany	Germany Azure Server.
usgov	US Government Azure Server.
local	Azure Stack Local Server.

user-id	User ID.	string	Maximum length: 127	
compartment-id	Compartment ID.	string	Maximum length: 127	
oci-region	OCI server region.	string	Maximum length: 31	
oci-region-type	OCI region type.	option	-	commercial

Parameter	Description	Type	Size	Default
	Option / **Description** *commercial* — Commercial region. *government* — Government region.			
oci-cert	OCI certificate.	string	Maximum length: 63	
oci-fingerprint	OCI pubkey fingerprint.	string	Maximum length: 63	
service-account	GCP service account email.	string	Maximum length: 127	
private-key	Private key of GCP service account.	user	Not Specified	
secret-token	Secret token of Kubernetes service account.	user	Not Specified	
domain	Domain name.	string	Maximum length: 127	
group-name	Group name of computers.	string	Maximum length: 127	
api-key	IBM cloud API key or service ID API key.	password	Not Specified	
compute-generation	Compute generation for IBM cloud infrastructure.	integer	Minimum value: 1 Maximum value: 2	2
ibm-region	IBM cloud region name.	option	-	dallas
	Option / **Description** *dallas* — US South (Dallas) Public Endpoint. *washington-dc* — US East (Washington DC) Public Endpoint. *london* — United Kingdom (London) Public Endpoint. *frankfurt* — Germany (Frankfurt) Public Endpoint. *sydney* — Australia (Sydney) Public Endpoint. *tokyo* — Japan (Tokyo) Public Endpoint. *osaka* — Japan (Osaka) Public Endpoint. *toronto* — Canada (Toronto) Public Endpoint. *sao-paulo* — Brazil (Sao Paulo) Public Endpoint.			

Parameter	Description	Type	Size	Default
update-interval	Dynamic object update interval .	integer	Minimum value: 0 Maximum value: 3600	60

config external-account-list

Parameter	Description	Type	Size	Default
region-list <region>	AWS region name list. AWS region name.	string	Maximum length: 31	

config ip

Parameter	Description	Type	Size	Default
public-ip	Public IP name.	string	Maximum length: 63	
resource-group	Resource group of Azure public IP.	string	Maximum length: 63	

config route-table

Parameter	Description	Type	Size	Default
subscription-id	Subscription ID of Azure route table.	string	Maximum length: 63	
resource-group	Resource group of Azure route table.	string	Maximum length: 63	

config route

Parameter	Description	Type	Size	Default
next-hop	Next hop address.	string	Maximum length: 127	

config route

Parameter	Description	Type	Size	Default
next-hop	Next hop address.	string	Maximum length: 127	

config gcp-project-list

Parameter	Description	Type	Size	Default
gcp-zone-list <name>	Configure GCP zone list. GCP zone name.	string	Maximum length: 127	

config forwarding-rule

Parameter	Description	Type	Size	Default
target	Target instance name.	string	Maximum length: 63	

config system session-ttl

Configure global session TTL timers for this FortiProxy.

```
config system session-ttl
    Description: Configure global session TTL timers for this FortiProxy.
    set default {user}
    config port
        Description: Session TTL port.
        edit <id>
            set protocol {integer}
            set start-port {integer}
            set end-port {integer}
            set timeout {user}
        next
    end
end
```

config system session-ttl

Parameter	Description	Type	Size	Default
default	Default timeout.	user	Not Specified	

config port

Parameter	Description	Type	Size	Default
protocol	Protocol .	integer	Minimum value: 0 Maximum value: 255	0
start-port	Start port number.	integer	Minimum value: 0 Maximum value: 65535	0
end-port	End port number.	integer	Minimum value: 0 Maximum value: 65535	0
timeout	Session timeout (TTL).	user	Not Specified	

config system session

System IPv4 session.

```
config system session
    Description: System IPv4 session.
end
```

config system session6

System IPv6 session.

```
config system session6
    Description: System IPv6 session.
end
```

config system settings

Configure VDOM settings.

```
config system settings
    Description: Configure VDOM settings.
    set comments {var-string}
    set opmode [nat|transparent]
    set http-external-dest [fortiweb|forticache]
    set firewall-session-dirty [check-all|check-new|...]
    set manageip {user}
    set gateway {ipv4-address}
    set ip {ipv4-classnet-host}
    set manageip6 {ipv6-prefix}
    set gateway6 {ipv6-address}
    set ip6 {ipv6-prefix}
    set device {string}
    set utf8-spam-tagging [enable|disable]
    set wccp-cache-engine [enable|disable]
    set wccp-local-route [enable|disable]
    set vpn-stats-log {option1}, {option2}, ...
    set vpn-stats-period {integer}
    set mac-ttl {integer}
    set fw-session-hairpin [enable|disable]
    set prp-trailer-action [enable|disable]
    set snat-hairpin-traffic [enable|disable]
    set dhcp-proxy [enable|disable]
    set dhcp-proxy-interface-select-method [auto|sdwan|...]
    set dhcp-proxy-interface {string}
    set dhcp-server-ip {user}
    set dhcp6-server-ip {user}
    set gui-default-policy-columns <name1>, <name2>, ...
    set link-down-access [enable|disable]
    set asymroute [enable|disable]
    set asymroute-icmp [enable|disable]
    set tcp-session-without-syn [enable|disable]
    set ses-denied-traffic [enable|disable]
    set strict-src-check [enable|disable]
    set allow-linkdown-path [enable|disable]
    set asymroute6 [enable|disable]
    set asymroute6-icmp [enable|disable]
    set sctp-session-without-init [enable|disable]
    set status [enable|disable]
    set allow-subnet-overlap [enable|disable]
    set deny-tcp-with-icmp [enable|disable]
    set discovered-device-timeout {integer}
    set email-portal-check-dns [disable|enable]
    set gui-icap [enable|disable]
    set gui-implicit-policy [enable|disable]
    set gui-dns-database [enable|disable]
    set gui-multicast-policy [enable|disable]
    set gui-dos-policy [enable|disable]
    set gui-object-colors [enable|disable]
    set gui-voip-profile [enable|disable]
    set gui-security-profile-group [enable|disable]
    set gui-local-reports [enable|disable]
    set gui-wanopt-cache [enable|disable]
    set gui-explicit-proxy [enable|disable]
    set gui-sslvpn-personal-bookmarks [enable|disable]
    set gui-sslvpn-realms [enable|disable]
```

```
    set gui-policy-based-ipsec [enable|disable]
    set gui-threat-weight [enable|disable]
    set gui-spamfilter [enable|disable]
    set gui-file-filter [enable|disable]
    set gui-application-control [enable|disable]
    set gui-ips [enable|disable]
    set gui-endpoint-control [enable|disable]
    set gui-endpoint-control-advanced [enable|disable]
    set gui-dhcp-advanced [enable|disable]
    set gui-vpn [enable|disable]
    set gui-webfilter-advanced [enable|disable]
    set gui-traffic-shaping [enable|disable]
    set gui-antivirus [enable|disable]
    set gui-webfilter [enable|disable]
    set gui-videofilter [enable|disable]
    set gui-dnsfilter [enable|disable]
    set gui-advanced-policy [enable|disable]
    set gui-allow-unnamed-policy [enable|disable]
    set gui-email-collection [enable|disable]
    set gui-multiple-interface-policy [enable|disable]
    set gui-policy-disclaimer [enable|disable]
    set gui-ztna [enable|disable]
    set block-land-attack [disable|enable]
    set application-bandwidth-tracking [disable|enable]
end
```

config system settings

Parameter	Description	Type	Size	Default
comments	VDOM comments.	var-string	Maximum length: 255	
opmode	Firewall operation mode (NAT or Transparent).	option	-	nat

Option	Description
nat	Change to NAT mode.
transparent	Change to transparent mode.

Parameter	Description	Type	Size	Default
http-external-dest	Offload HTTP traffic to FortiWeb or FortiCache.	option	-	fortiweb

Option	Description
fortiweb	Offload HTTP traffic to FortiWeb for Web Application Firewall inspection.
forticache	Offload HTTP traffic to FortiCache for external web caching and WAN optimization.

Parameter	Description	Type	Size	Default
firewall-session-dirty	Select how to manage sessions affected by firewall policy configuration changes.	option	-	check-all

Parameter	Description	Type	Size	Default
	Option / **Description** *check-all* — All sessions affected by a firewall policy change are flushed from the session table. When new packets are recived they are re-evaluated by stateful inspection and re-added to the session table. *check-new* — Estabished sessions for changed firewall policies continue without being affected by the policy configuration change. New sessions are evaluated according to the new firewall policy configuration. *check-policy-option* — Sessions are managed individually depending on the firewall policy. Some sessions may restart. Some may continue.			
manageip	Transparent mode IPv4 management IP address and netmask.	user	Not Specified	
gateway	Transparent mode IPv4 default gateway IP address.	ipv4-address	Not Specified	0.0.0.0
ip	IP address and netmask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
manageip6	Transparent mode IPv6 management IP address and netmask.	ipv6-prefix	Not Specified	::/0
gateway6	Transparent mode IPv4 default gateway IP address.	ipv6-address	Not Specified	::
ip6	IPv6 address prefix for NAT mode.	ipv6-prefix	Not Specified	::/0
device	Interface to use for management access for NAT mode.	string	Maximum length: 35	
utf8-spam-tagging	Enable/disable converting antispam tags to UTF-8 for better non-ASCII character support.	option	-	enable
	Option / **Description** *enable* — Convert antispam tags to UTF-8. *disable* — Do not convert antispam tags.			
wccp-cache-engine	Enable/disable WCCP cache engine.	option	-	disable
	Option / **Description** *enable* — Enable WCCP cache engine. *disable* — Disable WCCP cache engine.			

Parameter	Description	Type	Size	Default
wccp-local-route	Enable/disable WCCP to use local route.	option	-	disable

Option	Description
enable	Enable WCCP to use local route.
disable	Disable WCCP to use local route.

Parameter	Description	Type	Size	Default
vpn-stats-log	Enable/disable periodic VPN log statistics for one or more types of VPN. Separate names with a space.	option	-	ipsec pptp l2tp ssl

Option	Description
ipsec	IPsec.
pptp	PPTP.
l2tp	L2TP.
ssl	SSL.

Parameter	Description	Type	Size	Default
vpn-stats-period	Period to send VPN log statistics .	integer	Minimum value: 0 Maximum value: 4294967295	600
mac-ttl	Duration of MAC addresses in Transparent mode .	integer	Minimum value: 300 Maximum value: 8640000	300
fw-session-hairpin	Enable/disable checking for a matching policy each time hairpin traffic goes through the FortiProxy.	option	-	disable

Option	Description
enable	Perform a policy check every time.
disable	Perform a policy check only the first time the session is received.

Parameter	Description	Type	Size	Default
prp-trailer-action	Enable/disable action to take on PRP trailer.	option	-	disable

Option	Description
enable	Try to keep PRP trailer.
disable	Trim PRP trailer.

Parameter	Description	Type	Size	Default
snat-hairpin-traffic	Enable/disable source NAT (SNAT) for hairpin traffic.	option	-	enable
	Option / **Description** *enable* / Enable SNAT for hairpin traffic. *disable* / Disable SNAT for hairpin traffic.			
dhcp-proxy	Enable/disable the DHCP Proxy.	option	-	disable
	Option / **Description** *enable* / Enable the DHCP proxy. *disable* / Disable the DHCP proxy.			
dhcp-proxy-interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* / Set outgoing interface automatically. *sdwan* / Set outgoing interface by SD-WAN or policy routing rules. *specify* / Set outgoing interface manually.			
dhcp-proxy-interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
dhcp-server-ip	DHCP Server IPv4 address.	user	Not Specified	
dhcp6-server-ip	DHCPv6 server IPv6 address.	user	Not Specified	
gui-default-policy-columns `<name>`	Default columns to display for policy lists on GUI. Select column name.	string	Maximum length: 79	
link-down-access	Enable/disable link down access traffic.	option	-	enable
	Option / **Description** *enable* / Allow link down access traffic. *disable* / Block link down access traffic.			
asymroute	Enable/disable IPv4 asymmetric routing.	option	-	disable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable IPv4 asymmetric routing. *disable* Disable IPv4 asymmetric routing.			
asymroute-icmp	Enable/disable ICMP asymmetric routing.	option	-	disable
	Option **Description** *enable* Enable ICMP asymmetric routing. *disable* Disable ICMP asymmetric routing.			
tcp-session-without-syn	Enable/disable allowing TCP session without SYN flags.	option	-	disable
	Option **Description** *enable* Allow TCP session without SYN flags. *disable* Do not allow TCP session without SYN flags.			
ses-denied-traffic	Enable/disable including denied session in the session table.	option	-	disable
	Option **Description** *enable* Include denied sessions in the session table. *disable* Do not add denied sessions to the session table.			
strict-src-check	Enable/disable strict source verification.	option	-	disable
	Option **Description** *enable* Enable strict source verification. *disable* Disable strict source verification.			
allow-linkdown-path	Enable/disable link down path.	option	-	disable
	Option **Description** *enable* Allow link down path. *disable* Do not allow link down path.			
asymroute6	Enable/disable asymmetric IPv6 routing.	option	-	disable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable asymmetric IPv6 routing. *disable* Disable asymmetric IPv6 routing.			
asymroute6-icmp	Enable/disable asymmetric ICMPv6 routing.	option	-	disable
	Option **Description** *enable* Enable asymmetric ICMPv6 routing. *disable* Disable asymmetric ICMPv6 routing.			
sctp-session-without-init	Enable/disable SCTP session creation without SCTP INIT.	option	-	disable
	Option **Description** *enable* Enable SCTP session creation without SCTP INIT. *disable* Disable SCTP session creation without SCTP INIT.			
status	Enable/disable this VDOM.	option	-	enable
	Option **Description** *enable* Enable this VDOM. *disable* Disable this VDOM.			
allow-subnet-overlap	Enable/disable allowing interface subnets to use overlapping IP addresses.	option	-	disable
	Option **Description** *enable* Enable overlapping subnets. *disable* Disable overlapping subnets.			
deny-tcp-with-icmp	Enable/disable denying TCP by sending an ICMP communication prohibited packet.	option	-	disable
	Option **Description** *enable* Deny TCP with ICMP. *disable* Disable denying TCP with ICMP.			

Parameter	Description	Type	Size	Default
discovered-device-timeout	Timeout for discovered devices .	integer	Minimum value: 1 Maximum value: 365	28
email-portal-check-dns	Enable/disable using DNS to validate email addresses collected by a captive portal.	option	-	enable
	Option / **Description** *disable* — Disable email address checking with DNS. *enable* — Enable email address checking with DNS.			
gui-icap	Enable/disable ICAP on the GUI.	option	-	enable
	Option / **Description** *enable* — Enable ICAP on the GUI. *disable* — Disable ICAP on the GUI.			
gui-implicit-policy	Enable/disable implicit firewall policies on the GUI.	option	-	enable
	Option / **Description** *enable* — Enable implicit firewall policies on the GUI. *disable* — Disable implicit firewall policies on the GUI.			
gui-dns-database	Enable/disable DNS database settings on the GUI.	option	-	disable
	Option / **Description** *enable* — Enable DNS database settings on the GUI. *disable* — Disable DNS database settings on the GUI.			
gui-multicast-policy	Enable/disable multicast firewall policies on the GUI.	option	-	disable
	Option / **Description** *enable* — Enable multicast firewall policies on the GUI. *disable* — Disable multicast firewall policies on the GUI.			
gui-dos-policy	Enable/disable DoS policies on the GUI.	option	-	disable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable DoS policies on the GUI. *disable* Disable DoS policies on the GUI.			
gui-object-colors	Enable/disable object colors on the GUI.	option	-	enable
	Option **Description** *enable* Enable object colors on the GUI. *disable* Disable object colors on the GUI.			
gui-voip-profile	Enable/disable VoIP profiles on the GUI.	option	-	disable
	Option **Description** *enable* Enable VoIP profiles on the GUI. *disable* Disable VoIP profiles on the GUI.			
gui-security-profile-group	Enable/disable Security Profile Groups on the GUI.	option	-	enable
	Option **Description** *enable* Enable Security Profile Groups on the GUI. *disable* Disable Security Profile Groups on the GUI.			
gui-local-reports	Enable/disable local reports on the GUI.	option	-	disable
	Option **Description** *enable* Enable local reports on the GUI. *disable* Disable local reports on the GUI.			
gui-wanopt-cache	Enable/disable WAN Optimization and Web Caching on the GUI.	option	-	enable
	Option **Description** *enable* Enable WAN Optimization and Web Caching on the GUI. *disable* Disable WAN Optimization and Web Caching on the GUI.			
gui-explicit-proxy	Enable/disable the explicit proxy on the GUI.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable the explicit proxy on the GUI. *disable* — Disable the explicit proxy on the GUI.			
gui-sslvpn-personal-bookmarks	Enable/disable SSL-VPN personal bookmark management on the GUI.	option	-	disable
	Option / **Description** *enable* — Enable SSL-VPN personal bookmark management on the GUI. *disable* — Disable SSL-VPN personal bookmark management on the GUI.			
gui-sslvpn-realms	Enable/disable SSL-VPN realms on the GUI.	option	-	disable
	Option / **Description** *enable* — Enable SSL-VPN realms on the GUI. *disable* — Disable SSL-VPN realms on the GUI.			
gui-policy-based-ipsec	Enable/disable policy-based IPsec VPN on the GUI.	option	-	disable
	Option / **Description** *enable* — Enable policy-based IPsec VPN on the GUI. *disable* — Disable policy-based IPsec VPN on the GUI.			
gui-threat-weight	Enable/disable threat weight on the GUI.	option	-	enable
	Option / **Description** *enable* — Enable threat weight on the GUI. *disable* — Disable threat weight on the GUI.			
gui-spamfilter	Enable/disable Antispam on the GUI.	option	-	disable
	Option / **Description** *enable* — Enable Antispam on the GUI. *disable* — Disable Antispam on the GUI.			
gui-file-filter	Enable/disable File-filter on the GUI.	option	-	enable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable File-filter on the GUI. *disable* Disable File-filter on the GUI.			
gui-application-control	Enable/disable application control on the GUI.	option	-	enable
	Option **Description** *enable* Enable application control on the GUI. *disable* Disable application control on the GUI.			
gui-ips	Enable/disable IPS on the GUI.	option	-	enable
	Option **Description** *enable* Enable IPS on the GUI. *disable* Disable IPS on the GUI.			
gui-endpoint-control	Enable/disable endpoint control on the GUI.	option	-	disable
	Option **Description** *enable* Enable endpoint control on the GUI. *disable* Disable endpoint control on the GUI.			
gui-endpoint-control-advanced	Enable/disable advanced endpoint control options on the GUI.	option	-	disable
	Option **Description** *enable* Enable advanced endpoint control options on the GUI. *disable* Disable advanced endpoint control options on the GUI.			
gui-dhcp-advanced	Enable/disable advanced DHCP options on the GUI.	option	-	enable
	Option **Description** *enable* Enable advanced DHCP options on the GUI. *disable* Disable advanced DHCP options on the GUI.			
gui-vpn	Enable/disable VPN tunnels on the GUI.	option	-	enable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable VPN tunnels on the GUI. *disable* Disable VPN tunnels on the GUI.			
gui-webfilter-advanced	Enable/disable advanced web filtering on the GUI.	option	-	enable
	Option **Description** *enable* Enable advanced web filtering on the GUI. *disable* Disable advanced web filtering on the GUI.			
gui-traffic-shaping	Enable/disable traffic shaping on the GUI.	option	-	enable
	Option **Description** *enable* Enable traffic shaping on the GUI. *disable* Disable traffic shaping on the GUI.			
gui-antivirus	Enable/disable AntiVirus on the GUI.	option	-	enable
	Option **Description** *enable* Enable AntiVirus on the GUI. *disable* Disable AntiVirus on the GUI.			
gui-webfilter	Enable/disable Web filtering on the GUI.	option	-	enable
	Option **Description** *enable* Enable Web filtering on the GUI. *disable* Disable Web filtering on the GUI.			
gui-videofilter	Enable/disable Video filtering on the GUI.	option	-	enable
	Option **Description** *enable* Enable Video filtering on the GUI. *disable* Disable Video filtering on the GUI.			
gui-dnsfilter	Enable/disable DNS Filtering on the GUI.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable DNS Filtering on the GUI. *disable* — Disable DNS Filtering on the GUI.			
gui-advanced-policy	Enable/disable advanced policy configuration on the GUI.	option	-	disable
	Option / **Description** *enable* — Enable advanced policy configuration on the GUI. *disable* — Disable advanced policy configuration on the GUI.			
gui-allow-unnamed-policy	Enable/disable the requirement for policy naming on the GUI.	option	-	enable
	Option / **Description** *enable* — Enable the requirement for policy naming on the GUI. *disable* — Disable the requirement for policy naming on the GUI.			
gui-email-collection	Enable/disable email collection on the GUI.	option	-	disable
	Option / **Description** *enable* — Enable email collection on the GUI. *disable* — Disable email collection on the GUI.			
gui-multiple-interface-policy	Enable/disable adding multiple interfaces to a policy on the GUI.	option	-	enable
	Option / **Description** *enable* — Enable adding multiple interfaces to a policy on the GUI. *disable* — Disable adding multiple interfaces to a policy on the GUI.			
gui-policy-disclaimer	Enable/disable policy disclaimer on the GUI.	option	-	disable
	Option / **Description** *enable* — Enable policy disclaimer on the GUI. *disable* — Disable policy disclaimer on the GUI.			

Parameter	Description	Type	Size	Default
gui-ztna	Enable/disable Zero Trust Network Access features on the GUI.	option	-	enable

Option	Description
enable	Enable Zero Trust Network Access features on the GUI.
disable	Disable Zero Trust Network Access features on the GUI.

Parameter	Description	Type	Size	Default
block-land-attack	Enable/disable blocking of land attacks.	option	-	disable

Option	Description
disable	Do not block land attack.
enable	Block land attack.

Parameter	Description	Type	Size	Default
application-bandwidth-tracking	Enable/disable application bandwidth tracking.	option	-	disable

Option	Description
disable	Disable application bandwidth tracking.
enable	Enable application bandwidth tracking.

config system sms-server

Configure SMS server for sending SMS messages to support user authentication.

```
config system sms-server
    Description: Configure SMS server for sending SMS messages to support user
authentication.
    edit <name>
        set mail-server {string}
    next
end
```

config system sms-server

Parameter	Description	Type	Size	Default
mail-server	Email-to-SMS server domain name.	string	Maximum length: 63	

config system snmp community

SNMP community configuration.

```
config system snmp community
    Description: SNMP community configuration.
    edit <id>
        set name {string}
        set status [enable|disable]
        config hosts
            Description: Configure IPv4 SNMP managers (hosts).
            edit <id>
                set source-ip {ipv4-address}
                set ip {user}
                set ha-direct [enable|disable]
                set host-type [any|query|...]
            next
        end
        config hosts6
            Description: Configure IPv6 SNMP managers.
            edit <id>
                set source-ipv6 {ipv6-address}
                set ipv6 {ipv6-prefix}
                set ha-direct [enable|disable]
                set host-type [any|query|...]
            next
        end
        set query-v1-status [enable|disable]
        set query-v1-port {integer}
        set query-v2c-status [enable|disable]
        set query-v2c-port {integer}
        set trap-v1-status [enable|disable]
        set trap-v1-lport {integer}
        set trap-v1-rport {integer}
        set trap-v2c-status [enable|disable]
        set trap-v2c-lport {integer}
        set trap-v2c-rport {integer}
        set events {option1}, {option2}, ...
    next
end
```

config system snmp community

Parameter	Description	Type	Size	Default
name	Community name.	string	Maximum length: 35	
status	Enable/disable this SNMP community.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
query-v1-port	SNMP v1 query port .	integer	Minimum value: 1 Maximum value: 65535	161
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
query-v2c-port	SNMP v2c query port .	integer	Minimum value: 0 Maximum value: 65535	161
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
trap-v1-lport	SNMP v1 trap local port .	integer	Minimum value: 1 Maximum value: 65535	162

Parameter	Description	Type	Size	Default
trap-v1-rport	SNMP v1 trap remote port .	integer	Minimum value: 1 Maximum value: 65535	162
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
trap-v2c-lport	SNMP v2c trap local port .	integer	Minimum value: 1 Maximum value: 65535	162
trap-v2c-rport	SNMP v2c trap remote port .	integer	Minimum value: 1 Maximum value: 65535	162

Parameter	Description	Type	Size	Default
events	SNMP trap events.	option	-	cpu-high mem-low log-full intf-ip vpn-tun-up vpn-tun-down ha-switch ha-hb-failure ips-signature ips-anomaly av-virus av-oversize av-pattern av-fragmented fm-if-change ha-member-up ha-member-down ent-conf-change av-conserve av-bypass av-oversize-passed av-oversize-blocked ips-pkg-update ips-fail-open faz-disconnect load-balance-real-server-down per-cpu-high dhcp pool-usage

Option	Description
cpu-high	Send a trap when CPU usage is high.
mem-low	Send a trap when available memory is low.
log-full	Send a trap when log disk space becomes low.
intf-ip	Send a trap when an interface IP address is changed.
vpn-tun-up	Send a trap when a VPN tunnel comes up.

Parameter	Description	Type	Size	Default

Option	Description
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 FortiProxy administrator and the FortiProxy is managed by FortiManager.
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 FortiProxy enters conserve mode.
av-bypass	Send a trap when the FortiProxy enters bypass mode.
av-oversize-passed	Send a trap when AntiVirus passes an oversized file.
av-oversize-blocked	Send a trap when AntiVirus blocks an oversized file.
ips-pkg-update	Send a trap when the IPS signature database or engine is updated.
ips-fail-open	Send a trap when the IPS network buffer is full.
faz-disconnect	Send a trap when a FortiAnalyzer disconnects from the FortiProxy.
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.
dhcp	Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.
pool-usage	Send a trap about ippool usage.

config hosts

Parameter	Description	Type	Size	Default
source-ip	Source IPv4 address for SNMP traps.	ipv4-address	Not Specified	0.0.0.0
ip	IPv4 address of the SNMP manager (host).	user	Not Specified	
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
host-type	Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both. No traps will be sent when IP type is subnet.	option	-	any

Option	Description
any	Accept queries from and send traps to this SNMP manager.
query	Accept queries from this SNMP manager but do not send traps.
trap	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.

config hosts6

Parameter	Description	Type	Size	Default
source-ipv6	Source IPv6 address for SNMP traps.	ipv6-address	Not Specified	::
ipv6	SNMP manager IPv6 address prefix.	ipv6-prefix	Not Specified	::/0
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
host-type	Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both.	option	-	any

Parameter	Description	Type	Size	Default
	Option / **Description** *any* — Accept queries from and send traps to this SNMP manager. *query* — Accept queries from this SNMP manager but do not send traps. *trap* — Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.			

config system snmp sysinfo

SNMP system info configuration.

```
config system snmp sysinfo
    Description: SNMP system info configuration.
    set status [enable|disable]
    set engine-id-type [text|hex|...]
    set engine-id {string}
    set description {var-string}
    set contact-info {var-string}
    set location {var-string}
    set trap-high-cpu-threshold {integer}
    set trap-low-memory-threshold {integer}
    set trap-log-full-threshold {integer}
end
```

config system snmp sysinfo

Parameter	Description	Type	Size	Default
status	Enable/disable SNMP.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
engine-id-type	Local SNMP engineID type (text/hex/mac).	option	-	text
	Option / **Description** *text* — Text format. *hex* — Octets format. *mac* — MAC address format.			

Parameter	Description	Type	Size	Default
engine-id	Local SNMP engineID string (maximum 27 characters).	string	Maximum length: 54	
description	System description.	var-string	Maximum length: 255	
contact-info	Contact information.	var-string	Maximum length: 255	
location	System location.	var-string	Maximum length: 255	
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	80
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	80
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	90

config system snmp user

SNMP user configuration.

```
config system snmp user
    Description: SNMP user configuration.
    edit <name>
        set status [enable|disable]
        set trap-status [enable|disable]
        set trap-lport {integer}
        set trap-rport {integer}
        set queries [enable|disable]
        set query-port {integer}
        set notify-hosts {ipv4-address}
        set notify-hosts6 {ipv6-address}
        set source-ip {ipv4-address}
        set source-ipv6 {ipv6-address}
        set ha-direct [enable|disable]
        set events {option1}, {option2}, ...
        set security-level [no-auth-no-priv|auth-no-priv|...]
        set auth-proto [md5|sha|...]
        set auth-pwd {password}
        set priv-proto [aes|des|...]
        set priv-pwd {password}
```

```
    next
end
```

config system snmp user

Parameter	Description	Type	Size	Default
status	Enable/disable this SNMP user.	option	-	enable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
trap-status	Enable/disable traps for this SNMP user.	option	-	enable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
trap-lport	SNMPv3 local trap port .	integer	Minimum value: 0 Maximum value: 65535	162
trap-rport	SNMPv3 trap remote port .	integer	Minimum value: 0 Maximum value: 65535	162
queries	Enable/disable SNMP queries for this user.	option	-	enable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
query-port	SNMPv3 query port .	integer	Minimum value: 0 Maximum value: 65535	161
notify-hosts	SNMP managers to send notifications (traps) to.	ipv4-address	Not Specified	

Parameter	Description	Type	Size	Default
notify-hosts6	IPv6 SNMP managers to send notifications (traps) to.	ipv6-address	Not Specified	
source-ip	Source IP for SNMP trap.	ipv4-address	Not Specified	0.0.0.0
source-ipv6	Source IPv6 for SNMP trap.	ipv6-address	Not Specified	::
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
events	SNMP notifications (traps) to send.	option	-	cpu-high mem-low log-full intf-ip vpn-tun-up vpn-tun-down ha-switch ha-hb-failure ips-signature ips-anomaly av-virus av-oversize av-pattern av-fragmented fm-if-change ha-member-up ha-member-down ent-conf-change av-conserve av-bypass av-oversize-passed av-oversize-blocked ips-pkg-update ips-fail-open faz-disconnect load-balance-real-server-down per-cpu-high dhcp pool-usage

Option	Description
cpu-high	Send a trap when CPU usage is high.
mem-low	Send a trap when available memory is low.
log-full	Send a trap when log disk space becomes low.
intf-ip	Send a trap when an interface IP address is changed.
vpn-tun-up	Send a trap when a VPN tunnel comes up.

Parameter	Description	Type	Size	Default

Option	Description
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 FortiProxy administrator and the FortiProxy is managed by FortiManager.
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 FortiProxy enters conserve mode.
av-bypass	Send a trap when the FortiProxy enters bypass mode.
av-oversize-passed	Send a trap when AntiVirus passes an oversized file.
av-oversize-blocked	Send a trap when AntiVirus blocks an oversized file.
ips-pkg-update	Send a trap when the IPS signature database or engine is updated.
ips-fail-open	Send a trap when the IPS network buffer is full.
faz-disconnect	Send a trap when a FortiAnalyzer disconnects from the FortiProxy.
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.
dhcp	Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.

Parameter	Description	Type	Size	Default
	Option / **Description** *pool-usage* / Send a trap about ippool usage.			
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv
	Option / **Description** *no-auth-no-priv* / Message with no authentication and no privacy (encryption). *auth-no-priv* / Message with authentication but no privacy (encryption). *auth-priv* / Message with authentication and privacy (encryption).			
auth-proto	Authentication protocol.	option	-	sha
	Option / **Description** *md5* / HMAC-MD5-96 authentication protocol. *sha* / HMAC-SHA-96 authentication protocol. *sha224* / HMAC-SHA224 authentication protocol. *sha256* / HMAC-SHA256 authentication protocol. *sha384* / HMAC-SHA384 authentication protocol. *sha512* / HMAC-SHA512 authentication protocol.			
auth-pwd	Password for authentication protocol.	password	Not Specified	
priv-proto	Privacy (encryption) protocol.	option	-	aes
	Option / **Description** *aes* / CFB128-AES-128 symmetric encryption protocol. *des* / CBC-DES symmetric encryption protocol. *aes256* / CFB128-AES-256 symmetric encryption protocol. *aes256cisco* / CFB128-AES-256 symmetric encryption protocol compatible with CISCO.			
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified	

config system source-ip status

Show configured service source-IP.

```
config system source-ip status
    Description: Show configured service source-IP.
end
```

config system span-port

Configure SPAN port.

```
config system span-port
    Description: Configure SPAN port.
    edit <id>
        set status [disable|enable]
        set span-source-port {string}
        set span-dest-port {string}
        set span-direction [rx|tx|...]
    next
end
```

config system span-port

Parameter	Description	Type	Size	Default
status	Enable/disable SPAN.	option	-	disable
	Option / **Description** *disable* — Disable SPAN. *enable* — Enable SPAN.			
span-source-port	SPAN source ports.	string	Maximum length: 15	
span-dest-port	SPAN destination port.	string	Maximum length: 15	
span-direction	SPAN direction.	option	-	both
	Option / **Description** *rx* — Span receive direction only. *tx* — Span transmit direction only. *both* — Span both directions.			

config system speed-test-schedule

Speed test schedule for each interface.

```
config system speed-test-schedule
    Description: Speed test schedule for each interface.
    edit <interface>
        set status [disable|enable]
        set diffserv {user}
        set server-name {string}
        set schedules <name1>, <name2>, ...
        set dynamic-server [disable|enable]
        set update-inbandwidth [disable|enable]
        set update-outbandwidth [disable|enable]
        set update-inbandwidth-maximum {integer}
        set update-inbandwidth-minimum {integer}
        set update-outbandwidth-maximum {integer}
        set update-outbandwidth-minimum {integer}
    next
end
```

config system speed-test-schedule

Parameter	Description	Type	Size	Default
status	Enable/disable scheduled speed test.	option	-	enable
	Option / **Description** *disable* — Disable scheduled speed test. *enable* — Enable scheduled speed test.			
diffserv	DSCP used for speed test.	user	Not Specified	
server-name	Speed test server name.	string	Maximum length: 35	
schedules <name>	Schedules for the interface. Name of a firewall recurring schedule.	string	Maximum length: 31	
dynamic-server	Enable/disable dynamic server option.	option	-	disable
	Option / **Description** *disable* — Disable dynamic server. *enable* — Enable dynamic server.The speed test server will be found automatically.			
update-inbandwidth	Enable/disable bypassing interface's inbound bandwidth setting.	option	-	disable
	Option / **Description** *disable* — Honor interface's inbandwidth shaping. *enable* — Ignore interface's inbandwidth shaping.			

Parameter	Description	Type	Size	Default
update-outbandwidth	Enable/disable bypassing interface's outbound bandwidth setting.	option	-	disable
	Option / **Description** *disable* — Honor interface's outbandwidth shaping. *enable* — Ignore updating interface's outbandwidth shaping.			
update-inbandwidth-maximum	Maximum downloading bandwidth (kbps) to be used in a speed test.	integer	Minimum value: 0 Maximum value: 16776000	0
update-inbandwidth-minimum	Minimum downloading bandwidth (kbps) to be considered effective.	integer	Minimum value: 0 Maximum value: 16776000	0
update-outbandwidth-maximum	Maximum uploading bandwidth (kbps) to be used in a speed test.	integer	Minimum value: 0 Maximum value: 16776000	0
update-outbandwidth-minimum	Minimum uploading bandwidth (kbps) to be considered effective.	integer	Minimum value: 0 Maximum value: 16776000	0

config system speed-test-server

Configure speed test server list.

```
config system speed-test-server
    Description: Configure speed test server list.
    edit <name>
        set timestamp {integer}
        config host
            Description: Hosts of the server.
            edit <id>
                set ip {ipv4-address}
                set port {integer}
                set user {string}
                set password {password}
            next
        end
```

```
    next
end
```

config system speed-test-server

Parameter	Description	Type	Size	Default
timestamp	Speed test server timestamp.	integer	Minimum value: 0 Maximum value: 4294967295	0

config host

Parameter	Description	Type	Size	Default
ip	Server host IPv4 address.	ipv4-address	Not Specified	0.0.0.0
port	Server host port number to communicate with client.	integer	Minimum value: 1 Maximum value: 65535	5204
user	Speed test host user name.	string	Maximum length: 64	
password	Speed test host password.	password	Not Specified	

config system sso-admin

Configure SSO admin users.

```
config system sso-admin
    Description: Configure SSO admin users.
    edit <name>
        set accprofile {string}
        set vdom <name1>, <name2>, ...
    next
end
```

config system sso-admin

Parameter	Description	Type	Size	Default
accprofile	SSO admin user access profile.	string	Maximum length: 35	
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	

config system sso-forticloud-admin

Configure FortiCloud SSO admin users.

```
config system sso-forticloud-admin
    Description: Configure FortiCloud SSO admin users.
    edit <name>
        set vdom <name1>, <name2>, ...
    next
end
```

config system sso-forticloud-admin

Parameter	Description	Type	Size	Default
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	

config system startup-error-log

Display startup config error on console.

```
config system startup-error-log
    Description: Display startup config error on console.
end
```

config system status

System status.

```
config system status
    Description: System status.
end
```

config system storage

Configure logical storage.

```
config system storage
    Description: Configure logical storage.
    edit <name>
        set status [enable|disable]
        set media-status [enable|disable|...]
        set order {integer}
        set partition {string}
        set device {string}
        set size {integer}
        set usage [log|wanopt]
        set wanopt-mode [mix|wanopt|...]
    next
end
```

config system storage

Parameter	Description	Type	Size	Default
status	Enable/disable storage.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
media-status	The physical status of current media.	option	-	disable
	Option / **Description** *enable* — Storage is enabled. *disable* — Storage is disabled. *fail* — Storage have some fail sector.			
order	Set storage order.	integer	Minimum value: 0 Maximum value: 255	0
partition	Label of underlying partition.	string	Maximum length: 16	<unknown>
device	Partition device.	string	Maximum length: 19	?

Parameter	Description	Type	Size	Default
size	Partition size.	integer	Minimum value: 0 Maximum value: 4294967295	0
usage	Use hard disk for logging or WAN Optimization .	option	-	log

Option	Description
log	Use hard disk for logging.
wanopt	Use hard disk for WAN Optimization.

Parameter	Description	Type	Size	Default
wanopt-mode	WAN Optimization mode	option	-	webcache

Option	Description
mix	Use hard disk for WAN Optimization mix mode.
wanopt	Use hard disk for WAN Optimization wanopt mode.
webcache	Use hard disk for WAN Optimization webcache mode.

config system vdom-dns

Configure DNS servers for a non-management VDOM.

```
config system vdom-dns
    Description: Configure DNS servers for a non-management VDOM.
    set vdom-dns [enable|disable]
    set primary {ipv4-address}
    set secondary {ipv4-address}
    set protocol {option1}, {option2}, ...
    set ssl-certificate {string}
    set server-hostname <hostname1>, <hostname2>, ...
    set ip6-primary {ipv6-address}
    set ip6-secondary {ipv6-address}
    set source-ip {ipv4-address}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
    set server-select-method [least-rtt|failover]
    set alt-primary {ipv4-address}
    set alt-secondary {ipv4-address}
end
```

config system vdom-dns

Parameter	Description	Type	Size	Default
vdom-dns	Enable/disable configuring DNS servers for the current VDOM.	option	-	disable
	Option / **Description** *enable* — Enable configuring DNS servers for the current VDOM. *disable* — Disable configuring DNS servers for the current VDOM.			
primary	Primary DNS server IP address for the VDOM.	ipv4-address	Not Specified	0.0.0.0
secondary	Secondary DNS server IP address for the VDOM.	ipv4-address	Not Specified	0.0.0.0
protocol	DNS transport protocols.	option	-	cleartext
	Option / **Description** *cleartext* — DNS over UDP/53, DNS over TCP/53. *dot* — DNS over TLS/853. *doh* — DNS over HTTPS/443.			
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory
server-hostname <hostname>	DNS server host name list. DNS server host name list separated by space (maximum 4 domains).	string	Maximum length: 127	
ip6-primary	Primary IPv6 DNS server IP address for the VDOM.	ipv6-address	Not Specified	::
ip6-secondary	Secondary IPv6 DNS server IP address for the VDOM.	ipv6-address	Not Specified	::
source-ip	Source IP for communications with the DNS server.	ipv4-address	Not Specified	0.0.0.0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			

Parameter	Description	Type	Size	Default
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
server-select-method	Specify how configured servers are prioritized.	option	-	least-rtt

Option	Description
least-rtt	Select servers based on least round trip time.
failover	Select servers based on the order they are configured.

alt-primary	Alternate primary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0
alt-secondary	Alternate secondary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0

config system vdom-exception

Global configuration objects that can be configured independently across different ha peers for all VDOMs or for the defined VDOM scope.

```
config system vdom-exception
    Description: Global configuration objects that can be configured independently across
different ha peers for all VDOMs or for the defined VDOM scope.
    edit <id>
        set object [log.fortianalyzer.setting|log.fortianalyzer.override-setting|...]
        set scope [all|inclusive|...]
        set vdom <name1>, <name2>, ...
    next
end
```

config system vdom-exception

Parameter	Description	Type	Size	Default
object	Name of the configuration object that can be configured independently for all VDOMs.	option	-	

Option	Description
log.fortianalyzer.setting	log.fortianalyzer.setting
log.fortianalyzer.override-setting	log.fortianalyzer.override-setting

Parameter	Description	Type	Size	Default

Option	Description
log.fortianalyzer2.setting	log.fortianalyzer2.setting
log.fortianalyzer2.override-setting	log.fortianalyzer2.override-setting
log.fortianalyzer3.setting	log.fortianalyzer3.setting
log.fortianalyzer3.override-setting	log.fortianalyzer3.override-setting
log.fortianalyzer-cloud.setting	log.fortianalyzer-cloud.setting
log.fortianalyzer-cloud.override-setting	log.fortianalyzer-cloud.override-setting
log.syslogd.setting	log.syslogd.setting
log.syslogd.override-setting	log.syslogd.override-setting
log.syslogd2.setting	log.syslogd2.setting
log.syslogd2.override-setting	log.syslogd2.override-setting
log.syslogd3.setting	log.syslogd3.setting
log.syslogd3.override-setting	log.syslogd3.override-setting
log.syslogd4.setting	log.syslogd4.setting
log.syslogd4.override-setting	log.syslogd4.override-setting
system.gre-tunnel	system.gre-tunnel
system.central-management	system.central-management
system.csf	system.csf
user.radius	user.radius
system.interface	system.interface
vpn.ipsec.phase1-interface	vpn.ipsec.phase1-interface
vpn.ipsec.phase2-interface	vpn.ipsec.phase2-interface
router.bgp	router.bgp
router.route-map	router.route-map
router.prefix-list	router.prefix-list
firewall.ippool	firewall.ippool
firewall.ippool6	firewall.ippool6

Parameter	Description	Type	Size	Default
	Option / **Description** *router.static* / router.static *router.static6* / router.static6 *firewall.vip* / firewall.vip *firewall.vip6* / firewall.vip6 *system.sdwan* / system.sdwan *system.saml* / system.saml *router.policy* / router.policy *router.policy6* / router.policy6			
scope	Determine whether the configuration object can be configured separately for all VDOMs or if some VDOMs share the same configuration.	option	-	all
	Option / **Description** *all* / Object configuration independent for all VDOMs. *inclusive* / Object configuration independent for the listed VDOMs. Other VDOMs use the global configuration. *exclusive* / Use the global object configuration for the listed VDOMs. Other VDOMs can be configured independently.			
vdom <name>	Names of the VDOMs. VDOM name.	string	Maximum length: 79	

config system vdom-link

Configure VDOM links.

```
config system vdom-link
    Description: Configure VDOM links.
    edit <name>
    next
end
```

config system vdom-property

Configure VDOM property.

```
config system vdom-property
    Description: Configure VDOM property.
    edit <name>
        set description {string}
        set snmp-index {integer}
        set session {user}
        set ipsec-phase1-interface {user}
        set ipsec-phase2-interface {user}
        set firewall-policy {user}
        set firewall-address {user}
        set firewall-addrgrp {user}
        set custom-service {user}
        set service-group {user}
        set onetime-schedule {user}
        set recurring-schedule {user}
        set user {user}
        set user-group {user}
        set sslvpn {user}
        set proxy {user}
        set log-disk-quota {user}
    next
end
```

config system vdom-property

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	
snmp-index	Permanent SNMP Index of the virtual domain .	integer	Minimum value: 1 Maximum value: 2147483647	0
session	Maximum guaranteed number of sessions.	user	Not Specified	
ipsec-phase1-interface	Maximum guaranteed number of VPN IPsec phase1 interface tunnels.	user	Not Specified	
ipsec-phase2-interface	Maximum guaranteed number of VPN IPsec phase2 interface tunnels.	user	Not Specified	
firewall-policy	Maximum guaranteed number of firewall policies (policy, DoS-policy4, DoS-policy6, multicast).	user	Not Specified	
firewall-address	Maximum guaranteed number of firewall addresses (IPv4, IPv6, multicast).	user	Not Specified	
firewall-addrgrp	Maximum guaranteed number of firewall address groups (IPv4, IPv6).	user	Not Specified	

Parameter	Description	Type	Size	Default
custom-service	Maximum guaranteed number of firewall custom services.	user	Not Specified	
service-group	Maximum guaranteed number of firewall service groups.	user	Not Specified	
onetime-schedule	Maximum guaranteed number of firewall one-time schedules.	user	Not Specified	
recurring-schedule	Maximum guaranteed number of firewall recurring schedules.	user	Not Specified	
user	Maximum guaranteed number of local users.	user	Not Specified	
user-group	Maximum guaranteed number of user groups.	user	Not Specified	
sslvpn	Maximum guaranteed number of SSL-VPNs.	user	Not Specified	
proxy	Maximum guaranteed number of concurrent proxy users.	user	Not Specified	
log-disk-quota	Log disk quota in megabytes (MB). Range depends on how much disk space is available.	user	Not Specified	

config system vdom-radius-server

Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server for this VDOM.

```
config system vdom-radius-server
    Description: Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server
for this VDOM.
    edit <name>
        set status [enable|disable]
        set radius-server-vdom {string}
    next
end
```

config system vdom-radius-server

Parameter	Description	Type	Size	Default
status	Enable/disable the RSSO RADIUS server for this VDOM.	option	-	disable

Option	Description
enable	Enable the RSSO RADIUS server for this VDOM.
disable	Disable the RSSO RADIUS server for this VDOM.

Parameter	Description	Type	Size	Default
radius-server-vdom	Use this option to select another VDOM containing a VDOM RSSO RADIUS server to use for the current VDOM.	string	Maximum length: 31	

config system vdom

Configure virtual domain.

```
config system vdom
    Description: Configure virtual domain.
    edit <name>
        set short-name {string}
        set vcluster-id {integer}
        set flag {integer}
    next
end
```

config system vdom

Parameter	Description	Type	Size	Default
short-name	VDOM short name.	string	Maximum length: 11	
vcluster-id	Virtual cluster ID .	integer	Minimum value: 0 Maximum value: 4294967295	0
flag	Flag.	integer	Minimum value: 0 Maximum value: 4294967295	0

config system vne-tunnel

Configure virtual network enabler tunnel.

```
config system vne-tunnel
    Description: Configure virtual network enabler tunnel.
    set status [enable|disable]
    set interface {string}
    set ssl-certificate {string}
```

```
    set bmr-hostname {password}
    set ipv4-address {ipv4-classnet-host}
    set br {ipv6-address}
    set update-url {string}
    set mode [map-e|fixed-ip]
end
```

config system vne-tunnel

Parameter	Description	Type	Size	Default
status	Enable/disable VNE tunnel.	option	-	disable
	Option / **Description** *enable* — Enable VNE tunnel. *disable* — Disable VNE tunnel.			
interface	Interface name.	string	Maximum length: 15	
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory
bmr-hostname	BMR hostname.	password	Not Specified	
ipv4-address	Tunnel IPv4 address and netmask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
br	Border relay IPv6 address.	ipv6-address	Not Specified	::
update-url	URL of provisioning server.	string	Maximum length: 511	
mode	VNE tunnel mode.	option	-	map-e
	Option / **Description** *map-e* — Map-e mode. *fixed-ip* — Fixed-ip mode.			

config system vxlan

Configure VXLAN devices.

```
config system vxlan
    Description: Configure VXLAN devices.
```

```
    edit <name>
        set interface {string}
        set vni {integer}
        set ip-version [ipv4-unicast|ipv6-unicast]
        set remote-ip <ip1>, <ip2>, ...
        set remote-ip6 <ip61>, <ip62>, ...
        set dstport {integer}
        set multicast-ttl {integer}
    next
end
```

config system vxlan

Parameter	Description	Type	Size	Default
interface	Outgoing interface for VXLAN encapsulated traffic.	string	Maximum length: 15	
vni	VXLAN network ID.	integer	Minimum value: 1 Maximum value: 16777215	0
ip-version	IP version to use for the VXLAN interface and so for communication over the VXLAN. IPv4 or IPv6 unicast.	option	-	ipv4-unicast
	Option / **Description** *ipv4-unicast* — Use IPv4 unicast addressing over the VXLAN. *ipv6-unicast* — Use IPv6 unicast addressing over the VXLAN.			
remote-ip <ip>	IPv4 address of the VXLAN interface on the device at the remote end of the VXLAN. IPv4 address.	string	Maximum length: 15	
remote-ip6 <ip6>	IPv6 IP address of the VXLAN interface on the device at the remote end of the VXLAN. IPv6 address.	string	Maximum length: 45	
dstport	VXLAN destination port .	integer	Minimum value: 1 Maximum value: 65535	4789
multicast-ttl	VXLAN multicast TTL .	integer	Minimum value: 1 Maximum value: 255	0

config system wccp

Configure WCCP.

```
config system wccp
    Description: Configure WCCP.
    edit <service-id>
        set router-id {ipv4-address}
        set cache-id {ipv4-address}
        set group-address {ipv4-address-multicast}
        set server-list {user}
        set router-list {user}
        set ports-defined [source|destination]
        set server-type [forward|proxy]
        set ports {user}
        set authentication [enable|disable]
        set password {password}
        set forward-method [GRE|L2|...]
        set cache-engine-method [GRE|L2]
        set service-type [auto|standard|...]
        set primary-hash {option1}, {option2}, ...
        set priority {integer}
        set protocol {integer}
        set assignment-weight {integer}
        set assignment-bucket-format [wccp-v2|cisco-implementation]
        set return-method [GRE|L2|...]
        set assignment-method [HASH|MASK|...]
        set assignment-srcaddr-mask {ipv4-netmask-any}
        set assignment-dstaddr-mask {ipv4-netmask-any}
    next
end
```

config system wccp

Parameter	Description	Type	Size	Default
router-id	IP address known to all cache engines. If all cache engines connect to the same FortiProxy interface, use the default 0.0.0.0.	ipv4-address	Not Specified	0.0.0.0
cache-id	IP address known to all routers. If the addresses are the same, use the default 0.0.0.0.	ipv4-address	Not Specified	0.0.0.0
group-address	IP multicast address used by the cache routers. For the FortiProxy to ignore multicast WCCP traffic, use the default 0.0.0.0.	ipv4-address-multicast	Not Specified	0.0.0.0
server-list	IP addresses and netmasks for up to four cache servers.	user	Not Specified	

Parameter	Description	Type	Size	Default
router-list	IP addresses of one or more WCCP routers.	user	Not Specified	
ports-defined	Match method.	option	-	
	Option / **Description** *source* — Source port match. *destination* — Destination port match.			
server-type	Cache server type.	option	-	forward
	Option / **Description** *forward* — Forward server. *proxy* — Proxy server.			
ports	Service ports.	user	Not Specified	
authentication	Enable/disable MD5 authentication.	option	-	disable
	Option / **Description** *enable* — Enable MD5 authentication. *disable* — Disable MD5 authentication.			
password	Password for MD5 authentication.	password	Not Specified	
forward-method	Method used to forward traffic to the cache servers.	option	-	GRE
	Option / **Description** *GRE* — GRE encapsulation. *L2* — L2 rewrite. *any* — GRE or L2.			
cache-engine-method	Method used to forward traffic to the routers or to return to the cache engine.	option	-	GRE
	Option / **Description** *GRE* — GRE encapsulation. *L2* — L2 rewrite.			
service-type	WCCP service type used by the cache server for logical interception and redirection of traffic.	option	-	auto

Parameter	Description	Type	Size	Default
	Option / **Description** *auto* — auto *standard* — Standard service. *dynamic* — Dynamic service.			
primary-hash	Hash method.	option	-	dst-ip
	Option / **Description** *src-ip* — Source IP hash. *dst-ip* — Destination IP hash. *src-port* — Source port hash. *dst-port* — Destination port hash.			
priority	Service priority.	integer	Minimum value: 0 Maximum value: 255	0
protocol	Service protocol.	integer	Minimum value: 0 Maximum value: 255	0
assignment-weight	Assignment of hash weight/ratio for the WCCP cache engine.	integer	Minimum value: 0 Maximum value: 255	0
assignment-bucket-format	Assignment bucket format for the WCCP cache engine.	option	-	cisco-implementation
	Option / **Description** *wccp-v2* — WCCP-v2 bucket format. *cisco-implementation* — Cisco bucket format.			
return-method	Method used to decline a redirected packet and return it to the FortiProxy unit.	option	-	GRE
	Option / **Description** *GRE* — GRE encapsulation. *L2* — L2 rewrite. *any* — GRE or L2.			

Parameter	Description	Type	Size	Default
assignment-method	Hash key assignment preference.	option	-	HASH
	Option / **Description** *HASH* — HASH assignment method. *MASK* — MASK assignment method. *any* — HASH or MASK.			
assignment-srcaddr-mask	Assignment source address mask.	ipv4-netmask-any	Not Specified	0.0.23.65
assignment-dstaddr-mask	Assignment destination address mask.	ipv4-netmask-any	Not Specified	0.0.0.0

config system zone

Configure zones to group two or more interfaces. When a zone is created you can configure policies for the zone instead of individual interfaces in the zone.

```
config system zone
    Description: Configure zones to group two or more interfaces. When a zone is created you
can configure policies for the zone instead of individual interfaces in the zone.
    edit <name>
        config tagging
            Description: Config object tagging.
            edit <name>
                set category {string}
                set tags <name1>, <name2>, ...
            next
        end
        set description {string}
        set interface <interface-name1>, <interface-name2>, ...
    next
end
```

config system zone

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default
interface <interface-name>	Add interfaces to this zone. Interfaces must not be assigned to another zone or have firewall policies defined. Select interfaces to add to the zone.	string	Maximum length: 79	

config tagging

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

test

This section includes syntax for the following commands:

config test acd

Aggregate Controller.

```
config test acd
    Description: Aggregate Controller.
    set <Integer> {string}
end
```

config test acd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test acsd

Ali Cloud Service daemon.

```
config test acsd
    Description: Ali Cloud Service daemon.
    set <Integer> {string}
end
```

config test acsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test autod

Automation daemon.

```
config test autod
    Description: Automation daemon.
    set <Integer> {string}
end
```

config test autod

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test awsd

Amazon Web Services (AWS) daemon.

```
config test awsd
    Description: Amazon Web Services (AWS) daemon.
    set <Integer> {string}
end
```

config test awsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test azd

Microsoft Azure daemon.

```
config test azd
    Description: Microsoft Azure daemon.
    set <Integer> {string}
end
```

config test azd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test bfd

BFD daemon.

```
config test bfd
    Description: BFD daemon.
    set <Integer> {string}
end
```

config test bfd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test csfd

Security Fabric daemon.

```
config test csfd
    Description: Security Fabric daemon.
    set <Integer> {string}
end
```

config test csfd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test ddnscd

DDNS client daemon.

```
config test ddnscd
    Description: DDNS client daemon.
    set <Integer> {string}
end
```

config test ddnscd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test dhcp6c

DHCP6 client daemon.

```
config test dhcp6c
    Description: DHCP6 client daemon.
    set <Integer> {string}
end
```

config test dhcp6c

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test dhcp6r

DHCP6 relay daemon.

```
config test dhcp6r
    Description: DHCP6 relay daemon.
    set <Integer> {string}
end
```

config test dhcp6r

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test dhcprelay

DHCP relay daemon.

```
config test dhcprelay
    Description: DHCP relay daemon.
    set <Integer> {string}
end
```

config test dhcprelay

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test dlpfingerprint

DLP fingerprint daemon.

```
config test dlpfingerprint
    Description: DLP fingerprint daemon.
    set <Integer> {string}
end
```

config test dlpfingerprint

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test dlpfpcache

DLP fingerprint cache daemon.

```
config test dlpfpcache
    Description: DLP fingerprint cache daemon.
    set <Integer> {string}
end
```

config test dlpfpcache

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test dnsproxy

DNS proxy.

```
config test dnsproxy
    Description: DNS proxy.
    set <Integer> {string}
end
```

config test dnsproxy

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test dsd

DLP Statistics daemon.

```
config test dsd
    Description: DLP Statistics daemon.
    set <Integer> {string}
end
```

config test dsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test fas

FortiToken Cloud daemon.

```
config test fas
    Description: FortiToken Cloud daemon.
    set <Integer> {string}
end
```

config test fas

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test fcnacd

FortiClient NAC daemon.

```
config test fcnacd
    Description: FortiClient NAC daemon.
    set <Integer> {string}
end
```

config test fcnacd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test fds_notify

Update Notification daemon.

```
config test fds_notify
    Description: Update Notification daemon.
    set <Integer> {string}
end
```

config test fds_notify

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test fnbamd

Fortiproxy non-blocking auth daemon.

```
config test fnbamd
    Description: Fortiproxy non-blocking auth daemon.
    set <Integer> {string}
end
```

config test fnbamd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test forticldd

FortiCloud daemon.

```
config test forticldd
    Description: FortiCloud daemon.
    set <Integer> {string}
end
```

config test forticldd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test forticron

Forticron daemon.

```
config test forticron
    Description: Forticron daemon.
    set <Integer> {string}
end
```

config test forticron

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test fsd

FortiExplorer daemon.

```
config test fsd
    Description: FortiExplorer daemon.
    set <Integer> {string}
end
```

config test fsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test fsvrd

FortiService daemon.

```
config test fsvrd
    Description: FortiService daemon.
    set <Integer> {string}
end
```

config test fsvrd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test gcpd

Google Cloud Platform (GCP) daemon.

```
config test gcpd
    Description: Google Cloud Platform (GCP) daemon.
    set <Integer> {string}
end
```

config test gcpd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test harelay

HA relay daemon.

```
config test harelay
    Description: HA relay daemon.
    set <Integer> {string}
end
```

config test harelay

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test hasync

HA sync daemon.

```
config test hasync
    Description: HA sync daemon.
    set <Integer> {string}
end
```

config test hasync

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test hatalk

HA talk daemon.

```
config test hatalk
    Description: HA talk daemon.
    set <Integer> {string}
end
```

config test hatalk

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test ibmd

IBM Cloud Infrastructure daemon.

```
config test ibmd
    Description: IBM Cloud Infrastructure daemon.
    set <Integer> {string}
end
```

config test ibmd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test imap

IMAP proxy.

```
config test imap
    Description: IMAP proxy.
    set <Integer> {string}
end
```

config test imap

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test init

init process.

```
config test init
    Description: init process.
    set <Integer> {string}
end
```

config test init

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test iotd

IoT device info daemon.

```
config test iotd
    Description: IoT device info daemon.
    set <Integer> {string}
end
```

config test iotd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test ipamd

IP Address Management daemon.

```
config test ipamd
    Description: IP Address Management daemon.
    set <Integer> {string}
end
```

config test ipamd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test ipamsd

IPAM server daemon.

```
config test ipamsd
    Description: IPAM server daemon.
    set <Integer> {string}
end
```

config test ipamsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test ipldbd

IP load balancing daemon.

```
config test ipldbd
    Description: IP load balancing daemon.
    set <Integer> {string}
end
```

config test ipldbd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test ipsengine

IPS sensor.

```
config test ipsengine
    Description: IPS sensor.
    set <Integer> {string}
end
```

config test ipsengine

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test ipsmonitor

IPS monitor.

```
config test ipsmonitor
    Description: IPS monitor.
    set <Integer> {string}
end
```

config test ipsmonitor

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test ipsufd

IPS urlfilter daemon.

```
config test ipsufd
    Description: IPS urlfilter daemon.
    set <Integer> {string}
end
```

config test ipsufd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test kubed

Kubernetes daemon.

```
config test kubed
    Description: Kubernetes daemon.
    set <Integer> {string}
end
```

config test kubed

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test l2tpcd

L2TP client daemon.

```
config test l2tpcd
    Description: L2TP client daemon.
    set <Integer> {string}
end
```

config test l2tpcd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test lnkmtd

Link monitor daemon.

```
config test lnkmtd
    Description: Link monitor daemon.
    set <Integer> {string}
end
```

config test lnkmtd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test miglogd

Miglog logging daemon.

```
config test miglogd
    Description: Miglog logging daemon.
    set <Integer> {string}
end
```

config test miglogd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test mrd

Mobile router daemon.

```
config test mrd
    Description: Mobile router daemon.
    set <Integer> {string}
end
```

config test mrd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test netxd

VMWare NetX service manager daemon.

```
config test netxd
    Description: VMWare NetX service manager daemon.
    set <Integer> {string}
end
```

config test netxd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test nntp

NNTP proxy.

```
config test nntp
    Description: NNTP proxy.
    set <Integer> {string}
end
```

config test nntp

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test ocid

Oracle Cloud Infrastructure.

```
config test ocid
    Description: Oracle Cloud Infrastructure.
    set <Integer> {string}
end
```

config test ocid

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test openstackd

OpenStack SDN connector daemon.

```
config test openstackd
    Description: OpenStack SDN connector daemon.
    set <Integer> {string}
end
```

config test openstackd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test ovrd

Override daemon.

```
config test ovrd
    Description: Override daemon.
    set <Integer> {string}
end
```

config test ovrd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test pop3

POP3 proxy.

```
config test pop3
    Description: POP3 proxy.
    set <Integer> {string}
end
```

config test pop3

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test pptpcd

PPTP client.

```
config test pptpcd
    Description: PPTP client.
    set <Integer> {string}
end
```

config test pptpcd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test quarantined

Quarantine daemon.

```
config test quarantined
    Description: Quarantine daemon.
    set <Integer> {string}
end
```

config test quarantined

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test radius-das

Radius-das daemon.

```
config test radius-das
    Description: Radius-das daemon.
    set <Integer> {string}
end
```

config test radius-das

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test radiusd

RADIUS daemon.

```
config test radiusd
    Description: RADIUS daemon.
    set <Integer> {string}
end
```

config test radiusd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test radvd

radvd daemon.

```
config test radvd
    Description: radvd daemon.
    set <Integer> {string}
end
```

config test radvd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test reportd

Report daemon.

```
config test reportd
    Description: Report daemon.
    set <Integer> {string}
end
```

config test reportd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test rt_router

Router daemon

```
config test rt_router
    Description: Router daemon
    set <Integer> {string}
end
```

config test rt_router

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test sdncd

SDN Connector daemon.

```
config test sdncd
    Description: SDN Connector daemon.
    set <Integer> {string}
end
```

config test sdncd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test sdnd

SDN connector daemon.

```
config test sdnd
    Description: SDN connector daemon.
    set <Integer> {string}
end
```

config test sdnd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test sepmd

Symantec Endpoint Protection Manager daemon.

```
config test sepmd
    Description: Symantec Endpoint Protection Manager daemon.
    set <Integer> {string}
end
```

config test sepmd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test sessionsync

Session sync daemon.

```
config test sessionsync
    Description: Session sync daemon.
    set <Integer> {string}
end
```

config test sessionsync

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test sfupgraded

Security Fabric Upgrade daemon.

```
config test sfupgraded
    Description: Security Fabric Upgrade daemon.
    set <Integer> {string}
end
```

config test sfupgraded

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test smtp

SMTP proxy.

```
config test smtp
    Description: SMTP proxy.
    set <Integer> {string}
end
```

config test smtp

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test snmpd

SNMP daemon.

```
config test snmpd
    Description: SNMP daemon.
    set <Integer> {string}
end
```

config test snmpd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test syslogd

Syslog daemon.

```
config test syslogd
    Description: Syslog daemon.
    set <Integer> {string}
end
```

config test syslogd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test updated

Update daemon.

```
config test updated
    Description: Update daemon.
    set <Integer> {string}
end
```

config test updated

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test uploadd

Upload daemon.

```
config test uploadd
    Description: Upload daemon.
    set <Integer> {string}
end
```

config test uploadd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test urlfilter

URL filter daemon.

```
config test urlfilter
    Description: URL filter daemon.
    set <Integer> {string}
end
```

config test urlfilter

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test vned

Virtual network enabler daemon.

```
config test vned
    Description: Virtual network enabler daemon.
    set <Integer> {string}
end
```

config test vned

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test wad

WAD related processes.

```
config test wad
    Description: WAD related processes.
    set <Integer> {string}
end
```

config test wad

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test wccpd

WCCP daemon.

```
config test wccpd
    Description: WCCP daemon.
    set <Integer> {string}
end
```

config test wccpd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test wf_monitor

WF monitor.

```
config test wf_monitor
    Description: WF monitor.
    set <Integer> {string}
end
```

config test wf_monitor

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test wiredapd

Wiredapd daemon.

```
config test wiredapd
    Description: Wiredapd daemon.
    set <Integer> {string}
end
```

config test wiredapd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

user

This section includes syntax for the following commands:

config user adgrp

Configure FSSO groups.

```
config user adgrp
    Description: Configure FSSO groups.
    edit <name>
        set server-name {string}
        set connector-source {string}
        set id {integer}
    next
end
```

config user adgrp

Parameter	Description	Type	Size	Default
server-name	FSSO agent name.	string	Maximum length: 35	
connector-source	FSSO connector source.	string	Maximum length: 35	
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config user certificate

Configure certificate users.

```
config user certificate
    Description: Configure certificate users.
    edit <name>
        set id {integer}
        set status [enable|disable]
        set type [single-certificate|trusted-issuer]
        set common-name {string}
        set issuer {string}
    next
end
```

config user certificate

Parameter	Description	Type	Size	Default
id	User ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable allowing the certificate user to authenticate with the FortiGate unit.	option	-	enable

Option	Description
enable	Enable user.
disable	Disable user.

Parameter	Description	Type	Size	Default
type	Type of certificate authentication method.	option	-	single-certificate
	Option / **Description** *single-certificate* — Single certificate. *trusted-issuer* — Trusted CA issuer.			
common-name	Certificate common name.	string	Maximum length: 64	
issuer	CA certificate used for client certificate verification.	string	Maximum length: 79	

config user domain-controller

Configure domain controller entries.

```
config user domain-controller
    Description: Configure domain controller entries.
    edit <name>
        set ad-mode [none|ds|...]
        set hostname {string}
        set username {string}
        set password {password}
        set ip-address {ipv4-address}
        set ip6 {ipv6-address}
        set port {integer}
        set source-ip-address {ipv4-address}
        set source-ip6 {ipv6-address}
        set source-port {integer}
        set interface-select-method [auto|sdwan|...]
        set interface {string}
        config extra-server
            Description: Extra servers.
            edit <id>
                set ip-address {ipv4-address}
                set port {integer}
                set source-ip-address {ipv4-address}
                set source-port {integer}
            next
        end
        set domain-name {string}
        set domain-name-src [server|client]
        set replication-port {integer}
        set ldap-server <name1>, <name2>, ...
        set dns-srv-lookup [enable|disable]
        set adlds-dn {string}
        set adlds-ip-address {ipv4-address}
        set adlds-ip6 {ipv6-address}
```

```
        set adlds-port {integer}
    next
end
```

config user domain-controller

Parameter	Description	Type	Size	Default
ad-mode	Set Active Directory mode.	option	-	none
	Option / **Description** *none* — The server is not configured as an Active Directory Domain Server (AD DS). *ds* — The server is configured as an Active Directory Domain Server (AD DS). *lds* — The server is an Active Directory Lightweight Domain Server (AD LDS).			
hostname	Hostname of the server to connect to.	string	Maximum length: 255	
username	User name to sign in with. Must have proper permissions for service.	string	Maximum length: 64	
password	Password for specified username.	password	Not Specified	
ip-address	Domain controller IPv4 address.	ipv4-address	Not Specified	0.0.0.0
ip6	Domain controller IPv6 address.	ipv6-address	Not Specified	::
port	Port to be used for communication with the domain controller .	integer	Minimum value: 0 Maximum value: 65535	445
source-ip-address	FortiProxy IPv4 address to be used for communication with the domain controller.	ipv4-address	Not Specified	0.0.0.0
source-ip6	FortiProxy IPv6 address to be used for communication with the domain controller.	ipv6-address	Not Specified	::
source-port	Source port to be used for communication with the domain controller.	integer	Minimum value: 0 Maximum value: 65535	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Parameter	Description	Type	Size	Default
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
domain-name	Domain DNS name.	string	Maximum length: 255	
domain-name-src	Select where to extract domain name .	option	-	client
	Option / **Description** *server* — Extract domain name from server's (Domain Controller) data. *client* — Extract domain name from client's data.			
replication-port	Port to be used for communication with the domain controller for replication service. Port number 0 indicates automatic discovery.	integer	Minimum value: 0 Maximum value: 65535	0
ldap-server `<name>`	LDAP server name(s). LDAP server name.	string	Maximum length: 79	
dns-srv-lookup	Enable/disable DNS service lookup.	option	-	disable
	Option / **Description** *enable* — Enable DNS service lookup. *disable* — Disable DNS service lookup.			
adlds-dn	AD LDS distinguished name.	string	Maximum length: 255	
adlds-ip-address	AD LDS IPv4 address.	ipv4-address	Not Specified	0.0.0.0
adlds-ip6	AD LDS IPv6 address.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default
adlds-port	Port number of AD LDS service .	integer	Minimum value: 0 Maximum value: 65535	389

config extra-server

Parameter	Description	Type	Size	Default
ip-address	Domain controller IP address.	ipv4-address	Not Specified	0.0.0.0
port	Port to be used for communication with the domain controller .	integer	Minimum value: 0 Maximum value: 65535	445
source-ip-address	FortiProxy IPv4 address to be used for communication with the domain controller.	ipv4-address	Not Specified	0.0.0.0
source-port	Source port to be used for communication with the domain controller.	integer	Minimum value: 0 Maximum value: 65535	0

config user exchange

Configure MS Exchange server entries.

```
config user exchange
    Description: Configure MS Exchange server entries.
    edit <name>
        set server-name {string}
        set domain-name {string}
        set username {string}
        set password {password}
        set ip {ipv4-address-any}
        set connect-protocol [rpc-over-tcp|rpc-over-http|...]
        set auth-type [spnego|ntlm|...]
        set auth-level [connect|call|...]
        set http-auth-type [basic|ntlm]
        set ssl-min-proto-version [default|SSLv3|...]
        set auto-discover-kdc [enable|disable]
        set kdc-ip <ipv41>, <ipv42>, ...
```

```
    next
end
```

config user exchange

Parameter	Description	Type	Size	Default
server-name	MS Exchange server hostname.	string	Maximum length: 63	
domain-name	MS Exchange server fully qualified domain name.	string	Maximum length: 79	
username	User name used to sign in to the server. Must have proper permissions for service.	string	Maximum length: 64	
password	Password for the specified username.	password	Not Specified	
ip	Server IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0
connect-protocol	Connection protocol used to connect to MS Exchange service.	option	-	rpc-over-https

Option	Description
rpc-over-tcp	Connect using RPC-over-TCP. Use for MS Exchange 2010 and earlier versions. Supported in MS Exchange 2013.
rpc-over-http	Connect using RPC-over-HTTP. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.
rpc-over-https	Connect using RPC-over-HTTPS. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.

auth-type	Authentication security type used for the RPC protocol layer.	option	-	kerberos

Option	Description
spnego	Negotiate authentication.
ntlm	NTLM authentication.
kerberos	Kerberos authentication.

auth-level	Authentication security level used for the RPC protocol layer.	option	-	privacy

Parameter	Description	Type	Size	Default
	Option / **Description** *connect* / RPC authentication level 'connect'. *call* / RPC authentication level 'call'. *packet* / RPC authentication level 'packet'. *integrity* / RPC authentication level 'integrity'. *privacy* / RPC authentication level 'privacy'.			
http-auth-type	Authentication security type used for the HTTP transport.	option	-	ntlm
	Option / **Description** *basic* / Basic HTTP authentication. *ntlm* / NTLM HTTP authentication.			
ssl-min-proto-version	Minimum SSL/TLS protocol version for HTTPS transport .	option	-	default
	Option / **Description** *default* / Follow system global setting. *SSLv3* / SSLv3. *TLSv1* / TLSv1. *TLSv1-1* / TLSv1.1. *TLSv1-2* / TLSv1.2.			
auto-discover-kdc	Enable/disable automatic discovery of KDC IP addresses.	option	-	enable
	Option / **Description** *enable* / Enable automatic discovery of KDC IP addresses. *disable* / Disable automatic discovery of KDC IP addresses.			
kdc-ip <ipv4>	KDC IPv4 addresses for Kerberos authentication. KDC IPv4 addresses for Kerberos authentication.	string	Maximum length: 79	

config user fortitoken

Configure FortiToken.

```
config user fortitoken
    Description: Configure FortiToken.
    edit <serial-number>
        set status [active|lock]
        set comments {var-string}
        set license {string}
        set activation-code {string}
        set activation-expire {integer}
        set reg-id {string}
        set os-ver {string}
    next
end
```

config user fortitoken

Parameter	Description	Type	Size	Default
status	Status.	option	-	active
	Option / **Description** *active* / Activate FortiToken. *lock* / Lock FortiToken.			
comments	Comment.	var-string	Maximum length: 255	
license	Mobile token license.	string	Maximum length: 31	
activation-code	Mobile token user activation-code.	string	Maximum length: 32	
activation-expire	Mobile token user activation-code expire time.	integer	Minimum value: 0 Maximum value: 4294967295	0
reg-id	Device Reg ID.	string	Maximum length: 256	
os-ver	Device Mobile Version.	string	Maximum length: 15	

config user fsso-polling

Configure FSSO active directory servers for polling mode.

```
config user fsso-polling
    Description: Configure FSSO active directory servers for polling mode.
```

```
    edit <id>
        set status [enable|disable]
        set server {string}
        set default-domain {string}
        set port {integer}
        set user {string}
        set password {password}
        set ldap-server {string}
        set logon-history {integer}
        set polling-frequency {integer}
        config adgrp
            Description: LDAP Group Info.
            edit <name>
            next
        end
        set smbv1 [enable|disable]
        set smb-ntlmv1-auth [enable|disable]
    next
end
```

config user fsso-polling

Parameter	Description	Type	Size	Default
status	Enable/disable polling for the status of this Active Directory server.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
server	Host name or IP address of the Active Directory server.	string	Maximum length: 63	
default-domain	Default domain managed by this Active Directory server.	string	Maximum length: 35	
port	Port to communicate with this Active Directory server.	integer	Minimum value: 0 Maximum value: 65535	0
user	User name required to log into this Active Directory server.	string	Maximum length: 35	
password	Password required to log into this Active Directory server.	password	Not Specified	
ldap-server	LDAP server name used in LDAP connection strings.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
logon-history	Number of hours of logon history to keep, 0 means keep all history.	integer	Minimum value: 0 Maximum value: 48	8
polling-frequency	Polling frequency (every 1 to 30 seconds).	integer	Minimum value: 1 Maximum value: 30	10
smbv1	Enable/disable support of SMBv1 for Samba.	option	-	disable

Option	Description
enable	Enable support of SMBv1 for Samba.
disable	Disable support of SMBv1 for Samba.

Parameter	Description	Type	Size	Default
smb-ntlmv1-auth	Enable/disable support of NTLMv1 for Samba authentication.	option	-	disable

Option	Description
enable	Enable support of NTLMv1 for Samba authentication.
disable	Disable support of NTLMv1 for Samba authentication.

config user fsso

Configure Fortinet Single Sign On (FSSO) agents.

```
config user fsso
    Description: Configure Fortinet Single Sign On (FSSO) agents.
    edit <name>
        set type [default|fortinac]
        set server {string}
        set port {integer}
        set password {password}
        set server2 {string}
        set port2 {integer}
        set password2 {password}
        set server3 {string}
        set port3 {integer}
        set password3 {password}
        set server4 {string}
        set port4 {integer}
        set password4 {password}
        set server5 {string}
        set port5 {integer}
        set password5 {password}
        set logon-timeout {integer}
```

```
        set ldap-server {string}
        set group-poll-interval {integer}
        set ldap-poll [enable|disable]
        set ldap-poll-interval {integer}
        set ldap-poll-filter {string}
        set user-info-server {string}
        set ssl [enable|disable]
        set ssl-server-host-ip-check [enable|disable]
        set ssl-trusted-cert {string}
        set source-ip {ipv4-address}
        set source-ip6 {ipv6-address}
        set interface-select-method [auto|sdwan|...]
        set interface {string}
    next
end
```

config user fsso

Parameter	Description	Type	Size	Default
type	Server type.	option	-	default
	Option / **Description** *default* — All other unspecified types of servers. *fortinac* — FortiNAC server.			
server	Domain name or IP address of the first FSSO collector agent.	string	Maximum length: 63	
port	Port of the first FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password	Password of the first FSSO collector agent.	password	Not Specified	
server2	Domain name or IP address of the second FSSO collector agent.	string	Maximum length: 63	
port2	Port of the second FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password2	Password of the second FSSO collector agent.	password	Not Specified	
server3	Domain name or IP address of the third FSSO collector agent.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
port3	Port of the third FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password3	Password of the third FSSO collector agent.	password	Not Specified	
server4	Domain name or IP address of the fourth FSSO collector agent.	string	Maximum length: 63	
port4	Port of the fourth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password4	Password of the fourth FSSO collector agent.	password	Not Specified	
server5	Domain name or IP address of the fifth FSSO collector agent.	string	Maximum length: 63	
port5	Port of the fifth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password5	Password of the fifth FSSO collector agent.	password	Not Specified	
logon-timeout	Interval in minutes to keep logons after FSSO server down.	integer	Minimum value: 1 Maximum value: 2880	5
ldap-server	LDAP server to get group information.	string	Maximum length: 35	
group-poll-interval	Interval in minutes within to fetch groups from FSSO server, or unset to disable.	integer	Minimum value: 1 Maximum value: 2880	0
ldap-poll	Enable/disable automatic fetching of groups from LDAP server.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable automatic fetching of groups from LDAP server. *disable* / Disable automatic fetching of groups from LDAP server.			
ldap-poll-interval	Interval in minutes within to fetch groups from LDAP server.	integer	Minimum value: 1 Maximum value: 2880	180
ldap-poll-filter	Filter used to fetch groups.	string	Maximum length: 2047	(objectCategory=group)
user-info-server	LDAP server to get user information.	string	Maximum length: 35	
ssl	Enable/disable use of SSL.	option	-	disable
	Option / **Description** *enable* / Enable use of SSL. *disable* / Disable use of SSL.			
ssl-server-host-ip-check	Enable/disable server host/IP verification.	option	-	disable
	Option / **Description** *enable* / Enable server host/IP verification. *disable* / Disable server host/IP verification.			
ssl-trusted-cert	Trusted server certificate or CA certificate.	string	Maximum length: 79	
source-ip	Source IP for communications to FSSO agent.	ipv4-address	Not Specified	0.0.0.0
source-ip6	IPv6 source for communications to FSSO agent.	ipv6-address	Not Specified	::
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* / Set outgoing interface automatically. *sdwan* / Set outgoing interface by SD-WAN or policy routing rules. *specify* / Set outgoing interface manually.			

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

config user group

Configure user groups.

```
config user group
    Description: Configure user groups.
    edit <name>
        set id {integer}
        set group-type [firewall|fsso-service|...]
        set authtimeout {integer}
        set auth-concurrent-override [enable|disable]
        set auth-concurrent-value {integer}
        set http-digest-realm {string}
        set sso-attribute-value {string}
        set logic-type [or|and]
        set member <name1>, <name2>, ...
        config match
            Description: Group matches.
            edit <id>
                set server-name {string}
                set group-name {string}
            next
        end
        set user-id [email|auto-generate|...]
        set password [auto-generate|specify|...]
        set user-name [disable|enable]
        set sponsor [optional|mandatory|...]
        set company [optional|mandatory|...]
        set email [disable|enable]
        set mobile-phone [disable|enable]
        set sms-server [fortiguard|custom]
        set sms-custom-server {string}
        set expire-type [immediately|first-successful-login]
        set expire {integer}
        set max-accounts {integer}
        set multiple-guest-add [disable|enable]
        config guest
            Description: Guest User.
            edit <id>
                set user-id {string}
                set name {string}
                set password {password}
                set mobile-phone {string}
                set sponsor {string}
                set company {string}
                set email {string}
                set expiration {user}
                set comment {var-string}
```

```
            next
        end
    next
end
```

config user group

Parameter	Description	Type	Size	Default
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
group-type	Set the group to be for firewall authentication, FSSO, RSSO, or guest users.	option	-	firewall

Option	Description
firewall	Firewall.
fsso-service	Fortinet Single Sign-On Service.
rsso	RADIUS based Single Sign-On Service.
guest	Guest.

Parameter	Description	Type	Size	Default
authtimeout	Authentication timeout in minutes for this user group. 0 to use the global user setting auth-timeout.	integer	Minimum value: 0 Maximum value: 43200	0
auth-concurrent-override	Enable/disable overriding the global number of concurrent authentication sessions for this user group.	option	-	disable

Option	Description
enable	Enable auth-concurrent-override.
disable	Disable auth-concurrent-override.

Parameter	Description	Type	Size	Default
auth-concurrent-value	Maximum number of concurrent authenticated connections per user .	integer	Minimum value: 0 Maximum value: 100	0
http-digest-realm	Realm attribute for MD5-digest authentication.	string	Maximum length: 35	
sso-attribute-value	Name of the RADIUS user group that this local user group represents.	string	Maximum length: 511	

Parameter	Description	Type	Size	Default
logic-type	Set the logic between members or matching entries.	option	-	or
	Option / **Description** *or* — Logic OR between members or match entries. *and* — Logic AND between members or match entries.			
member <name>	Names of users, peers, LDAP severs, or RADIUS servers to add to the user group. Group member name.	string	Maximum length: 511	
user-id	Guest user ID type.	option	-	email
	Option / **Description** *email* — Email address. *auto-generate* — Automatically generate. *specify* — Specify.			
password	Guest user password type.	option	-	auto-generate
	Option / **Description** *auto-generate* — Automatically generate. *specify* — Specify. *disable* — Disable.			
user-name	Enable/disable the guest user name entry.	option	-	disable
	Option / **Description** *disable* — Enable setting. *enable* — Disable setting.			
sponsor	Set the action for the sponsor guest user field.	option	-	optional
	Option / **Description** *optional* — Optional. *mandatory* — Mandatory. *disabled* — Disabled.			
company	Set the action for the company guest user field.	option	-	optional

Parameter	Description	Type	Size	Default
	Option / **Description** *optional* — Optional. *mandatory* — Mandatory. *disabled* — Disabled.			
email	Enable/disable the guest user email address field.	option	-	enable
	Option / **Description** *disable* — Enable setting. *enable* — Disable setting.			
mobile-phone	Enable/disable the guest user mobile phone number field.	option	-	disable
	Option / **Description** *disable* — Enable setting. *enable* — Disable setting.			
sms-server	Send SMS through FortiGuard or other external server.	option	-	fortiguard
	Option / **Description** *fortiguard* — Send SMS by FortiGuard. *custom* — Send SMS by custom server.			
sms-custom-server	SMS server.	string	Maximum length: 35	
expire-type	Determine when the expiration countdown begins.	option	-	immediately
	Option / **Description** *immediately* — Immediately. *first-successful-login* — First successful login.			
expire	Time in seconds before guest user accounts expire.	integer	Minimum value: 1 Maximum value: 31536000	14400

Parameter	Description	Type	Size	Default
max-accounts	Maximum number of guest accounts that can be created for this group (0 means unlimited).	integer	Minimum value: 0 Maximum value: 1024	0
multiple-guest-add	Enable/disable addition of multiple guests.	option	-	disable

Option	Description
disable	Enable setting.
enable	Disable setting.

config match

Parameter	Description	Type	Size	Default
server-name	Name of remote auth server.	string	Maximum length: 35	
group-name	Name of matching user or group on remote authentication server.	string	Maximum length: 511	

config guest

Parameter	Description	Type	Size	Default
user-id	Guest ID.	string	Maximum length: 64	
name	Guest name.	string	Maximum length: 64	
password	Guest password.	password	Not Specified	
mobile-phone	Mobile phone.	string	Maximum length: 35	
sponsor	Set the action for the sponsor guest user field.	string	Maximum length: 35	
company	Set the action for the company guest user field.	string	Maximum length: 35	
email	Email.	string	Maximum length: 64	
expiration	Expire time.	user	Not Specified	

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

config user krb-keytab

Configure Kerberos keytab entries.

```
config user krb-keytab
    Description: Configure Kerberos keytab entries.
    edit <name>
        set pac-data [enable|disable]
        set principal {string}
        set ldap-server <name1>, <name2>, ...
        set keytab {string}
    next
end
```

config user krb-keytab

Parameter	Description	Type	Size	Default
pac-data	Enable/disable parsing PAC data in the ticket.	option	-	enable

Option	Description
enable	Enable parsing PAC data in the ticket.
disable	Disable parsing PAC data in the ticket.

principal	Kerberos service principal. For example, HTTP/myfgt.example.com@example.com.	string	Maximum length: 511	
ldap-server <name>	LDAP server name(s). LDAP server name.	string	Maximum length: 79	
keytab	Base64 coded keytab file containing a pre-shared key.	string	Maximum length: 8191	

config user ldap

Configure LDAP server entries.

```
config user ldap
    Description: Configure LDAP server entries.
    edit <name>
        set server {string}
```

```
        set secondary-server {string}
        set tertiary-server {string}
        set server-identity-check [enable|disable]
        set source-ip {string}
        set source-port {integer}
        set cnid {string}
        set dn {string}
        set type [simple|anonymous|...]
        set two-factor [disable|fortitoken-cloud]
        set two-factor-authentication [fortitoken|email|...]
        set two-factor-notification [email|sms]
        set username {string}
        set password {password}
        set group-member-check [user-attr|group-object|...]
        set group-search-base {string}
        set group-object-filter {string}
        set group-filter {string}
        set secure [disable|starttls|...]
        set ssl-min-proto-version [default|SSLv3|...]
        set ca-cert {string}
        set port {integer}
        set password-expiry-warning [enable|disable]
        set password-renewal [enable|disable]
        set member-attr {string}
        set account-key-processing [same|strip]
        set account-key-filter {string}
        set search-type {option1}, {option2}, ...
        set obtain-user-info [enable|disable]
        set user-info-exchange-server {string}
        set interface-select-method [auto|sdwan|...]
        set interface {string}
        set antiphish [enable|disable]
        set password-attr {string}
    next
end
```

config user ldap

Parameter	Description	Type	Size	Default
server	LDAP server CN domain name or IP.	string	Maximum length: 63	
secondary-server	Secondary LDAP server CN domain name or IP.	string	Maximum length: 63	
tertiary-server	Tertiary LDAP server CN domain name or IP.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
server-identity-check	Enable/disable LDAP server identity check (verify server domain name/IP address against the server certificate).	option	-	enable
	Option / **Description** *enable* — Enable server identity check. *disable* — Disable server identity check.			
source-ip	FortiProxy IP address to be used for communication with the LDAP server.	string	Maximum length: 63	
source-port	Source port to be used for communication with the LDAP server.	integer	Minimum value: 0 Maximum value: 65535	0
cnid	Common name identifier for the LDAP server. The common name identifier for most LDAP servers is "cn".	string	Maximum length: 20	cn
dn	Distinguished name used to look up entries on the LDAP server.	string	Maximum length: 511	
type	Authentication type for LDAP searches.	option	-	simple
	Option / **Description** *simple* — Simple password authentication without search.			

Parameter	Description	Type	Size	Default
	Option / **Description** *anonymous* / Bind using anonymous user search. *regular* / Bind using username/password and then search.			
two-factor	Enable/disable two-factor authentication.	option	-	disable
	Option / **Description** *disable* / disable two-factor authentication. *fortitoken-cloud* / FortiToken Cloud Service.			
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-	
	Option / **Description** *fortitoken* / FortiToken authentication. *email* / Email one time password. *sms* / SMS one time password.			
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-	
	Option / **Description** *email* / Email notification for activation code. *sms* / SMS notification for activation code.			
username	Username (full DN) for initial binding.	string	Maximum length: 511	
password	Password for initial binding.	password	Not Specified	
group-member-check	Group member checking methods.	option	-	user-attr

Parameter	Description	Type	Size	Default
	Option / **Description** *user-attr* — User attribute checking. *group-object* — Group object checking. *posix-group-object* — POSIX group object checking.			
group-search-base	Search base used for group searching.	string	Maximum length: 511	
group-object-filter	Filter used for group searching.	string	Maximum length: 2047	(&(objectcategory=group)(member=*))
group-filter	Filter used for group matching.	string	Maximum length: 2047	
secure	Port to be used for authentication.	option	-	disable
	Option / **Description** *disable* — No SSL. *starttls* — Use StartTLS. *ldaps* — Use LDAPS.			
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			
ca-cert	CA certificate name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
port	Port to be used for communication with the LDAP server .	integer	Minimum value: 1 Maximum value: 65535	389
password-expiry-warning	Enable/disable password expiry warnings.	option	-	disable

Option	Description
enable	Enable password expiry warnings.
disable	Disable password expiry warnings.

password-renewal	Enable/disable online password renewal.	option	-	disable

Option	Description
enable	Enable online password renewal.
disable	Disable online password renewal.

member-attr	Name of attribute from which to get group membership.	string	Maximum length: 63	memberOf
account-key-processing	Account key processing operation, either keep or strip domain string of UPN in the token.	option	-	same

Option	Description
same	Same as UPN.
strip	Strip domain string from UPN.

account-key-filter	Account key filter, using the UPN as the search filter.	string	Maximum length: 2047	(&(userPrincipalName=%s)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))

Parameter	Description	Type	Size	Default
search-type	Search type.	option	-	

Option	Description
recursive	Recursively retrieve the user-group chain information of a user in a particular Microsoft AD domain.

Parameter	Description	Type	Size	Default
obtain-user-info	Enable/disable obtaining of user information.	option	-	enable

Option	Description
enable	Enable obtaining of user information.
disable	Disable obtaining of user information.

Parameter	Description	Type	Size	Default
user-info-exchange-server	MS Exchange server from which to fetch user information.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	Set outgoing interface manually.

Parameter	Description	Type	Size	Default
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
antiphish	Enable/disable AntiPhishing credential backend.	option	-	disable

Option	Description
enable	Enable AntiPhishing credential backend.
disable	Disable AntiPhishing credential backend.

Parameter	Description	Type	Size	Default
password-attr	Name of attribute to get password hash.	string	Maximum length: 35	userPassword

config user local

Configure local users.

```
config user local
    Description: Configure local users.
    edit <name>
        set id {integer}
        set status [enable|disable]
        set type [password|radius|...]
        set passwd {password}
        set ldap-server {string}
        set radius-server {string}
        set tacacs+-server {string}
        set two-factor [disable|fortitoken|...]
        set two-factor-authentication [fortitoken|email|...]
        set two-factor-notification [email|sms]
        set fortitoken {string}
        set email-to {string}
        set sms-server [fortiguard|custom]
        set sms-custom-server {string}
        set sms-phone {string}
        set passwd-policy {string}
        set passwd-time {user}
        set authtimeout {integer}
        set workstation {string}
        set auth-concurrent-override [enable|disable]
        set auth-concurrent-value {integer}
        set ppk-secret {password-3}
        set ppk-identity {string}
        set username-sensitivity [disable|enable]
    next
end
```

config user local

Parameter	Description	Type	Size	Default
id	User ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable allowing the local user to authenticate with the FortiProxy unit.	option	-	enable

Option	Description
enable	Enable user.
disable	Disable user.

Parameter	Description	Type	Size	Default
type	Authentication method.	option	-	password
	Option / **Description** *password* — Password authentication. *radius* — RADIUS server authentication. *tacacs+* — TACACS+ server authentication. *ldap* — LDAP server authentication.			
passwd	User's password.	password	Not Specified	
ldap-server	Name of LDAP server with which the user must authenticate.	string	Maximum length: 35	
radius-server	Name of RADIUS server with which the user must authenticate.	string	Maximum length: 35	
tacacs+-server	Name of TACACS+ server with which the user must authenticate.	string	Maximum length: 35	
two-factor	Enable/disable two-factor authentication.	option	-	disable
	Option / **Description** *disable* — disable *fortitoken* — FortiToken *fortitoken-cloud* — FortiToken Cloud Service. *email* — Email authentication code. *sms* — SMS authentication code.			
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-	
	Option / **Description** *fortitoken* — FortiToken authentication. *email* — Email one time password. *sms* — SMS one time password.			
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-	
	Option / **Description** *email* — Email notification for activation code. *sms* — SMS notification for activation code.			

Parameter	Description	Type	Size	Default
fortitoken	Two-factor recipient's FortiToken serial number.	string	Maximum length: 16	
email-to	Two-factor recipient's email address.	string	Maximum length: 63	
sms-server	Send SMS through FortiGuard or other external server.	option	-	fortiguard
	Option / **Description** *fortiguard* — Send SMS by FortiGuard. *custom* — Send SMS by custom server.			
sms-custom-server	Two-factor recipient's SMS server.	string	Maximum length: 35	
sms-phone	Two-factor recipient's mobile phone number.	string	Maximum length: 15	
passwd-policy	Password policy to apply to this user, as defined in config user password-policy.	string	Maximum length: 35	
passwd-time	Time of the last password update.	user	Not Specified	
authtimeout	Time in minutes before the authentication timeout for a user is reached.	integer	Minimum value: 0 Maximum value: 1440	0
workstation	Name of the remote user workstation, if you want to limit the user to authenticate only from a particular workstation.	string	Maximum length: 35	
auth-concurrent-override	Enable/disable overriding the policy-auth-concurrent under config system global.	option	-	disable
	Option / **Description** *enable* — Enable auth-concurrent-override. *disable* — Disable auth-concurrent-override.			
auth-concurrent-value	Maximum number of concurrent logins permitted from the same user.	integer	Minimum value: 0 Maximum value: 100	0
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	

Parameter	Description	Type	Size	Default
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35	
username-sensitivity	Enable/disable case and accent sensitivity when performing username matching (accents are stripped and case is ignored when disabled).	option	-	enable

Option	Description
disable	Ignore case and accents. Username at prompt not required to match case or accents.
enable	Do not ignore case and accents. Username at prompt must be an exact match.

config user password-policy

Configure user password policy.

```
config user password-policy
    Description: Configure user password policy.
    edit <name>
        set expire-days {integer}
        set warn-days {integer}
        set expired-password-renewal [enable|disable]
    next
end
```

config user password-policy

Parameter	Description	Type	Size	Default
expire-days	Time in days before the user's password expires.	integer	Minimum value: 0 Maximum value: 999	180
warn-days	Time in days before a password expiration warning message is displayed to the user upon login.	integer	Minimum value: 0 Maximum value: 30	15
expired-password-renewal	Enable/disable renewal of a password that already is expired.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable renewal of a password that already is expired. *disable* / Disable renewal of a password that already is expired.			

config user peer

Configure peer users.

```
config user peer
    Description: Configure peer users.
    edit <name>
        set mandatory-ca-verify [enable|disable]
        set ca {string}
        set subject {string}
        set cn {string}
        set cn-type [string|email|...]
        set ldap-server {string}
        set ldap-username {string}
        set ldap-password {password}
        set ldap-mode [password|principal-name]
        set ocsp-override-server {string}
        set two-factor [enable|disable]
        set passwd {password}
    next
end
```

config user peer

Parameter	Description	Type	Size	Default
mandatory-ca-verify	Determine what happens to the peer if the CA certificate is not installed. Disable to automatically consider the peer certificate as valid. **Option** / **Description** *enable* / Enable setting. *disable* / Disable setting.	option	-	enable
ca	Name of the CA certificate.	string	Maximum length: 127	
subject	Peer certificate name constraints.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default
cn	Peer certificate common name.	string	Maximum length: 255	
cn-type	Peer certificate common name type.	option	-	string

Option	Description
string	Normal string.
email	Email address.
FQDN	Fully Qualified Domain Name.
ipv4	IPv4 address.
ipv6	IPv6 address.

ldap-server	Name of an LDAP server defined under the user ldap command. Performs client access rights check.	string	Maximum length: 35	
ldap-username	Username for LDAP server bind.	string	Maximum length: 35	
ldap-password	Password for LDAP server bind.	password	Not Specified	
ldap-mode	Mode for LDAP peer authentication.	option	-	password

Option	Description
password	Username/password.
principal-name	Principal name.

ocsp-override-server	Online Certificate Status Protocol (OCSP) server for certificate retrieval.	string	Maximum length: 35	
two-factor	Enable/disable two-factor authentication, applying certificate and password-based authentication.	option	-	disable

Option	Description
enable	Enable 2-factor authentication.
disable	Disable 2-factor authentication.

passwd	Peer's password used for two-factor authentication.	password	Not Specified	

config user peergrp

Configure peer groups.

```
config user peergrp
    Description: Configure peer groups.
    edit <name>
        set member <name1>, <name2>, ...
    next
end
```

config user peergrp

Parameter	Description	Type	Size	Default
member <name>	Peer group members. Peer group member name.	string	Maximum length: 35	

config user pop3

POP3 server entry configuration.

```
config user pop3
    Description: POP3 server entry configuration.
    edit <name>
        set server {string}
        set port {integer}
        set secure [none|starttls|...]
        set ssl-min-proto-version [default|SSLv3|...]
    next
end
```

config user pop3

Parameter	Description	Type	Size	Default
server	Server domain name or IP address.	string	Maximum length: 63	
port	POP3 service port number.	integer	Minimum value: 0 Maximum value: 65535	0
secure	SSL connection.	option	-	starttls

Option	Description
none	None.

Parameter	Description	Type	Size	Default
	Option / **Description** *starttls* — Use StartTLS. *pop3s* — Use POP3 over SSL.			
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			

config user radius

Configure RADIUS server entries.

```
config user radius
    Description: Configure RADIUS server entries.
    edit <name>
        set server {string}
        set secret {password}
        set secondary-server {string}
        set secondary-secret {password}
        set tertiary-server {string}
        set tertiary-secret {password}
        set timeout {integer}
        set all-usergroup [disable|enable]
        set use-management-vdom [enable|disable]
        set nas-ip {ipv4-address}
        set acct-interim-interval {integer}
        set radius-coa [enable|disable]
        set radius-port {integer}
        set h3c-compatibility [enable|disable]
        set auth-type [auto|ms_chap_v2|...]
        set source-ip {string}
        set username-case-sensitive [enable|disable]
        set group-override-attr-type [filter-Id|class]
        set class <name1>, <name2>, ...
        set password-renewal [enable|disable]
        set password-encoding [auto|ISO-8859-1]
        set acct-all-servers [enable|disable]
        set switch-controller-acct-fast-framedip-detect {integer}
        set interface-select-method [auto|sdwan|...]
```

```
        set interface {string}
        set switch-controller-service-type {option1}, {option2}, ...
        set rsso [enable|disable]
        set rsso-radius-server-port {integer}
        set rsso-radius-response [enable|disable]
        set rsso-validate-request-secret [enable|disable]
        set rsso-secret {password}
        set rsso-endpoint-attribute [User-Name|NAS-IP-Address|...]
        set rsso-endpoint-block-attribute [User-Name|NAS-IP-Address|...]
        set sso-attribute [User-Name|NAS-IP-Address|...]
        set sso-attribute-key {string}
        set sso-attribute-value-override [enable|disable]
        set rsso-context-timeout {integer}
        set rsso-log-period {integer}
        set rsso-log-flags {option1}, {option2}, ...
        set rsso-flush-ip-session [enable|disable]
        set rsso-ep-one-ip-only [enable|disable]
        config accounting-server
            Description: Additional accounting servers.
            edit <id>
                set status [enable|disable]
                set server {string}
                set secret {password}
                set port {integer}
                set source-ip {string}
                set interface-select-method [auto|sdwan|...]
                set interface {string}
            next
        end
    next
end
```

config user radius

Parameter	Description	Type	Size	Default
server	Primary RADIUS server CN domain name or IP address.	string	Maximum length: 63	
secret	Pre-shared secret key used to access the primary RADIUS server.	password	Not Specified	
secondary-server	Secondary RADIUS CN domain name or IP address.	string	Maximum length: 63	
secondary-secret	Secret key to access the secondary server.	password	Not Specified	
tertiary-server	Tertiary RADIUS CN domain name or IP address.	string	Maximum length: 63	
tertiary-secret	Secret key to access the tertiary server.	password	Not Specified	

Parameter	Description	Type	Size	Default
timeout	Time in seconds between re-sending authentication requests.	integer	Minimum value: 1 Maximum value: 300	5
all-usergroup	Enable/disable automatically including this RADIUS server in all user groups.	option	-	disable
	Option / **Description** *disable* — Do not automatically include this server in a user group. *enable* — Include this RADIUS server in every user group.			
use-management-vdom	Enable/disable using management VDOM to send requests.	option	-	disable
	Option / **Description** *enable* — Send requests using the management VDOM. *disable* — Send requests using the current VDOM.			
nas-ip	IP address used to communicate with the RADIUS server and used as NAS-IP-Address and Called-Station-ID attributes.	ipv4-address	Not Specified	0.0.0.0
acct-interim-interval	Time in seconds between each accounting interim update message.	integer	Minimum value: 60 Maximum value: 86400	0
radius-coa	Enable to allow a mechanism to change the attributes of an authentication, authorization, and accounting session after it is authenticated.	option	-	disable
	Option / **Description** *enable* — Enable RADIUS CoA. *disable* — Disable RADIUS CoA.			
radius-port	RADIUS service port number.	integer	Minimum value: 0 Maximum value: 65535	0
h3c-compatibility	Enable/disable compatibility with the H3C, a mechanism that performs security checking for authentication.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable H3C compatibility. *disable* — Disable H3C compatibility.			
auth-type	Authentication methods/protocols permitted for this RADIUS server.	option	-	auto
	Option / **Description** *auto* — Use PAP, MSCHAP_v2, and CHAP (in that order). *ms_chap_v2* — Microsoft Challenge Handshake Authentication Protocol version 2. *ms_chap* — Microsoft Challenge Handshake Authentication Protocol. *chap* — Challenge Handshake Authentication Protocol. *pap* — Password Authentication Protocol.			
source-ip	Source IP address for communications to the RADIUS server.	string	Maximum length: 63	
username-case-sensitive	Enable/disable case sensitive user names.	option	-	disable
	Option / **Description** *enable* — Enable username case-sensitive. *disable* — Disable username case-sensitive.			
group-override-attr-type	RADIUS attribute type to override user group information.	option	-	
	Option / **Description** *filter-Id* — Filter-Id *class* — Class			
class <name>	Class attribute name(s). Class name.	string	Maximum length: 79	
password-renewal	Enable/disable password renewal.	option	-	enable
	Option / **Description** *enable* — Enable password renewal. *disable* — Disable password renewal.			

Parameter	Description	Type	Size	Default
password-encoding	Password encoding.	option	-	auto

Option	Description
auto	Use original password encoding.
ISO-8859-1	Use ISO-8859-1 password encoding.

acct-all-servers	Enable/disable sending of accounting messages to all configured servers .	option	-	disable

Option	Description
enable	Send accounting messages to all configured servers.
disable	Send accounting message only to servers that are confirmed to be reachable.

switch-controller-acct-fast-framedip-detect	Switch controller accounting message Framed-IP detection from DHCP snooping .	integer	Minimum value: 2 Maximum value: 600	2
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	Set outgoing interface manually.

interface	Specify outgoing interface to reach server.	string	Maximum length: 15
switch-controller-service-type	RADIUS service type.	option	-

Option	Description
login	User should be connected to a host.
framed	User use Framed Protocol.
callback-login	User disconnected and called back.
callback-framed	User disconnected and called back, then a Framed Protocol.
outbound	User granted access to outgoing devices.

Parameter	Description	Type	Size	Default
	Option / **Description** *administrative* — User granted access to the administrative unsigned interface. *nas-prompt* — User provided a command prompt on the NAS. *authenticate-only* — Authentication requested, and no auth info needs to be returned. *callback-nas-prompt* — User disconnected and called back, then provided a command prompt. *call-check* — Used by the NAS in an Access-Request packet, Access-Accept to answer the call. *callback-administrative* — User disconnected and called back, granted access to the admin unsigned interface.			
rsso	Enable/disable RADIUS based single sign on feature.	option	-	disable
	Option / **Description** *enable* — Enable RADIUS based single sign on feature. *disable* — Disable RADIUS based single sign on feature.			
rsso-radius-server-port	UDP port to listen on for RADIUS Start and Stop records.	integer	Minimum value: 0 Maximum value: 65535	1813
rsso-radius-response	Enable/disable sending RADIUS response packets after receiving Start and Stop records.	option	-	disable
	Option / **Description** *enable* — Enable sending RADIUS response packets. *disable* — Disable sending RADIUS response packets.			
rsso-validate-request-secret	Enable/disable validating the RADIUS request shared secret in the Start or End record.	option	-	disable
	Option / **Description** *enable* — Enable validating RADIUS request shared secret. *disable* — Disable validating RADIUS request shared secret.			
rsso-secret	RADIUS secret used by the RADIUS accounting server.	password	Not Specified	

Parameter	Description	Type	Size	Default
rsso-endpoint-attribute	RADIUS attributes used to extract the user end point identifier from the RADIUS Start record.	option	-	Calling-Station-Id

Option	Description
User-Name	Use this attribute.
NAS-IP-Address	Use this attribute.
Framed-IP-Address	Use this attribute.
Framed-IP-Netmask	Use this attribute.
Filter-Id	Use this attribute.
Login-IP-Host	Use this attribute.
Reply-Message	Use this attribute.
Callback-Number	Use this attribute.
Callback-Id	Use this attribute.
Framed-Route	Use this attribute.
Framed-IPX-Network	Use this attribute.
Class	Use this attribute.
Called-Station-Id	Use this attribute.
Calling-Station-Id	Use this attribute.
NAS-Identifier	Use this attribute.
Proxy-State	Use this attribute.
Login-LAT-Service	Use this attribute.
Login-LAT-Node	Use this attribute.
Login-LAT-Group	Use this attribute.
Framed-AppleTalk-Zone	Use this attribute.
Acct-Session-Id	Use this attribute.
Acct-Multi-Session-Id	Use this attribute.

Parameter	Description	Type	Size	Default
rsso-endpoint-block-attribute	RADIUS attributes used to block a user.	option	-	

Option	Description
User-Name	Use this attribute.
NAS-IP-Address	Use this attribute.
Framed-IP-Address	Use this attribute.
Framed-IP-Netmask	Use this attribute.
Filter-Id	Use this attribute.
Login-IP-Host	Use this attribute.
Reply-Message	Use this attribute.
Callback-Number	Use this attribute.
Callback-Id	Use this attribute.
Framed-Route	Use this attribute.
Framed-IPX-Network	Use this attribute.
Class	Use this attribute.
Called-Station-Id	Use this attribute.
Calling-Station-Id	Use this attribute.
NAS-Identifier	Use this attribute.
Proxy-State	Use this attribute.
Login-LAT-Service	Use this attribute.
Login-LAT-Node	Use this attribute.
Login-LAT-Group	Use this attribute.
Framed-AppleTalk-Zone	Use this attribute.
Acct-Session-Id	Use this attribute.
Acct-Multi-Session-Id	Use this attribute.

Parameter	Description	Type	Size	Default
sso-attribute	RADIUS attribute that contains the profile group name to be extracted from the RADIUS Start record.	option	-	Class

Option	Description
User-Name	Use this attribute.
NAS-IP-Address	Use this attribute.
Framed-IP-Address	Use this attribute.
Framed-IP-Netmask	Use this attribute.
Filter-Id	Use this attribute.
Login-IP-Host	Use this attribute.
Reply-Message	Use this attribute.
Callback-Number	Use this attribute.
Callback-Id	Use this attribute.
Framed-Route	Use this attribute.
Framed-IPX-Network	Use this attribute.
Class	Use this attribute.
Called-Station-Id	Use this attribute.
Calling-Station-Id	Use this attribute.
NAS-Identifier	Use this attribute.
Proxy-State	Use this attribute.
Login-LAT-Service	Use this attribute.
Login-LAT-Node	Use this attribute.
Login-LAT-Group	Use this attribute.
Framed-AppleTalk-Zone	Use this attribute.
Acct-Session-Id	Use this attribute.

Parameter	Description	Type	Size	Default
	Option / **Description** *Acct-Multi-Session-Id* — Use this attribute.			
sso-attribute-key	Key prefix for SSO group value in the SSO attribute.	string	Maximum length: 35	
sso-attribute-value-override	Enable/disable override old attribute value with new value for the same endpoint. **Option** / **Description** *enable* — Enable override old attribute value with new value for the same endpoint. *disable* — Disable override old attribute value with new value for the same endpoint.	option	-	enable
rsso-context-timeout	Time in seconds before the logged out user is removed from the "user context list" of logged on users.	integer	Minimum value: 0 Maximum value: 4294967295	28800
rsso-log-period	Time interval in seconds that group event log messages will be generated for dynamic profile events.	integer	Minimum value: 0 Maximum value: 4294967295	0
rsso-log-flags	Events to log. **Option** / **Description** *protocol-error* — Enable this log type. *profile-missing* — Enable this log type. *accounting-stop-missed* — Enable this log type.	option	-	protocol-error profile-missing accounting-stop-missed accounting-event endpoint-block radiusd-other

Parameter	Description	Type	Size	Default
	Option / **Description** *accounting-event* — Enable this log type. *endpoint-block* — Enable this log type. *radiusd-other* — Enable this log type. *none* — Disable all logging.			
rsso-flush-ip-session	Enable/disable flushing user IP sessions on RADIUS accounting Stop messages.	option	-	disable
	Option / **Description** *enable* — Enable flush user IP sessions on RADIUS accounting stop. *disable* — Disable flush user IP sessions on RADIUS accounting stop.			
rsso-ep-one-ip-only	Enable/disable the replacement of old IP addresses with new ones for the same endpoint on RADIUS accounting Start messages.	option	-	disable
	Option / **Description** *enable* — Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start. *disable* — Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.			

config accounting-server

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	Option / **Description** *enable* — Log to remote syslog server. *disable* — Do not log to remote syslog server.			
server	Server CN domain name or IP address.	string	Maximum length: 63	
secret	Secret key.	password	Not Specified	

Parameter	Description	Type	Size	Default
port	RADIUS accounting port number.	integer	Minimum value: 0 Maximum value: 65535	0
source-ip	Source IP address for communications to the RADIUS server.	string	Maximum length: 63	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	Set outgoing interface manually.

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

config user saml

SAML server entry configuration.

```
config user saml
    Description: SAML server entry configuration.
    edit <name>
        set cert {string}
        set entity-id {string}
        set single-sign-on-url {string}
        set single-logout-url {string}
        set idp-entity-id {string}
        set idp-single-sign-on-url {string}
        set idp-single-logout-url {string}
        set idp-cert {string}
        set user-name {string}
        set group-name {string}
        set digest-method [sha1|sha256]
        set limit-relaystate [enable|disable]
        set clock-tolerance {integer}
        set adfs-claim [enable|disable]
        set user-claim-type [email|given-name|...]
        set group-claim-type [email|given-name|...]
    next
end
```

config user saml

Parameter	Description	Type	Size	Default
cert	Certificate to sign SAML messages.	string	Maximum length: 35	
entity-id	SP entity ID.	string	Maximum length: 255	
single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255	
single-logout-url	SP single logout URL.	string	Maximum length: 255	
idp-entity-id	IDP entity ID.	string	Maximum length: 255	
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255	
idp-single-logout-url	IDP single logout url.	string	Maximum length: 255	
idp-cert	IDP Certificate name.	string	Maximum length: 35	
user-name	User name in assertion statement.	string	Maximum length: 255	
group-name	Group name in assertion statement.	string	Maximum length: 255	
digest-method	Digest method algorithm .	option	-	sha1

Option	Description
sha1	Digest Method Algorithm is SHA1.
sha256	Digest Method Algorithm is SHA256.

limit-relaystate	Enable/disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).	option	-	disable

Option	Description
enable	Enable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).
disable	Disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).

Parameter	Description	Type	Size	Default
clock-tolerance	Clock skew tolerance in seconds .	integer	Minimum value: 0 Maximum value: 300	15
adfs-claim	Enable/disable ADFS Claim for user/group attribute in assertion statement .	option	-	disable

Option	Description
enable	Enable ADFS Claim for user/group attribute in assertion statement.
disable	Disable ADFS Claim for user/group attribute in assertion statement.

Parameter	Description	Type	Size	Default
user-claim-type	User name claim in assertion statement.	option	-	upn

Option	Description
email	E-mail address of the user.
given-name	Given name of the user.
name	Unique name of the user.
upn	User principal name (UPN) of the user.
common-name	Common name of the user.
email-adfs-1x	E-mail address of the user when interoperating with AD FS 1.1 or ADFS 1.0.
group	Group that the user is a member of.
upn-adfs-1x	User principal name (UPN) of the user.
role	Role that the user has.
sur-name	Surname of the user
ppid	Private identifier of the user.
name-identifier	SAML name identifier of the user.
authentication-method	Method used to authenticate the user.
deny-only-group-sid	Deny-only group SID of the user.
deny-only-primary-sid	Deny-only primary SID of the user.
deny-only-primary-group-sid	Deny-only primary group SID of the user.

Parameter	Description	Type	Size	Default
	Option / **Description** *group-sid* — Group SID of the user. *primary-group-sid* — Primary group SID of the user. *primary-sid* — Primary SID of the user. *windows-account-name* — Domain account name of the user in the form of <domain>\<user>.			
group-claim-type	Group claim in assertion statement.	option	-	group
	Option / **Description** *email* — E-mail address of the user. *given-name* — Given name of the user. *name* — Unique name of the user. *upn* — User principal name (UPN) of the user. *common-name* — Common name of the user. *email-adfs-1x* — E-mail address of the user when interoperating with AD FS 1.1 or ADFS 1.0. *group* — Group that the user is a member of. *upn-adfs-1x* — User principal name (UPN) of the user. *role* — Role that the user has. *sur-name* — Surname of the user *ppid* — Private identifier of the user. *name-identifier* — SAML name identifier of the user. *authentication-method* — Method used to authenticate the user. *deny-only-group-sid* — Deny-only group SID of the user. *deny-only-primary-sid* — Deny-only primary SID of the user. *deny-only-primary-group-sid* — Deny-only primary group SID of the user. *group-sid* — Group SID of the user.			

Parameter	Description	Type	Size	Default
	Option — **Description** *primary-group-sid* — Primary group SID of the user. *primary-sid* — Primary SID of the user. *windows-account-name* — Domain account name of the user in the form of <domain>\<user>.			

config user security-exempt-list

Configure security exemption list.

```
config user security-exempt-list
    Description: Configure security exemption list.
    edit <name>
        set description {string}
        config rule
            Description: Configure rules for exempting users from captive portal
authentication.
            edit <id>
                set srcaddr <name1>, <name2>, ...
                set dstaddr <name1>, <name2>, ...
                set service <name1>, <name2>, ...
            next
        end
    next
end
```

config user security-exempt-list

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	

config rule

Parameter	Description	Type	Size	Default
srcaddr <name>	Source addresses or address groups. Address or group name.	string	Maximum length: 79	
dstaddr <name>	Destination addresses or address groups. Address or group name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
service <name>	Destination services. Service name.	string	Maximum length: 79	

config user setting

Configure user authentication setting.

```
config user setting
    Description: Configure user authentication setting.
    set auth-type {option1}, {option2}, ...
    set auth-cert {string}
    set auth-ca-cert {string}
    set auth-secure-http [enable|disable]
    set auth-http-basic [enable|disable]
    set auth-ssl-allow-renegotiation [enable|disable]
    set auth-src-mac [enable|disable]
    set auth-on-demand [always|implicitly]
    set auth-timeout {integer}
    set auth-timeout-type [idle-timeout|hard-timeout|...]
    set auth-portal-timeout {integer}
    set radius-ses-timeout-act [hard-timeout|ignore-timeout]
    set auth-blackout-time {integer}
    set auth-invalid-max {integer}
    set auth-lockout-threshold {integer}
    set auth-lockout-duration {integer}
    set per-policy-disclaimer [enable|disable]
    config auth-ports
        Description: Set up non-standard ports for authentication with HTTP, HTTPS, FTP, and
TELNET.
        edit <id>
            set type [http|https|...]
            set port {integer}
        next
    end
    set auth-ssl-min-proto-version [default|SSLv3|...]
    set auth-ssl-max-proto-version [sslv3|tlsv1|...]
    set auth-ssl-sigalgs [no-rsa-pss|all]
end
```

config user setting

Parameter	Description	Type	Size	Default
auth-type	Supported firewall policy authentication protocols/methods.	option	-	http https ftp telnet

Parameter	Description	Type	Size	Default
	Option / **Description** *http* — Allow HTTP authentication. *https* — Allow HTTPS authentication. *ftp* — Allow FTP authentication. *telnet* — Allow TELNET authentication.			
auth-cert	HTTPS server certificate for policy authentication.	string	Maximum length: 35	
auth-ca-cert	HTTPS CA certificate for policy authentication.	string	Maximum length: 35	
auth-secure-http	Enable/disable redirecting HTTP user authentication to more secure HTTPS.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
auth-http-basic	Enable/disable use of HTTP basic authentication for identity-based firewall policies.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
auth-ssl-allow-renegotiation	Allow/forbid SSL re-negotiation for HTTPS authentication.	option	-	disable
	Option / **Description** *enable* — Allow SSL re-negotiation. *disable* — Forbid SSL re-negotiation.			
auth-src-mac	Enable/disable source MAC for user identity.	option	-	enable
	Option / **Description** *enable* — Enable source MAC for user identity. *disable* — Disable source MAC for user identity.			
auth-on-demand	Always/implicitly trigger firewall authentication on demand.	option	-	implicitly

Parameter	Description	Type	Size	Default
	Option / **Description** *always* — Always trigger firewall authentication on demand. *implicitly* — Implicitly trigger firewall authentication on demand.			
auth-timeout	Time in minutes before the firewall user authentication timeout requires the user to re-authenticate.	integer	Minimum value: 1 Maximum value: 1440	5
auth-timeout-type	Control if authenticated users have to login again after a hard timeout, after an idle timeout, or after a session timeout.	option	-	idle-timeout
	Option / **Description** *idle-timeout* — Idle timeout. *hard-timeout* — Hard timeout. *new-session* — New session timeout.			
auth-portal-timeout	Time in minutes before captive portal user have to re-authenticate .	integer	Minimum value: 1 Maximum value: 30	3
radius-ses-timeout-act	Set the RADIUS session timeout to a hard timeout or to ignore RADIUS server session timeouts.	option	-	hard-timeout
	Option / **Description** *hard-timeout* — Use session timeout from RADIUS as hard-timeout. *ignore-timeout* — Ignore session timeout from RADIUS.			
auth-blackout-time	Time in seconds an IP address is denied access after failing to authenticate five times within one minute.	integer	Minimum value: 0 Maximum value: 3600	0
auth-invalid-max	Maximum number of failed authentication attempts before the user is blocked.	integer	Minimum value: 1 Maximum value: 100	5
auth-lockout-threshold	Maximum number of failed login attempts before login lockout is triggered.	integer	Minimum value: 1 Maximum value: 10	3

Parameter	Description	Type	Size	Default
auth-lockout-duration	Lockout period in seconds after too many login failures.	integer	Minimum value: 0 Maximum value: 4294967295	0
per-policy-disclaimer	Enable/disable per policy disclaimer.	option	-	disable

Option	Description
enable	Enable per policy disclaimer.
disable	Disable per policy disclaimer.

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

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.

Parameter	Description	Type	Size	Default
auth-ssl-max-proto-version	Maximum supported protocol version for SSL/TLS connections .	option	-	

Option	Description
sslv3	SSLv3.
tlsv1	TLSv1.
tlsv1-1	TLSv1.1.
tlsv1-2	TLSv1.2.
tlsv1-3	TLSv1.3.

Parameter	Description	Type	Size	Default
auth-ssl-sigalgs	Set signature algorithms related to HTTPS authentication .	option	-	all

Option	Description
no-rsa-pss	Disable RSA-PSS signature algorithms for HTTPS authentication.
all	Enable all supported signature algorithms for HTTPS authentication.

config auth-ports

Parameter	Description	Type	Size	Default
type	Service type.	option	-	http
	Option / **Description** *http* — HTTP service. *https* — HTTPS service. *ftp* — FTP service. *telnet* — TELNET service.			
port	Non-standard port for firewall user authentication.	integer	Minimum value: 1 Maximum value: 65535	1024

config user tacacs+

Configure TACACS+ server entries.

```
config user tacacs+
    Description: Configure TACACS+ server entries.
    edit <name>
        set server {string}
        set secondary-server {string}
        set tertiary-server {string}
        set port {integer}
        set key {password}
        set secondary-key {password}
        set tertiary-key {password}
        set authen-type [mschap|chap|...]
        set authorization [enable|disable]
        set source-ip {string}
        set interface-select-method [auto|sdwan|...]
        set interface {string}
    next
end
```

config user tacacs+

Parameter	Description	Type	Size	Default
server	Primary TACACS+ server CN domain name or IP address.	string	Maximum length: 63	
secondary-server	Secondary TACACS+ server CN domain name or IP address.	string	Maximum length: 63	
tertiary-server	Tertiary TACACS+ server CN domain name or IP address.	string	Maximum length: 63	
port	Port number of the TACACS+ server.	integer	Minimum value: 1 Maximum value: 65535	49
key	Key to access the primary server.	password	Not Specified	
secondary-key	Key to access the secondary server.	password	Not Specified	
tertiary-key	Key to access the tertiary server.	password	Not Specified	
authen-type	Allowed authentication protocols/methods.	option	-	auto

Option	Description
mschap	MSCHAP.
chap	CHAP.
pap	PAP.
ascii	ASCII.
auto	Use PAP, MSCHAP, and CHAP (in that order).

Parameter	Description	Type	Size	Default
authorization	Enable/disable TACACS+ authorization.	option	-	disable

Option	Description
enable	Enable TACACS+ authorization.
disable	Disable TACACS+ authorization.

Parameter	Description	Type	Size	Default
source-ip	Source IP address for communications to TACACS+ server.	string	Maximum length: 63	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

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

videofilter

This section includes syntax for the following commands:

config videofilter profile

Configure VideoFilter profile.

```
config videofilter profile
    Description: Configure VideoFilter profile.
    edit <name>
        set comment {var-string}
        set youtube-channel-filter {integer}
        config fortiguard-category
            Description: Configure FortiGuard categories.
            config filters
                Description: Configure VideoFilter FortiGuard category.
                edit <id>
                    set action [allow|monitor|...]
                    set category-id {integer}
                    set log [enable|disable]
                next
            end
        end
        set youtube [enable|disable]
        set vimeo [enable|disable]
        set dailymotion [enable|disable]
        set replacemsg-group {string}
    next
end
```

config videofilter profile

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

Parameter	Description	Type	Size	Default
youtube-channel-filter	Set YouTube channel filter.	integer	Minimum value: 0 Maximum value: 4294967295	0
youtube	Enable/disable YouTube video source.	option	-	enable
	Option / **Description** *enable* — Enable YouTube source. *disable* — Disable YouTube source.			
vimeo	Enable/disable Vimeo video source.	option	-	enable
	Option / **Description** *enable* — Enable Vimeo source. *disable* — Disable Vimeo source.			
dailymotion	Enable/disable Dailymotion video source.	option	-	enable
	Option / **Description** *enable* — Enable Dailymotion source. *disable* — Disable Dailymotion source.			
replacemsg-group	Replacement message group.	string	Maximum length: 35	

config filters

Parameter	Description	Type	Size	Default
action	VideoFilter action.	option	-	monitor
	Option / **Description** *allow* — Allow videos to be accessed. *monitor* — Monitor videos. *block* — Block videos.			
category-id	Category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

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

Option	Description
enable	Enable logging.
disable	Disable logging.

config videofilter youtube-channel-filter

Configure YouTube channel filter.

```
config videofilter youtube-channel-filter
    Description: Configure YouTube channel filter.
    edit <id>
        set name {string}
        set comment {var-string}
        set default-action [allow|monitor|...]
        config entries
            Description: YouTube filter entries.
            edit <id>
                set comment {var-string}
                set action [allow|monitor|...]
                set channel-id {string}
            next
        end
        set override-category [enable|disable]
        set log [enable|disable]
    next
end
```

config videofilter youtube-channel-filter

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
default-action	YouTube channel filter default action.	option	-	monitor

Option	Description
allow	Allow videos to be accessed.

Parameter	Description	Type	Size	Default
	Option / **Description** *monitor* — Monitor videos. *block* — Block videos.			
override-category	Enable/disable overriding category filtering result.	option	-	disable
	Option / **Description** *enable* — Enable overriding category filtering result. *disable* — Disable overriding category filtering result.			
log	Enable/disable logging.	option	-	disable
	Option / **Description** *enable* — Enable logging. *disable* — Disable logging.			

config entries

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
action	YouTube channel filter action.	option	-	monitor
	Option / **Description** *allow* — Allow videos to be accessed. *monitor* — Monitor videos. *block* — Block videos.			
channel-id	Channel ID.	string	Maximum length: 255	

config videofilter youtube-key

Configure YouTube API keys.

```
config videofilter youtube-key
    Description: Configure YouTube API keys.
    edit <id>
```

```
        set key {string}
    next
end
```

config videofilter youtube-key

Parameter	Description	Type	Size	Default
key	Key.	string	Maximum length: 47	

vpn

This section includes syntax for the following commands:

config vpn certificate ca

CA certificate.

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

config vpn certificate ca

Parameter	Description	Type	Size	Default
ca	CA certificate as a PEM file.	user	Not Specified	
range	Either global or VDOM IP address range for the CA certificate.	option	-	vdom
	Option / **Description** *global* — Global range. *vdom* — VDOM IP address range.			
source	CA certificate source type.	option	-	user
	Option / **Description** *factory* — Factory installed certificate. *user* — User generated certificate. *bundle* — Bundle file certificate.			
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-	enable
	Option / **Description** *enable* — Trusted CA for SSL inspection. *disable* — Untrusted CA for SSL inspection.			
scep-url	URL of the SCEP server.	string	Maximum length: 255	
auto-update-days	Number of days to wait before requesting an updated CA certificate .	integer	Minimum value: 0 Maximum value: 4294967295	0
auto-update-days-warning	Number of days before an expiry-warning message is generated .	integer	Minimum value: 0 Maximum value: 4294967295	0
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0
ca-identifier	CA identifier of the SCEP server.	string	Maximum length: 255	

config vpn certificate crl

Certificate Revocation List as a PEM file.

```
config vpn certificate crl
    Description: Certificate Revocation List as a PEM file.
    edit <name>
        set crl {user}
        set range [global|vdom]
        set source [factory|user|...]
        set update-vdom {string}
        set ldap-server {string}
        set ldap-username {string}
        set ldap-password {password}
        set http-url {string}
        set scep-url {string}
        set scep-cert {string}
        set update-interval {integer}
        set source-ip {ipv4-address}
    next
end
```

config vpn certificate crl

Parameter	Description	Type	Size	Default
crl	Certificate Revocation List as a PEM file.	user	Not Specified	
range	Either global or VDOM IP address range for the certificate.	option	-	vdom
	Option / **Description** *global* — Global range. *vdom* — VDOM IP address range.			
source	Certificate source type.	option	-	user
	Option / **Description** *factory* — Factory installed certificate. *user* — User generated certificate. *bundle* — Bundle file certificate.			
update-vdom	VDOM for CRL update.	string	Maximum length: 31	root
ldap-server	LDAP server name for CRL auto-update.	string	Maximum length: 35	

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

config vpn certificate local

Local keys and certificates.

```
config vpn certificate local
    Description: Local keys and certificates.
    edit <name>
        set type [normal|hsm]
        set nethsm-slot {string}
        set password {password}
        set comments {string}
        set private-key {user}
        set certificate {user}
        set csr {user}
        set state {user}
        set scep-url {string}
        set range [global|vdom]
        set source [factory|user|...]
        set auto-regenerate-days {integer}
        set auto-regenerate-days-warning {integer}
        set scep-password {password}
        set ca-identifier {string}
        set name-encoding [printable|utf8]
        set source-ip {ipv4-address}
        set ike-localid {string}
        set ike-localid-type [asn1dn|fqdn]
        set enroll-protocol [none|scep|...]
```

```
        set cmp-server {string}
        set cmp-path {string}
        set cmp-server-cert {string}
        set cmp-regeneration-method [keyupate|renewal]
        set acme-ca-url {string}
        set acme-domain {string}
        set acme-email {string}
        set acme-rsa-key-size {integer}
        set acme-renew-window {integer}
    next
end
```

config vpn certificate local

Parameter	Description	Type	Size	Default
type	Type.	option	-	normal
	Option / **Description** *normal* — Normal *hsm* — HSM			
nethsm-slot	Network HSM slot name.	string	Maximum length: 35	
password	Password as a PEM file.	password	Not Specified	
comments	Comment.	string	Maximum length: 511	
private-key	PEM format key encrypted with a password.	user	Not Specified	
certificate	PEM format certificate.	user	Not Specified	
csr	Certificate Signing Request.	user	Not Specified	
state	Certificate Signing Request State.	user	Not Specified	
scep-url	SCEP server URL.	string	Maximum length: 255	
range	Either a global or VDOM IP address range for the certificate.	option	-	vdom
	Option / **Description** *global* — Global range. *vdom* — VDOM IP address range.			

Parameter	Description	Type	Size	Default
source	Certificate source type.	option	-	user

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

auto-regenerate-days	Number of days to wait before expiry of an updated local certificate is requested (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0
auto-regenerate-days-warning	Number of days to wait before an expiry warning message is generated (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0
scep-password	SCEP server challenge password for auto-regeneration.	password	Not Specified	
ca-identifier	CA identifier of the CA server for signing via SCEP.	string	Maximum length: 255	
name-encoding	Name encoding method for auto-regeneration.	option	-	printable

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

source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0
ike-localid	Local ID the FortiProxy uses for authentication as a VPN client.	string	Maximum length: 63	
ike-localid-type	IKE local ID type.	option	-	asn1dn

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

Parameter	Description	Type	Size	Default
enroll-protocol	Certificate enrollment protocol.	option	-	none

Option	Description
none	None (default).
scep	Simple Certificate Enrollment Protocol.
cmpv2	Certificate Management Protocol Version 2.
acme2	Automated Certificate Management Environment Version 2.

cmp-server	Address and port for CMP server (format = address:port).	string	Maximum length: 63	
cmp-path	Path location inside CMP server.	string	Maximum length: 255	
cmp-server-cert	CMP server certificate.	string	Maximum length: 79	
cmp-regeneration-method	CMP auto-regeneration method.	option	-	keyupate

Option	Description
keyupate	Key Update.
renewal	Renewal.

acme-ca-url	The URL for the ACME CA server .	string	Maximum length: 255	https://acme-v02.api.letsencrypt.org/directory
acme-domain	A valid domain that resolves to this FortiProxy unit.	string	Maximum length: 255	
acme-email	Contact email address that is required by some CAs like LetsEncrypt.	string	Maximum length: 255	
acme-rsa-key-size	Length of the RSA private key of the generated cert (Minimum 2048 bits).	integer	Minimum value: 2048 Maximum value: 4096	2048
acme-renew-window	Beginning of the renewal window .	integer	Minimum value: 1 Maximum value: 60	30

config vpn certificate ocsp-server

OCSP server configuration.

```
config vpn certificate ocsp-server
    Description: OCSP server configuration.
    edit <name>
        set url {string}
        set cert {string}
        set secondary-url {string}
        set secondary-cert {string}
        set unavail-action [revoke|ignore]
        set source-ip {ipv4-address}
    next
end
```

config vpn certificate ocsp-server

Parameter	Description	Type	Size	Default
url	OCSP server URL.	string	Maximum length: 127	
cert	OCSP server certificate.	string	Maximum length: 127	
secondary-url	Secondary OCSP server URL.	string	Maximum length: 127	
secondary-cert	Secondary OCSP server certificate.	string	Maximum length: 127	
unavail-action	Action when server is unavailable (revoke the certificate or ignore the result of the check).	option	-	revoke

Option	Description
revoke	Revoke certificate if server is unavailable.
ignore	Ignore OCSP check if server is unavailable.

source-ip	Source IP address for communications to the OCSP server.	ipv4-address	Not Specified	0.0.0.0

config vpn certificate remote

Remote certificate as a PEM file.

```
config vpn certificate remote
    Description: Remote certificate as a PEM file.
```

```
    edit <name>
        set remote {user}
        set range [global|vdom]
        set source [factory|user|...]
    next
end
```

config vpn certificate remote

Parameter	Description	Type	Size	Default
remote	Remote certificate.	user	Not Specified	
range	Either the global or VDOM IP address range for the remote certificate.	option	-	vdom

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

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

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

config vpn certificate setting

VPN certificate setting.

```
config vpn certificate setting
    Description: VPN certificate setting.
    set ocsp-status [enable|disable]
    set ocsp-option [certificate|server]
    set proxy {string}
    set proxy-port {integer}
    set proxy-username {string}
    set proxy-password {password}
    set ssl-ocsp-source-ip {ipv4-address}
    set ocsp-default-server {string}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
    set check-ca-cert [enable|disable]
    set check-ca-chain [enable|disable]
    set subject-match [substring|value]
```

```
    set subject-set [subset|superset]
    set cn-match [substring|value]
    set cn-allow-multi [disable|enable]
    config crl-verification
        Description: CRL verification options.
        set expiry [ignore|revoke]
        set leaf-crl-absence [ignore|revoke]
        set chain-crl-absence [ignore|revoke]
    end
    set strict-ocsp-check [enable|disable]
    set ssl-min-proto-version [default|SSLv3|...]
    set cmp-save-extra-certs [enable|disable]
    set cmp-key-usage-checking [enable|disable]
    set certname-rsa1024 {string}
    set certname-rsa2048 {string}
    set certname-rsa4096 {string}
    set certname-dsa1024 {string}
    set certname-dsa2048 {string}
    set certname-ecdsa256 {string}
    set certname-ecdsa384 {string}
    set certname-ecdsa521 {string}
    set certname-ed25519 {string}
    set certname-ed448 {string}
end
```

config vpn certificate setting

Parameter	Description	Type	Size	Default
ocsp-status	Enable/disable receiving certificates using the OCSP.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
ocsp-option	Specify whether the OCSP URL is from certificate or configured OCSP server.	option	-	server
	Option / **Description** *certificate* — Use URL from certificate. *server* — Use URL from configured OCSP server.			
proxy	Proxy server FQDN or IP for OCSP/CA queries during certificate verification.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default
proxy-port	Proxy server port .	integer	Minimum value: 1 Maximum value: 65535	8080
proxy-username	Proxy server user name.	string	Maximum length: 63	
proxy-password	Proxy server password.	password	Not Specified	
ssl-ocsp-source-ip	Source IP address to use to communicate with the OCSP server.	ipv4-address	Not Specified	0.0.0.0
ocsp-default-server	Default OCSP server.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
check-ca-cert	Enable/disable verification of the user certificate and pass authentication if any CA in the chain is trusted .	option	-	enable
	Option / **Description** *enable* — Enable verification of the user certificate. *disable* — Disable verification of the user certificate.			
check-ca-chain	Enable/disable verification of the entire certificate chain and pass authentication only if the chain is complete and all of the CAs in the chain are trusted .	option	-	disable
	Option / **Description** *enable* — Enable verification of the entire certificate chain. *disable* — Disable verification of the entire certificate chain.			

Parameter	Description	Type	Size	Default
subject-match	When searching for a matching certificate, control how to do RDN value matching with certificate subject name .	option	-	substring

Option	Description
substring	Find a match if the name being searched for is a part or the same as a certificate subject RDN.
value	Find a match if the name being searched for is same as a certificate subject RDN.

Parameter	Description	Type	Size	Default
subject-set	When searching for a matching certificate, control how to do RDN set matching with certificate subject name .	option	-	subset

Option	Description
subset	Find a match if the name being searched for is a subset of a certificate subject.
superset	Find a match if the name being searched for is a superset of a certificate subject.

Parameter	Description	Type	Size	Default
cn-match	When searching for a matching certificate, control how to do CN value matching with certificate subject name .	option	-	substring

Option	Description
substring	Find a match if the name being searched for is a part or the same as a certificate CN.
value	Find a match if the name being searched for is same as a certificate CN.

Parameter	Description	Type	Size	Default
cn-allow-multi	When searching for a matching certificate, allow multiple CN fields in certificate subject name .	option	-	enable

Option	Description
disable	Does not allow multiple CN entries in certificate matching.
enable	Allow multiple CN entries in certificate matching.

Parameter	Description	Type	Size	Default
strict-ocsp-check	Enable/disable strict mode OCSP checking.	option	-	disable

Option	Description
enable	Enable strict mode OCSP checking.
disable	Disable strict mode OCSP checking.

Parameter	Description	Type	Size	Default
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections . **Option** — **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.	option	-	default
cmp-save-extra-certs	Enable/disable saving extra certificates in CMP mode . **Option** — **Description** *enable* — Enable saving extra certificates in CMP mode. *disable* — Disable saving extra certificates in CMP mode.	option	-	disable
cmp-key-usage-checking	Enable/disable server certificate key usage checking in CMP mode . **Option** — **Description** *enable* — Enable server certificate key usage checking in CMP mode. *disable* — Disable server certificate key usage checking in CMP mode.	option	-	enable
certname-rsa1024	1024 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_RSA1024
certname-rsa2048	2048 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_RSA2048
certname-rsa4096	4096 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_RSA4096
certname-dsa1024	1024 bit DSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_DSA1024
certname-dsa2048	2048 bit DSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_DSA2048

Parameter	Description	Type	Size	Default
certname-ecdsa256	256 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ECDSA256
certname-ecdsa384	384 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ECDSA384
certname-ecdsa521	521 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ECDSA521
certname-ed25519	253 bit EdDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ED25519
certname-ed448	456 bit EdDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ED448

config crl-verification

Parameter	Description	Type	Size	Default
expiry	CRL verification option when CRL is expired .	option	-	ignore

Option	Description
ignore	Certificate status will be verified even if CRL is expired.
revoke	Certificate will be revoked if CRL is expired.

Parameter	Description	Type	Size	Default
leaf-crl-absence	CRL verification option when leaf CRL is absent .	option	-	ignore

Option	Description
ignore	CRL verification against leaf certificate is ignored if CRL is absent.
revoke	Certificate will be revoked if CRL of leaf certificate is absent.

Parameter	Description	Type	Size	Default
chain-crl-absence	CRL verification option when CRL of any certificate in chain is absent .	option	-	ignore

Option	Description
ignore	CRL verification is ignored if CRL of any certificate in chain is absent.
revoke	Certificate will be revoked if CRL of any certificate in chain is absent.

config vpn ipsec phase1-interface

Configure VPN remote gateway.

```
config vpn ipsec phase1-interface
    Description: Configure VPN remote gateway.
    edit <name>
        set interface {string}
        set ike-version [1|2]
        set local-gw {ipv4-address}
        set remote-gw {ipv4-address}
        set keylife {integer}
        set certificate <name1>, <name2>, ...
        set authmethod [psk|signature]
        set mode [aggressive|main]
        set peertype {option}
        set peerid {string}
        set peer {string}
        set proposal {option1}, {option2}, ...
        set psksecret {password-3}
        set keepalive {integer}
        set distance {integer}
        set priority {integer}
        set localid {string}
        set localid-type [auto|fqdn|...]
        set negotiate-timeout {integer}
        set fragmentation [enable|disable]
        set comments {var-string}
        set send-cert-chain [enable|disable]
        set dhgrp {option1}, {option2}, ...
        set eap [enable|disable]
        set eap-identity [use-id-payload|send-request]
        set eap-exclude-peergrp {string}
        set acct-verify [enable|disable]
        set ppk [disable|allow|...]
        set ppk-secret {password-3}
        set ppk-identity {string}
        set wizard-type [custom|dialup-forticlient|...]
        set xauthtype [disable|client|...]
        set reauth [disable|enable]
        set authusr {string}
        set authpasswd {password}
        set group-authentication [enable|disable]
        set group-authentication-secret {password-3}
        set authusrgrp {string}
        set idle-timeout [enable|disable]
        set idle-timeoutinterval {integer}
        set inbound-dscp-copy [enable|disable]
        set auto-discovery-sender [enable|disable]
        set auto-discovery-receiver [enable|disable]
        set auto-discovery-forwarder [enable|disable]
        set auto-discovery-psk [enable|disable]
        set auto-discovery-shortcuts [independent|dependent]
        set fragmentation-mtu {integer}
        set childless-ike [enable|disable]
```

```
        set rekey [enable|disable]
        set digital-signature-auth [enable|disable]
        set signature-hash-alg {option1}, {option2}, ...
        set rsa-signature-format [pkcs1|pss]
        set enforce-unique-id [disable|keep-new|...]
        set cert-id-validation [enable|disable]
        set network-overlay [disable|enable]
        set network-id {integer}
        set loopback-asymroute [enable|disable]
    next
end
```

config vpn ipsec phase1-interface

Parameter	Description	Type	Size	Default
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35	
ike-version	IKE protocol version.	option	-	1
	Option / **Description** *1* — Use IKEv1 protocol. *2* — Use IKEv2 protocol.			
local-gw	IPv4 address of the local gateway's external interface.	ipv4-address	Not Specified	0.0.0.0
remote-gw	IPv4 address of the remote gateway's external interface.	ipv4-address	Not Specified	0.0.0.0
keylife	Time to wait in seconds before phase 1 encryption key expires.	integer	Minimum value: 120 Maximum value: 172800	86400
certificate <name>	The names of up to 4 signed personal certificates. Certificate name.	string	Maximum length: 79	
authmethod	Authentication method.	option	-	psk
	Option / **Description** *psk* — PSK authentication method. *signature* — Signature authentication method.			
mode	The ID protection mode used to establish a secure channel.	option	-	main

Parameter	Description	Type	Size	Default
	Option / **Description** *aggressive* / Aggressive mode. *main* / Main mode.			
peertype	Accept this peer type.	option	-	
	Option / **Description** *any* / Accept any peer ID.			
peerid	Accept this peer identity.	string	Maximum length: 255	
peer	Accept this peer certificate.	string	Maximum length: 35	
proposal	Phase1 proposal.	option	-	
	Option / **Description** *des-md5* / des-md5 *des-sha1* / des-sha1 *des-sha256* / des-sha256 *des-sha384* / des-sha384 *des-sha512* / des-sha512			
psksecret	Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	
keepalive	NAT-T keep alive interval.	integer	Minimum value: 10 Maximum value: 900	10
distance	Distance for routes added by IKE .	integer	Minimum value: 1 Maximum value: 255	15
priority	Priority for routes added by IKE .	integer	Minimum value: 1 Maximum value: 65535	1

Parameter	Description	Type	Size	Default
localid	Local ID.	string	Maximum length: 63	
localid-type	Local ID type.	option	-	auto

Option	Description
auto	Select ID type automatically.
fqdn	Use fully qualified domain name.
user-fqdn	Use user fully qualified domain name.
keyid	Use key-id string.
address	Use local IP address.
asn1dn	Use ASN.1 distinguished name.

Parameter	Description	Type	Size	Default
negotiate-timeout	IKE SA negotiation timeout in seconds .	integer	Minimum value: 1 Maximum value: 300	30
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-	enable

Option	Description
enable	Enable intra-IKE fragmentation support on re-transmission.
disable	Disable intra-IKE fragmentation support.

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 255	
send-cert-chain	Enable/disable sending certificate chain.	option	-	enable

Option	Description
enable	Enable sending certificate chain.
disable	Disable sending certificate chain.

Parameter	Description	Type	Size	Default
dhgrp	DH group.	option	-	14

Option	Description
1	DH Group 1.
2	DH Group 2.
5	DH Group 5.

Parameter	Description	Type	Size	Default
	Option / **Description** *14* DH Group 14. *15* DH Group 15. *16* DH Group 16. *17* DH Group 17. *18* DH Group 18. *19* DH Group 19. *20* DH Group 20. *21* DH Group 21. *27* DH Group 27. *28* DH Group 28. *29* DH Group 29. *30* DH Group 30. *31* DH Group 31. *32* DH Group 32.			
eap	Enable/disable IKEv2 EAP authentication.	option	-	disable
	Option / **Description** *enable* Enable IKEv2 EAP authentication. *disable* Disable IKEv2 EAP authentication.			
eap-identity	IKEv2 EAP peer identity type.	option	-	use-id-payload
	Option / **Description** *use-id-payload* Use IKEv2 IDi payload to resolve peer identity. *send-request* Use EAP identity request to resolve peer identity.			
eap-exclude-peergrp	Peer group excluded from EAP authentication.	string	Maximum length: 35	
acct-verify	Enable/disable verification of RADIUS accounting record.	option	-	disable
	Option / **Description** *enable* Enable verification of RADIUS accounting record. *disable* Disable verification of RADIUS accounting record.			

Parameter	Description	Type	Size	Default
ppk	Enable/disable IKEv2 Postquantum Preshared Key (PPK).	option	-	disable
	Option / **Description** *disable* — Disable use of IKEv2 Postquantum Preshared Key (PPK). *allow* — Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK). *require* — Require use of IKEv2 Postquantum Preshared Key (PPK).			
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35	
wizard-type	GUI VPN Wizard Type.	option	-	custom
	Option / **Description** *custom* — Custom VPN configuration. *dialup-forticlient* — Dial Up - FortiClient Windows, Mac and Android. *dialup-ios* — Dial Up - iPhone / iPad Native IPsec Client. *dialup-android* — Dial Up - Android Native IPsec Client. *dialup-windows* — Dial Up - Windows Native IPsec Client. *dialup-cisco* — Dial Up - Cisco IPsec Client. *static-fortiproxy* — Site to Site - FortiProxy. *dialup-fortiproxy* — Dial Up - FortiProxy. *static-cisco* — Site to Site - Cisco. *dialup-cisco-fw* — Dialup Up - Cisco Firewall. *simplified-static-fortiproxy* — Site to Site - FortiProxy (SD-WAN). *hub-fortiproxy-auto-discovery* — Hub role in a Hub-and-Spoke auto-discovery VPN. *spoke-fortiproxy-auto-discovery* — Spoke role in a Hub-and-Spoke auto-discovery VPN.			
xauthtype	XAuth type.	option	-	disable
	Option / **Description** *disable* — Disable.			

Parameter	Description	Type	Size	Default
	Option / **Description** *client* — Enable as client. *pap* — Enable as server PAP. *chap* — Enable as server CHAP. *auto* — Enable as server auto.			
reauth	Enable/disable re-authentication upon IKE SA lifetime expiration. **Option** / **Description** *disable* — Disable IKE SA re-authentication. *enable* — Enable IKE SA re-authentication.	option	-	disable
authusr	XAuth user name.	string	Maximum length: 64	
authpasswd	XAuth password (max 35 characters).	password	Not Specified	
group-authentication	Enable/disable IKEv2 IDi group authentication. **Option** / **Description** *enable* — Enable IKEv2 IDi group authentication. *disable* — Disable IKEv2 IDi group authentication.	option	-	disable
group-authentication-secret	Password for IKEv2 ID group authentication. ASCII string or hexadecimal indicated by a leading 0x.	password-3	Not Specified	
authusrgrp	Authentication user group.	string	Maximum length: 35	
idle-timeout	Enable/disable IPsec tunnel idle timeout. **Option** / **Description** *enable* — Enable IPsec tunnel idle timeout. *disable* — Disable IPsec tunnel idle timeout.	option	-	disable

Parameter	Description	Type	Size	Default
idle-timeoutinterval	IPsec tunnel idle timeout in minutes .	integer	Minimum value: 5 Maximum value: 43200	15
inbound-dscp-copy	Enable/disable copy the dscp in the ESP header to the inner IP Header.	option	-	disable
	Option / **Description** *enable* — Enable copy the dscp in the ESP header to the inner IP Header. *disable* — Disable copy the dscp in the ESP header to the inner IP Header.			
auto-discovery-sender	Enable/disable sending auto-discovery short-cut messages.	option	-	disable
	Option / **Description** *enable* — Enable sending auto-discovery short-cut messages. *disable* — Disable sending auto-discovery short-cut messages.			
auto-discovery-receiver	Enable/disable accepting auto-discovery short-cut messages.	option	-	disable
	Option / **Description** *enable* — Enable receiving auto-discovery short-cut messages. *disable* — Disable receiving auto-discovery short-cut messages.			
auto-discovery-forwarder	Enable/disable forwarding auto-discovery short-cut messages.	option	-	disable
	Option / **Description** *enable* — Enable forwarding auto-discovery short-cut messages. *disable* — Disable forwarding auto-discovery short-cut messages.			
auto-discovery-psk	Enable/disable use of pre-shared secrets for authentication of auto-discovery tunnels.	option	-	disable
	Option / **Description** *enable* — Enable use of pre-shared-secret authentication for auto-discovery tunnels. *disable* — Disable use of authentication defined by 'authmethod' for auto-discovery tunnels.			

Parameter	Description	Type	Size	Default
auto-discovery-shortcuts	Control deletion of child short-cut tunnels when the parent tunnel goes down.	option	-	independent
	Option / **Description** *independent* — Short-cut tunnels remain up if the parent tunnel goes down. *dependent* — Short-cut tunnels are brought down if the parent tunnel goes down.			
fragmentation-mtu	IKE fragmentation MTU .	integer	Minimum value: 500 Maximum value: 16000	1200
childless-ike	Enable/disable childless IKEv2 initiation (RFC 6023).	option	-	disable
	Option / **Description** *enable* — Enable childless IKEv2 initiation (RFC 6023). *disable* — Disable childless IKEv2 initiation (RFC 6023).			
rekey	Enable/disable phase1 rekey.	option	-	enable
	Option / **Description** *enable* — Enable phase1 rekey. *disable* — Disable phase1 rekey.			
digital-signature-auth	Enable/disable IKEv2 Digital Signature Authentication (RFC 7427).	option	-	disable
	Option / **Description** *enable* — Enable IKEv2 Digital Signature Authentication (RFC 7427). *disable* — Disable IKEv2 Digital Signature Authentication (RFC 7427).			
signature-hash-alg	Digital Signature Authentication hash algorithms.	option	-	sha2-512
	Option / **Description** *sha1* — SHA1. *sha2-256* — SHA2-256. *sha2-384* — SHA2-384. *sha2-512* — SHA2-512.			

Parameter	Description	Type	Size	Default
rsa-signature-format	Digital Signature Authentication RSA signature format.	option	-	pkcs1
	Option / **Description** *pkcs1* — RSASSA PKCS#1 v1.5. *pss* — RSASSA Probabilistic Signature Scheme (PSS).			
enforce-unique-id	Enable/disable peer ID uniqueness check.	option	-	disable
	Option / **Description** *disable* — Disable peer ID uniqueness enforcement. *keep-new* — Enforce peer ID uniqueness, keep new connection if collision found. *keep-old* — Enforce peer ID uniqueness, keep old connection if collision found.			
cert-id-validation	Enable/disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	option	-	enable
	Option / **Description** *enable* — Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945. *disable* — Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.			
network-overlay	Enable/disable network overlays.	option	-	disable
	Option / **Description** *disable* — Disable network overlays. *enable* — Enable network overlays.			
network-id	VPN gateway network ID.	integer	Minimum value: 0 Maximum value: 255	0
loopback-asymroute	Enable/disable asymmetric routing for IKE traffic on loopback interface.	option	-	enable
	Option / **Description** *enable* — Allow ingress/egress IKE traffic to be routed over different interfaces. *disable* — Ingress/egress IKE traffic must be routed over the same interface.			

config vpn ipsec phase2-interface

Configure VPN autokey tunnel.

```
config vpn ipsec phase2-interface
    Description: Configure VPN autokey tunnel.
    edit <name>
        set phase1name {string}
        set proposal {option1}, {option2}, ...
        set dhgrp {option1}, {option2}, ...
        set replay [enable|disable]
        set keepalive [enable|disable]
        set auto-negotiate [enable|disable]
        set add-route [phase1|enable|...]
        set inbound-dscp-copy [phase1|enable|...]
        set auto-discovery-sender [phase1|enable|...]
        set auto-discovery-forwarder [phase1|enable|...]
        set keylifeseconds {integer}
        set keylifekbs {integer}
        set keylife-type [seconds|kbs|...]
        set single-source [enable|disable]
        set route-overlap [use-old|use-new|...]
        set comments {var-string}
        set protocol {integer}
        set src-name {string}
        set src-name6 {string}
        set src-addr-type [subnet|range|...]
        set src-start-ip {ipv4-address-any}
        set src-start-ip6 {ipv6-address}
        set src-end-ip {ipv4-address-any}
        set src-end-ip6 {ipv6-address}
        set src-subnet {ipv4-classnet-any}
        set src-subnet6 {ipv6-prefix}
        set src-port {integer}
        set dst-name {string}
        set dst-name6 {string}
        set dst-addr-type [subnet|range|...]
        set dst-start-ip {ipv4-address-any}
        set dst-start-ip6 {ipv6-address}
        set dst-end-ip {ipv4-address-any}
        set dst-end-ip6 {ipv6-address}
        set dst-subnet {ipv4-classnet-any}
        set dst-subnet6 {ipv6-prefix}
        set dst-port {integer}
    next
end
```

config vpn ipsec phase2-interface

Parameter	Description	Type	Size	Default
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 15	
proposal	Phase2 proposal.	option	-	

Option	Description
null-md5	null-md5
null-sha1	null-sha1
null-sha256	null-sha256
null-sha384	null-sha384
null-sha512	null-sha512
des-null	des-null
des-md5	des-md5
des-sha1	des-sha1
des-sha256	des-sha256
des-sha384	des-sha384
des-sha512	des-sha512

Parameter	Description	Type	Size	Default
dhgrp	Phase2 DH group.	option	-	14

Option	Description
1	DH Group 1.
2	DH Group 2.
5	DH Group 5.
14	DH Group 14.
15	DH Group 15.
16	DH Group 16.
17	DH Group 17.
18	DH Group 18.
19	DH Group 19.
20	DH Group 20.
21	DH Group 21.

Parameter	Description	Type	Size	Default
	Option / **Description** *27* DH Group 27. *28* DH Group 28. *29* DH Group 29. *30* DH Group 30. *31* DH Group 31. *32* DH Group 32.			
replay	Enable/disable replay detection.	option	-	enable
	Option / **Description** *enable* Enable setting. *disable* Disable setting.			
keepalive	Enable/disable keep alive.	option	-	disable
	Option / **Description** *enable* Enable setting. *disable* Disable setting.			
auto-negotiate	Enable/disable IPsec SA auto-negotiation.	option	-	disable
	Option / **Description** *enable* Enable setting. *disable* Disable setting.			
add-route	Enable/disable automatic route addition.	option	-	phase1
	Option / **Description** *phase1* Add route according to phase1 add-route setting. *enable* Add route for remote proxy ID. *disable* Do not add route for remote proxy ID.			
inbound-dscp-copy	Enable/disable copy the dscp in the ESP header to the inner IP Header.	option	-	phase1

Parameter	Description	Type	Size	Default
	Option / **Description** *phase1* — copy the dscp in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting. *enable* — Enable copy the dscp in the ESP header to the inner IP Header. *disable* — Disable copy the dscp in the ESP header to the inner IP Header.			
auto-discovery-sender	Enable/disable sending short-cut messages.	option	-	phase1
	Option / **Description** *phase1* — Send short-cut messages according to the phase1 auto-discovery-sender setting. *enable* — Enable sending auto-discovery short-cut messages. *disable* — Disable sending auto-discovery short-cut messages.			
auto-discovery-forwarder	Enable/disable forwarding short-cut messages.	option	-	phase1
	Option / **Description** *phase1* — Forward short-cut messages according to the phase1 auto-discovery-forwarder setting. *enable* — Enable forwarding auto-discovery short-cut messages. *disable* — Disable forwarding auto-discovery short-cut messages.			
keylifeseconds	Phase2 key life in time in seconds .	integer	Minimum value: 120 Maximum value: 172800	43200
keylifekbs	Phase2 key life in number of kilobytes of traffic .	integer	Minimum value: 5120 Maximum value: 4294967295	5120
keylife-type	Keylife type.	option	-	seconds
	Option / **Description** *seconds* — Key life in seconds. *kbs* — Key life in kilobytes. *both* — Key life both.			

Parameter	Description	Type	Size	Default
single-source	Enable/disable single source IP restriction.	option	-	disable
	Option / **Description** *enable* — Only single source IP will be accepted. *disable* — Source IP range will be accepted.			
route-overlap	Action for overlapping routes.	option	-	use-new
	Option / **Description** *use-old* — Use the old route and do not add the new route. *use-new* — Delete the old route and add the new route. *allow* — Allow overlapping routes.			
comments	Comment.	var-string	Maximum length: 255	
protocol	Quick mode protocol selector .	integer	Minimum value: 0 Maximum value: 255	0
src-name	Local proxy ID name.	string	Maximum length: 79	
src-name6	Local proxy ID name.	string	Maximum length: 79	
src-addr-type	Local proxy ID type.	option	-	subnet
	Option / **Description** *subnet* — IPv4 subnet. *range* — IPv4 range. *ip* — IPv4 IP. *name* — IPv4 firewall address or group name. *subnet6* — IPv6 subnet. *range6* — IPv6 range. *ip6* — IPv6 IP. *name6* — IPv6 firewall address or group name.			
src-start-ip	Local proxy ID start.	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
src-start-ip6	Local proxy ID IPv6 start.	ipv6-address	Not Specified	::
src-end-ip	Local proxy ID end.	ipv4-address-any	Not Specified	0.0.0.0
src-end-ip6	Local proxy ID IPv6 end.	ipv6-address	Not Specified	::
src-subnet	Local proxy ID subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
src-subnet6	Local proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0
src-port	Quick mode source port .	integer	Minimum value: 0 Maximum value: 65535	0
dst-name	Remote proxy ID name.	string	Maximum length: 79	
dst-name6	Remote proxy ID name.	string	Maximum length: 79	
dst-addr-type	Remote proxy ID type.	option	-	subnet

Option	Description
subnet	IPv4 subnet.
range	IPv4 range.
ip	IPv4 IP.
name	IPv4 firewall address or group name.
subnet6	IPv6 subnet.
range6	IPv6 range.
ip6	IPv6 IP.
name6	IPv6 firewall address or group name.

dst-start-ip	Remote proxy ID IPv4 start.	ipv4-address-any	Not Specified	0.0.0.0
dst-start-ip6	Remote proxy ID IPv6 start.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default
dst-end-ip	Remote proxy ID IPv4 end.	ipv4-address-any	Not Specified	0.0.0.0
dst-end-ip6	Remote proxy ID IPv6 end.	ipv6-address	Not Specified	::
dst-subnet	Remote proxy ID IPv4 subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
dst-subnet6	Remote proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0
dst-port	Quick mode destination port .	integer	Minimum value: 0 Maximum value: 65535	0

config vpn ssl monitor

SSL-VPN session.

```
config vpn ssl monitor
    Description: SSL-VPN session.
end
```

config vpn ssl settings

Configure SSL-VPN.

```
config vpn ssl settings
    Description: Configure SSL-VPN.
    set status [enable|disable]
    set reqclientcert [enable|disable]
    set user-peer {string}
    set ssl-max-proto-ver [tls1-0|tls1-1|...]
    set ssl-min-proto-ver [tls1-0|tls1-1|...]
    set banned-cipher {option1}, {option2}, ...
    set ciphersuite {option1}, {option2}, ...
    set ssl-insert-empty-fragment [enable|disable]
    set https-redirect [enable|disable]
    set x-content-type-options [enable|disable]
    set ssl-client-renegotiation [disable|enable]
    set force-two-factor-auth [enable|disable]
    set unsafe-legacy-renegotiation [enable|disable]
    set servercert {string}
    set idle-timeout {integer}
    set auth-timeout {integer}
```

```
    set login-attempt-limit {integer}
    set login-block-time {integer}
    set login-timeout {integer}
    set dtls-hello-timeout {integer}
    set tunnel-ip-pools <name1>, <name2>, ...
    set tunnel-ipv6-pools <name1>, <name2>, ...
    set dns-suffix {var-string}
    set dns-server1 {ipv4-address}
    set dns-server2 {ipv4-address}
    set wins-server1 {ipv4-address}
    set wins-server2 {ipv4-address}
    set ipv6-dns-server1 {ipv6-address}
    set ipv6-dns-server2 {ipv6-address}
    set ipv6-wins-server1 {ipv6-address}
    set ipv6-wins-server2 {ipv6-address}
    set url-obscuration [enable|disable]
    set http-compression [enable|disable]
    set http-only-cookie [enable|disable]
    set deflate-compression-level {integer}
    set deflate-min-data-size {integer}
    set port {integer}
    set port-precedence [enable|disable]
    set auto-tunnel-static-route [enable|disable]
    set header-x-forwarded-for [pass|add|...]
    set source-interface <name1>, <name2>, ...
    set source-address <name1>, <name2>, ...
    set source-address-negate [enable|disable]
    set source-address6 <name1>, <name2>, ...
    set source-address6-negate [enable|disable]
    set default-portal {string}
    config authentication-rule
        Description: Authentication rule for SSL-VPN.
        edit <id>
            set source-interface <name1>, <name2>, ...
            set source-address <name1>, <name2>, ...
            set source-address-negate [enable|disable]
            set source-address6 <name1>, <name2>, ...
            set source-address6-negate [enable|disable]
            set users <name1>, <name2>, ...
            set groups <name1>, <name2>, ...
            set portal {string}
            set realm {string}
            set client-cert [enable|disable]
            set user-peer {string}
            set auth [any|local|...]
        next
    end
    set dtls-tunnel [enable|disable]
    set dtls-max-proto-ver [dtls1-0|dtls1-2]
    set dtls-min-proto-ver [dtls1-0|dtls1-2]
    set check-referer [enable|disable]
    set http-request-header-timeout {integer}
    set http-request-body-timeout {integer}
    set auth-session-check-source-ip [enable|disable]
    set tunnel-connect-without-reauth [enable|disable]
    set tunnel-user-session-timeout {integer}
```

```
    set hsts-include-subdomains [enable|disable]
    set transform-backward-slashes [enable|disable]
    set encode-2f-sequence [enable|disable]
    set encrypt-and-store-password [enable|disable]
    set client-sigalgs [no-rsa-pss|all]
    set dual-stack-mode [enable|disable]
    set tunnel-addr-assigned-method [first-available|round-robin]
    set saml-redirect-port {integer}
    set web-mode-snat [enable|disable]
end
```

config vpn ssl settings

Parameter	Description	Type	Size	Default
status	Enable/disable SSL-VPN.	option	-	enable
	Option / **Description** *enable* — Enable SSL-VPN. *disable* — Disable SSL-VPN.			
reqclientcert	Enable/disable to require client certificates for all SSL-VPN users.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
user-peer	Name of user peer.	string	Maximum length: 35	
ssl-max-proto-ver	SSL maximum protocol version.	option	-	tls1-3
	Option / **Description** *tls1-0* — TLS version 1.0. *tls1-1* — TLS version 1.1. *tls1-2* — TLS version 1.2. *tls1-3* — TLS version 1.3.			
ssl-min-proto-ver	SSL minimum protocol version.	option	-	tls1-2
	Option / **Description** *tls1-0* — TLS version 1.0.			

Parameter	Description	Type	Size	Default
	Option / **Description** *tls1-1* — TLS version 1.1. *tls1-2* — TLS version 1.2. *tls1-3* — TLS version 1.3.			
banned-cipher	Select one or more cipher technologies that cannot be used in SSL-VPN negotiations. Only applies to TLS 1.2 and below.	option	-	
	Option / **Description** *RSA* — Ban the use of cipher suites using RSA key. *DHE* — Ban the use of cipher suites using authenticated ephemeral DH key agreement. *ECDHE* — Ban the use of cipher suites using authenticated ephemeral ECDH key agreement. *DSS* — Ban the use of cipher suites using DSS authentication. *ECDSA* — Ban the use of cipher suites using ECDSA authentication. *AES* — Ban the use of cipher suites using either 128 or 256 bit AES. *AESGCM* — Ban the use of cipher suites AES in Galois Counter Mode (GCM). *CAMELLIA* — Ban the use of cipher suites using either 128 or 256 bit CAMELLIA. *3DES* — Ban the use of cipher suites using triple DES *SHA1* — Ban the use of cipher suites using HMAC-SHA1. *SHA256* — Ban the use of cipher suites using HMAC-SHA256. *SHA384* — Ban the use of cipher suites using HMAC-SHA384. *STATIC* — Ban the use of cipher suites using static keys. *CHACHA20* — Ban the use of cipher suites using ChaCha20. *ARIA* — Ban the use of cipher suites using ARIA. *AESCCM* — Ban the use of cipher suites using AESCCM.			

Parameter	Description	Type	Size	Default
ciphersuite	Select one or more TLS 1.3 ciphersuites to enable. Does not affect ciphers in TLS 1.2 and below. At least one must be enabled. To disable all, set ssl-max-proto-ver to tls1-2 or below.	option	-	TLS-AES-128-GCM-SHA256 TLS-AES-256-GCM-SHA384 TLS-CHACHA20-POLY1305-SHA256
	Option / **Description** *TLS-AES-128-GCM-SHA256* — Enable TLS-AES-128-GCM-SHA256 in TLS 1.3. *TLS-AES-256-GCM-SHA384* — Enable TLS-AES-256-GCM-SHA384 in TLS 1.3. *TLS-CHACHA20-POLY1305-SHA256* — Enable TLS-CHACHA20-POLY1305-SHA256 in TLS 1.3. *TLS-AES-128-CCM-SHA256* — Enable TLS-AES-128-CCM-SHA256 in TLS 1.3. *TLS-AES-128-CCM-8-SHA256* — Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.			
ssl-insert-empty-fragment	Enable/disable insertion of empty fragment.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
https-redirect	Enable/disable redirect of port 80 to SSL-VPN port.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
x-content-type-options	Add HTTP X-Content-Type-Options header.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
ssl-client-renegotiation	Enable/disable to allow client renegotiation by the server if the tunnel goes down.	option	-	disable
	Option / **Description** *disable* / Abort any SSL connection that attempts to renegotiate. *enable* / Allow a SSL client to renegotiate.			
force-two-factor-auth	Enable/disable only PKI users with two-factor authentication for SSL-VPNs.	option	-	disable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
unsafe-legacy-renegotiation	Enable/disable unsafe legacy re-negotiation.	option	-	disable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
servercert	Name of the server certificate to be used for SSL-VPNs.	string	Maximum length: 35	self-sign
idle-timeout	SSL-VPN disconnects if idle for specified time in seconds.	integer	Minimum value: 0 Maximum value: 259200	300
auth-timeout	SSL-VPN authentication timeout .	integer	Minimum value: 0 Maximum value: 259200	28800
login-attempt-limit	SSL-VPN maximum login attempt times before block .	integer	Minimum value: 0 Maximum value: 4294967295	2

Parameter	Description	Type	Size	Default
login-block-time	Time for which a user is blocked from logging in after too many failed login attempts .	integer	Minimum value: 0 Maximum value: 4294967295	60
login-timeout	SSLVPN maximum login timeout .	integer	Minimum value: 10 Maximum value: 180	30
dtls-hello-timeout	SSLVPN maximum DTLS hello timeout .	integer	Minimum value: 10 Maximum value: 60	10
tunnel-ip-pools <name>	Names of the IPv4 IP Pool firewall objects that define the IP addresses reserved for remote clients. Address name.	string	Maximum length: 79	
tunnel-ipv6-pools <name>	Names of the IPv6 IP Pool firewall objects that define the IP addresses reserved for remote clients. Address name.	string	Maximum length: 79	
dns-suffix	DNS suffix used for SSL-VPN clients.	var-string	Maximum length: 253	
dns-server1	DNS server 1.	ipv4-address	Not Specified	0.0.0.0
dns-server2	DNS server 2.	ipv4-address	Not Specified	0.0.0.0
wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0
wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::
ipv6-wins-server1	IPv6 WINS server 1.	ipv6-address	Not Specified	::
ipv6-wins-server2	IPv6 WINS server 2.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default
url-obscuration	Enable/disable to obscure the host name of the URL of the web browser display. **Option** — **Description** *enable* — Enable setting. *disable* — Disable setting.	option	-	disable
http-compression	Enable/disable to allow HTTP compression over SSL-VPN tunnels. **Option** — **Description** *enable* — Enable setting. *disable* — Disable setting.	option	-	disable
http-only-cookie	Enable/disable SSL-VPN support for HttpOnly cookies. **Option** — **Description** *enable* — Enable setting. *disable* — Disable setting.	option	-	enable
deflate-compression-level	Compression level (0~9).	integer	Minimum value: 0 Maximum value: 9	6
deflate-min-data-size	Minimum amount of data that triggers compression .	integer	Minimum value: 200 Maximum value: 65535	300
port	SSL-VPN access port .	integer	Minimum value: 1 Maximum value: 65535	10443
port-precedence	Enable/disable, Enable means that if SSL-VPN connections are allowed on an interface admin GUI connections are blocked on that interface. **Option** — **Description** *enable* — Enable setting. *disable* — Disable setting.	option	-	enable

Parameter	Description	Type	Size	Default
auto-tunnel-static-route	Enable/disable to auto-create static routes for the SSL-VPN tunnel IP addresses.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
header-x-forwarded-for	Forward the same, add, or remove HTTP header.	option	-	add
	Option / **Description** *pass* — Forward the same HTTP header. *add* — Add the HTTP header. *remove* — Remove the HTTP header.			
source-interface <name>	SSL-VPN source interface of incoming traffic. Interface name.	string	Maximum length: 35	
source-address <name>	Source address of incoming traffic. Address name.	string	Maximum length: 79	
source-address-negate	Enable/disable negated source address match.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
source-address6 <name>	IPv6 source address of incoming traffic. IPv6 address name.	string	Maximum length: 79	
source-address6-negate	Enable/disable negated source IPv6 address match.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
default-portal	Default SSL-VPN portal.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
dtls-tunnel	Enable/disable DTLS to prevent eavesdropping, tampering, or message forgery.	option	-	disable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
dtls-max-proto-ver	DTLS maximum protocol version.	option	-	dtls1-2
	Option / **Description** *dtls1-0* / DTLS version 1.0. *dtls1-2* / DTLS version 1.2.			
dtls-min-proto-ver	DTLS minimum protocol version.	option	-	dtls1-0
	Option / **Description** *dtls1-0* / DTLS version 1.0. *dtls1-2* / DTLS version 1.2.			
check-referer	Enable/disable verification of referer field in HTTP request header.	option	-	disable
	Option / **Description** *enable* / Enable verification of referer field in HTTP request header. *disable* / Disable verification of referer field in HTTP request header.			
http-request-header-timeout	SSL-VPN session is disconnected if an HTTP request header is not received within this time .	integer	Minimum value: 0 Maximum value: 4294967295	20
http-request-body-timeout	SSL-VPN session is disconnected if an HTTP request body is not received within this time .	integer	Minimum value: 0 Maximum value: 4294967295	30
auth-session-check-source-ip	Enable/disable checking of source IP for authentication session.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable checking of source IP for authentication session. *disable* — Disable checking of source IP for authentication session.			
tunnel-connect-without-reauth	Enable/disable tunnel connection without re-authorization if previous connection dropped.	option	-	disable
	Option / **Description** *enable* — Enable tunnel connection without re-authorization. *disable* — Disable tunnel connection without re-authorization.			
tunnel-user-session-timeout	Time out value to clean up user session after tunnel connection is dropped .	integer	Minimum value: 1 Maximum value: 255	30
hsts-include-subdomains	Add HSTS includeSubDomains response header.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
transform-backward-slashes	Transform backward slashes to forward slashes in URLs.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
encode-2f-sequence	Encode \2F sequence to forward slash in URLs.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
encrypt-and-store-password	Encrypt and store user passwords for SSL-VPN web sessions.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
client-sigalgs	Set signature algorithms related to client authentication. Affects TLS version <= 1.2 only.	option	-	all
	Option / **Description** *no-rsa-pss* — Disable RSA-PSS signature algorithms for client authentication. *all* — Enable all supported signature algorithms for client authentication.			
dual-stack-mode	Tunnel mode: enable parallel IPv4 and IPv6 tunnel. Web mode: support IPv4 and IPv6 bookmarks in the portal.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
tunnel-addr-assigned-method	Method used for assigning address for tunnel.	option	-	first-available
	Option / **Description** *first-available* — Assign the first available address from the pools. *round-robin* — Assign the available address from the pool with a round robin fashion.			
saml-redirect-port	SAML local redirect port in the machine running FortiClient . 0 is to disable redirection on FGT side.	integer	Minimum value: 0 Maximum value: 65535	8020
web-mode-snat	Enable/disable use of IP pools defined in firewall policy while using web-mode.	option	-	disable
	Option / **Description** *enable* — Enable use of IP pools defined in firewall policy while using web-mode. *disable* — Disable use of IP pools defined in firewall policy while using web-mode.			

config authentication-rule

Parameter	Description	Type	Size	Default
source-interface <name>	SSL-VPN source interface of incoming traffic. Interface name.	string	Maximum length: 35	
source-address <name>	Source address of incoming traffic. Address name.	string	Maximum length: 79	
source-address-negate	Enable/disable negated source address match.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
source-address6 <name>	IPv6 source address of incoming traffic. IPv6 address name.	string	Maximum length: 79	
source-address6-negate	Enable/disable negated source IPv6 address match.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
users <name>	User name. User name.	string	Maximum length: 79	
groups <name>	User groups. Group name.	string	Maximum length: 79	
portal	SSL-VPN portal.	string	Maximum length: 35	
realm	SSL-VPN realm.	string	Maximum length: 35	
client-cert	Enable/disable SSL-VPN client certificate restrictive.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			

Parameter	Description	Type	Size	Default
user-peer	Name of user peer.	string	Maximum length: 35	
auth	SSL-VPN authentication method restriction.	option	-	any

Option	Description
any	Any
local	Local
radius	RADIUS
tacacs+	TACACS+
ldap	LDAP
peer	PEER

config vpn ssl web host-check-software

SSL-VPN host check software.

```
config vpn ssl web host-check-software
    Description: SSL-VPN host check software.
    edit <name>
        set os-type [windows|macos]
        set type [av|fw]
        set version {string}
        set guid {user}
        config check-item-list
            Description: Check item list.
            edit <id>
                set action [require|deny]
                set type [file|registry|...]
                set target {string}
                set version {string}
                set md5s <id1>, <id2>, ...
            next
        end
    next
end
```

config vpn ssl web host-check-software

Parameter	Description	Type	Size	Default
os-type	OS type.	option	-	windows

Parameter	Description	Type	Size	Default
	Option / **Description** *windows* / Microsoft Windows operating system. *macos* / Apple MacOS operating system.			
type	Type.	option	-	av
	Option / **Description** *av* / AntiVirus. *fw* / Firewall.			
version	Version.	string	Maximum length: 35	
guid	Globally unique ID.	user	Not Specified	

config check-item-list

Parameter	Description	Type	Size	Default
action	Action.	option	-	require
	Option / **Description** *require* / Require. *deny* / Deny.			
type	Type.	option	-	file
	Option / **Description** *file* / File. *registry* / Registry. *process* / Process.			
target	Target.	string	Maximum length: 255	
version	Version.	string	Maximum length: 35	
md5s <id>	MD5 checksum. Hex string of MD5 checksum.	string	Maximum length: 32	

config vpn ssl web portal

Portal.

```
config vpn ssl web portal
    Description: Portal.
    edit <name>
        set tunnel-mode [enable|disable]
        set ip-mode [range|user-group|...]
        set dhcp-ip-overlap [use-new|use-old]
        set auto-connect [enable|disable]
        set keep-alive [enable|disable]
        set save-password [enable|disable]
        set ip-pools <name1>, <name2>, ...
        set exclusive-routing [enable|disable]
        set service-restriction [enable|disable]
        set split-tunneling [enable|disable]
        set split-tunneling-routing-negate [enable|disable]
        set split-tunneling-routing-address <name1>, <name2>, ...
        set dns-server1 {ipv4-address}
        set dns-server2 {ipv4-address}
        set dns-suffix {var-string}
        set wins-server1 {ipv4-address}
        set wins-server2 {ipv4-address}
        set ipv6-tunnel-mode [enable|disable]
        set ipv6-pools <name1>, <name2>, ...
        set ipv6-exclusive-routing [enable|disable]
        set ipv6-service-restriction [enable|disable]
        set ipv6-split-tunneling [enable|disable]
        set ipv6-split-tunneling-routing-negate [enable|disable]
        set ipv6-split-tunneling-routing-address <name1>, <name2>, ...
        set ipv6-dns-server1 {ipv6-address}
        set ipv6-dns-server2 {ipv6-address}
        set ipv6-wins-server1 {ipv6-address}
        set ipv6-wins-server2 {ipv6-address}
        set web-mode [enable|disable]
        set display-bookmark [enable|disable]
        set user-bookmark [enable|disable]
        set allow-user-access {option1}, {option2}, ...
        set user-group-bookmark [enable|disable]
        config bookmark-group
            Description: Portal bookmark group.
            edit <name>
                config bookmarks
                    Description: Bookmark table.
                    edit <name>
                        set apptype [ftp|rdp|...]
                        set url {var-string}
                        set host {var-string}
                        set folder {var-string}
                        set domain {var-string}
                        set additional-params {var-string}
                        set description {var-string}
                        set keyboard-layout [ar-101|ar-102|...]
                        set security [rdp|nla|...]
```

```
                set send-preconnection-id [enable|disable]
                set preconnection-id {integer}
                set preconnection-blob {var-string}
                set load-balancing-info {var-string}
                set restricted-admin [enable|disable]
                set port {integer}
                set logon-user {var-string}
                set logon-password {password}
                set color-depth [32|16|...]
                set sso [disable|static|...]
                config form-data
                    Description: Form data.
                    edit <name>
                        set value {var-string}
                    next
                end
                set sso-credential [sslvpn-login|alternative]
                set sso-username {var-string}
                set sso-password {password}
                set sso-credential-sent-once [enable|disable]
                set width {integer}
                set height {integer}
            next
        end
    next
end
set display-connection-tools [enable|disable]
set display-history [enable|disable]
set display-status [enable|disable]
set rewrite-ip-uri-ui [enable|disable]
set heading {string}
set redir-url {var-string}
set theme [jade|neutrino|...]
set custom-lang {string}
set smb-ntlmv1-auth [enable|disable]
set smbv1 [enable|disable]
set smb-min-version [smbv1|smbv2|...]
set smb-max-version [smbv1|smbv2|...]
set use-sdwan [enable|disable]
set prefer-ipv6-dns [enable|disable]
set clipboard [enable|disable]
set default-window-width {integer}
set default-window-height {integer}
set host-check [none|av|...]
set host-check-interval {integer}
set host-check-policy <name1>, <name2>, ...
set limit-user-logins [enable|disable]
set mac-addr-check [enable|disable]
set mac-addr-action [allow|deny]
config mac-addr-check-rule
    Description: Client MAC address check rule.
    edit <name>
        set mac-addr-mask {integer}
        set mac-addr-list <addr1>, <addr2>, ...
    next
end
```

```
        set os-check [enable|disable]
        config os-check-list
            Description: SSL-VPN OS checks.
            edit <name>
                set action [deny|allow|...]
                set tolerance {integer}
                set latest-patch-level {user}
            next
        end
        set forticlient-download [enable|disable]
        set forticlient-download-method [direct|ssl-vpn]
        set customize-forticlient-download-url [enable|disable]
        set windows-forticlient-download-url {var-string}
        set macos-forticlient-download-url {var-string}
        set skip-check-for-unsupported-os [enable|disable]
        set skip-check-for-browser [enable|disable]
        set hide-sso-credential [enable|disable]
        config split-dns
            Description: Split DNS for SSL-VPN.
            edit <id>
                set domains {var-string}
                set dns-server1 {ipv4-address}
                set dns-server2 {ipv4-address}
            next
        end
    next
end
```

config vpn ssl web portal

Parameter	Description	Type	Size	Default
tunnel-mode	Enable/disable IPv4 SSL-VPN tunnel mode.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
ip-mode	Method by which users of this SSL-VPN tunnel obtain IP addresses.	option	-	range

Option	Description
range	Use the IP addresses available for all SSL-VPN users as defined by the SSL settings command.
user-group	Use the IP addresses associated with individual users or user groups (usually from external auth servers).
dhcp	Use IP addresses obtained from external DHCP server.

Parameter	Description	Type	Size	Default
dhcp-ip-overlap	Configure overlapping DHCP IP allocation assignment.	option	-	use-new
	Option / **Description** *use-new* — Assign DHCP lease to new client and remove old client lease. *use-old* — Preserve previous client IP allocation and disconnect new client.			
auto-connect	Enable/disable automatic connect by client when system is up.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
keep-alive	Enable/disable automatic reconnect for FortiClient connections.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
save-password	Enable/disable FortiClient saving the user's password.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
ip-pools <name>	IPv4 firewall source address objects reserved for SSL-VPN tunnel mode clients. Address name.	string	Maximum length: 79	
exclusive-routing	Enable/disable all traffic go through tunnel only.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
service-restriction	Enable/disable tunnel service restriction.	option	-	disable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
split-tunneling	Enable/disable IPv4 split tunneling. **Option** **Description** *enable* Enable setting. *disable* Disable setting.	option	-	enable
split-tunneling-routing-negate	Enable to negate split tunneling routing address. **Option** **Description** *enable* Enable setting. *disable* Disable setting.	option	-	disable
split-tunneling-routing-address <name>	IPv4 SSL-VPN tunnel mode firewall address objects that override firewall policy destination addresses to control split-tunneling access. Address name.	string	Maximum length: 79	
dns-server1	IPv4 DNS server 1.	ipv4-address	Not Specified	0.0.0.0
dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified	0.0.0.0
dns-suffix	DNS suffix.	var-string	Maximum length: 253	
wins-server1	IPv4 WINS server 1.	ipv4-address	Not Specified	0.0.0.0
wins-server2	IPv4 WINS server 1.	ipv4-address	Not Specified	0.0.0.0
ipv6-tunnel-mode	Enable/disable IPv6 SSL-VPN tunnel mode. **Option** **Description** *enable* Enable setting. *disable* Disable setting.	option	-	disable
ipv6-pools <name>	IPv6 firewall source address objects reserved for SSL-VPN tunnel mode clients.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
	Address name.			
ipv6-exclusive-routing	Enable/disable all IPv6 traffic go through tunnel only.	option	-	disable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
ipv6-service-restriction	Enable/disable IPv6 tunnel service restriction.	option	-	disable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
ipv6-split-tunneling	Enable/disable IPv6 split tunneling.	option	-	enable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
ipv6-split-tunneling-routing-negate	Enable to negate IPv6 split tunneling routing address.	option	-	disable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
ipv6-split-tunneling-routing-address `<name>`	IPv6 SSL-VPN tunnel mode firewall address objects that override firewall policy destination addresses to control split-tunneling access. Address name.	string	Maximum length: 79	
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::
ipv6-wins-server1	IPv6 WINS server 1.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default
ipv6-wins-server2	IPv6 WINS server 2.	ipv6-address	Not Specified	::
web-mode	Enable/disable SSL-VPN web mode.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
display-bookmark	Enable to display the web portal bookmark widget.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
user-bookmark	Enable to allow web portal users to create their own bookmarks.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
allow-user-access	Allow user access to SSL-VPN applications.	option	-	web ftp smb sftp telnet ssh vnc rdp ping

Option	Description
web	HTTP/HTTPS access.
ftp	FTP access.
smb	SMB/CIFS access.
sftp	SFTP access.
telnet	TELNET access.
ssh	SSH access.
vnc	VNC access.
rdp	RDP access.
ping	PING access.

Parameter	Description	Type	Size	Default
user-group-bookmark	Enable to allow web portal users to create bookmarks for all users in the same user group.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
display-connection-tools	Enable to display the web portal connection tools widget.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
display-history	Enable to display the web portal user login history widget.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
display-status	Enable to display the web portal status widget.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
rewrite-ip-uri-ui	Rewrite contents for URI contains IP and /ui/ .	option	-	disable
	Option / **Description** *enable* — Enable contents rewrite for URI contains "IP-address/ui/". *disable* — Disable contents rewrite for URI contains "IP-address/ui/".			
heading	Web portal heading message.	string	Maximum length: 31	SSL-VPN Portal
redir-url	Client login redirect URL.	var-string	Maximum length: 255	
theme	Web portal color scheme.	option	-	neutrino

Parameter	Description	Type	Size	Default
	Option / **Description** *jade* — Jade theme. *neutrino* — Neutrino theme. *mariner* — Mariner theme. *graphite* — Graphite theme. *melongene* — Melongene theme. *dark-matter* — Dark Matter theme. *onyx* — Onyx theme. *eclipse* — Eclipse theme.			
custom-lang	Change the web portal display language. Overrides config system global set language. You can use config system custom-language and execute system custom-language to add custom language files.	string	Maximum length: 35	
smb-ntlmv1-auth	Enable support of NTLMv1 for Samba authentication.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
smbv1	SMB version 1.	option	-	disable
	Option / **Description** *enable* — enable *disable* — disable			
smb-min-version	SMB minimum client protocol version.	option	-	smbv2
	Option / **Description** *smbv1* — SMB version 1. *smbv2* — SMB version 2. *smbv3* — SMB version 3.			
smb-max-version	SMB maximum client protocol version.	option	-	smbv3

Parameter	Description	Type	Size	Default
	Option / **Description** *smbv1* / SMB version 1. *smbv2* / SMB version 2. *smbv3* / SMB version 3.			
use-sdwan	Use SD-WAN rules to get output interface. **Option** / **Description** *enable* / Enable setting. *disable* / Disable setting.	option	-	disable
prefer-ipv6-dns	Prefer to query IPv6 DNS server first if enabled. **Option** / **Description** *enable* / Enable setting. *disable* / Disable setting.	option	-	disable
clipboard	Enable to support RDP/VPC clipboard functionality. **Option** / **Description** *enable* / Enable support of RDP/VNC clipboard. *disable* / Disable support of RDP/VNC clipboard.	option	-	enable
default-window-width	Screen width .	integer	Minimum value: 0 Maximum value: 65535	1024
default-window-height	Screen height .	integer	Minimum value: 0 Maximum value: 65535	768
host-check	Type of host checking performed on endpoints. **Option** / **Description** *none* / No host checking. *av* / AntiVirus software recognized by the Windows Security Center.	option	-	none

Parameter	Description	Type	Size	Default
	Option / **Description** *fw* — Firewall software recognized by the Windows Security Center. *av-fw* — AntiVirus and firewall software recognized by the Windows Security Center. *custom* — Custom.			
host-check-interval	Periodic host check interval. Value of 0 means disabled and host checking only happens when the endpoint connects.	integer	Minimum value: 120 Maximum value: 259200	0
host-check-policy <name>	One or more policies to require the endpoint to have specific security software. Host check software list name.	string	Maximum length: 79	
limit-user-logins	Enable to limit each user to one SSL-VPN session at a time.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
mac-addr-check	Enable/disable MAC address host checking.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
mac-addr-action	Client MAC address action.	option	-	allow
	Option / **Description** *allow* — Allow connection when client MAC address is matched. *deny* — Deny connection when client MAC address is matched.			
os-check	Enable to let the FortiProxy decide action based on client OS.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			

Parameter	Description	Type	Size	Default
forticlient-download	Enable/disable download option for FortiClient.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
forticlient-download-method	FortiClient download method.	option	-	direct

Option	Description
direct	Download via direct link.
ssl-vpn	Download via SSL-VPN.

Parameter	Description	Type	Size	Default
customize-forticlient-download-url	Enable support of customized download URL for FortiClient.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
windows-forticlient-download-url	Download URL for Windows FortiClient.	var-string	Maximum length: 1023	
macos-forticlient-download-url	Download URL for Mac FortiClient.	var-string	Maximum length: 1023	
skip-check-for-unsupported-os	Enable to skip host check if client OS does not support it.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
skip-check-for-browser	Enable to skip host check for browser support.	option	-	enable

Option	Description
enable	Enable setting.

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* / Disable setting.			
hide-sso-credential	Enable to prevent SSO credential being sent to client.	option	-	enable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			

config bookmarks

Parameter	Description	Type	Size	Default
apptype	Application type.	option	-	web
	Option / **Description** *ftp* / FTP. *rdp* / RDP. *sftp* / SFTP. *smb* / SMB/CIFS. *ssh* / SSH. *telnet* / Telnet. *vnc* / VNC. *web* / HTTP/HTTPS.			
url	URL parameter.	var-string	Maximum length: 128	
host	Host name/IP parameter.	var-string	Maximum length: 128	
folder	Network shared file folder parameter.	var-string	Maximum length: 128	
domain	Login domain.	var-string	Maximum length: 128	
additional-params	Additional parameters.	var-string	Maximum length: 128	
description	Description.	var-string	Maximum length: 128	

Parameter	Description	Type	Size	Default
keyboard-layout	Keyboard layout.	option	-	en-us

Option	Description
ar-101	Arabic (101).
ar-102	Arabic (102).
ar-102-azerty	Arabic (102) AZERTY.
can-mul	Canadian Multilingual Standard.
cz	Czech.
cz-qwerty	Czech (QWERTY).
cz-pr	Czech Programmers.
da	Danish.
nl	Dutch.
de	German.
de-ch	German, Switzerland.
de-ibm	German (IBM).
en-uk	English, United Kingdom.
en-uk-ext	English, United Kingdom Extended.
en-us	English, United States.
en-us-dvorak	English, United States-Dvorak.
es	Spanish.
es-var	Spanish Variation.
fi	Finish.
fi-sami	Finnish with Sami.
fr	French.
fr-apple	French, Apple.
fr-ca	French, Canada.
fr-ch	French, Switzerland.
fr-be	French, Belgian.
hr	Croatian.
hu	Hungarian.
hu-101	Hungarian 101-Key.

Parameter	Description	Type	Size	Default

Option	Description
it	Italian.
it-142	Italian (142).
ja	Japanese.
ko	Korean.
lt	Lithuanian.
lt-ibm	Lithuanian IBM.
lt-std	Lithuanian Standard.
lav-std	Latvian (Standard).
lav-leg	Latvian (Legacy).
mk	Macedonian (FYROM).
mk-std	Macedonia (FYROM) - Standard.
no	Norwegian.
no-sami	Norwegian with Sami.
pol-214	Polish (214).
pol-pr	Polish (Programmers).
pt	Portuguese.
pt-br	Portuguese (Brazilian ABNT).
pt-br-abnt2	Portuguese (Brazilian ABNT2).
ru	Russian.
ru-mne	Russian - Mnemonic.
ru-t	Russian (Typewriter).
sl	Slovenian.
sv	Swedish.
sv-sami	Swedish with Sami.
tuk	Turkmen.
tur-f	Turkish F.
tur-q	Turkish Q.
zh-sym-sg-us	Chinese (Simplified, Singapore) - US keyboard.
zh-sym-us	Chinese (Simplified) - US Keyboard.

Parameter	Description	Type	Size	Default
	Option / **Description** *zh-tr-hk* — Chinese (Traditional, Hong Kong S.A.R.). *zh-tr-mo* — Chinese (Traditional Macao S.A.R.) - US Keyboard. *zh-tr-us* — Chinese (Traditional) - US keyboard.			
security	Security mode for RDP connection.	option	-	rdp
	Option / **Description** *rdp* — Standard RDP encryption. *nla* — Network Level Authentication. *tls* — TLS encryption. *any* — Allow the server to choose the type of security.			
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable
	Option / **Description** *enable* — Enable sending of preconnection ID. *disable* — Disable sending of preconnection ID.			
preconnection-id	The numeric ID of the RDP source .	integer	Minimum value: 0 Maximum value: 4294967295	0
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511	
load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511	
restricted-admin	Enable/disable restricted admin mode for RDP.	option	-	disable
	Option / **Description** *enable* — Enable restricted admin mode for RDP. *disable* — Disable restricted admin mode for RDP.			
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535	0

Parameter	Description	Type	Size	Default
logon-user	Logon user.	var-string	Maximum length: 35	
logon-password	Logon password.	password	Not Specified	
color-depth	Color depth per pixel.	option	-	16
	Option / **Description** *32* / 32bits per pixel. *16* / 16bits per pixel. *8* / 8bits per pixel.			
sso	Single Sign-On.	option	-	disable
	Option / **Description** *disable* / Disable SSO. *static* / Static SSO. *auto* / Auto SSO.			
sso-credential	Single sign-on credentials.	option	-	sslvpn-login
	Option / **Description** *sslvpn-login* / SSL-VPN login. *alternative* / Alternative.			
sso-username	SSO user name.	var-string	Maximum length: 35	
sso-password	SSO password.	password	Not Specified	
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-	disable
	Option / **Description** *enable* / Single sign-on credentials are only sent once to remote server. *disable* / Single sign-on credentials are sent to remote server for every HTTP request.			
width	Screen width .	integer	Minimum value: 0 Maximum value: 65535	0

Parameter	Description	Type	Size	Default
height	Screen height .	integer	Minimum value: 0 Maximum value: 65535	0

config form-data

Parameter	Description	Type	Size	Default
value	Value.	var-string	Maximum length: 63	

config mac-addr-check-rule

Parameter	Description	Type	Size	Default
mac-addr-mask	Client MAC address mask.	integer	Minimum value: 1 Maximum value: 48	48
mac-addr-list <addr>	Client MAC address list. Client MAC address.	mac-address	Not Specified	

config os-check-list

Parameter	Description	Type	Size	Default
action	OS check options.	option	-	allow

Option	Description
deny	Deny all OS versions.
allow	Allow any OS version.
check-up-to-date	Verify OS is up-to-date.

Parameter	Description	Type	Size	Default
tolerance	OS patch level tolerance.	integer	Minimum value: 0 Maximum value: 65535	0
latest-patch-level	Latest OS patch level.	user	Not Specified	0

config split-dns

Parameter	Description	Type	Size	Default
domains	Split DNS domains used for SSL-VPN clients separated by comma.	var-string	Maximum length: 1024	
dns-server1	DNS server 1.	ipv4-address	Not Specified	0.0.0.0
dns-server2	DNS server 2.	ipv4-address	Not Specified	0.0.0.0

config vpn ssl web realm

Realm.

```
config vpn ssl web realm
    Description: Realm.
    edit <url-path>
        set max-concurrent-user {integer}
        set login-page {var-string}
        set virtual-host {var-string}
        set virtual-host-only [enable|disable]
        set virtual-host-server-cert {string}
        set radius-server {string}
        set nas-ip {ipv4-address}
        set radius-port {integer}
    next
end
```

config vpn ssl web realm

Parameter	Description	Type	Size	Default
max-concurrent-user	Maximum concurrent users .	integer	Minimum value: 0 Maximum value: 65535	0
login-page	Replacement HTML for SSL-VPN login page.	var-string	Maximum length: 32768	
virtual-host	Virtual host name for realm.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default
virtual-host-only	Enable/disable enforcement of virtual host method for SSL-VPN client access. **Option** — **Description** *enable* — Enable setting. *disable* — Disable setting.	option	-	disable
virtual-host-server-cert	Name of the server certificate to used for this realm.	string	Maximum length: 35	
radius-server	RADIUS server associated with realm.	string	Maximum length: 35	
nas-ip	IP address used as a NAS-IP to communicate with the RADIUS server.	ipv4-address	Not Specified	0.0.0.0
radius-port	RADIUS service port number .	integer	Minimum value: 0 Maximum value: 65535	0

config vpn ssl web user-bookmark

Configure SSL-VPN user bookmark.

```
config vpn ssl web user-bookmark
    Description: Configure SSL-VPN user bookmark.
    edit <name>
        set custom-lang {string}
        config bookmarks
            Description: Bookmark table.
            edit <name>
                set apptype [ftp|rdp|...]
                set url {var-string}
                set host {var-string}
                set folder {var-string}
                set domain {var-string}
                set additional-params {var-string}
                set description {var-string}
                set keyboard-layout [ar-101|ar-102|...]
                set security [rdp|nla|...]
                set send-preconnection-id [enable|disable]
                set preconnection-id {integer}
                set preconnection-blob {var-string}
                set load-balancing-info {var-string}
                set restricted-admin [enable|disable]
                set port {integer}
                set logon-user {var-string}
```

```
                set logon-password {password}
                set color-depth [32|16|...]
                set sso [disable|static|...]
                config form-data
                    Description: Form data.
                    edit <name>
                        set value {var-string}
                    next
                end
                set sso-credential [sslvpn-login|alternative]
                set sso-username {var-string}
                set sso-password {password}
                set sso-credential-sent-once [enable|disable]
                set width {integer}
                set height {integer}
            next
        end
    next
end
```

config vpn ssl web user-bookmark

Parameter	Description	Type	Size	Default
custom-lang	Personal language.	string	Maximum length: 35	

config bookmarks

Parameter	Description	Type	Size	Default
apptype	Application type.	option	-	web

Option	Description
ftp	FTP.
rdp	RDP.
sftp	SFTP.
smb	SMB/CIFS.
ssh	SSH.
telnet	Telnet.
vnc	VNC.
web	HTTP/HTTPS.

url	URL parameter.	var-string	Maximum length: 128	

Parameter	Description	Type	Size	Default
host	Host name/IP parameter.	var-string	Maximum length: 128	
folder	Network shared file folder parameter.	var-string	Maximum length: 128	
domain	Login domain.	var-string	Maximum length: 128	
additional-params	Additional parameters.	var-string	Maximum length: 128	
description	Description.	var-string	Maximum length: 128	
keyboard-layout	Keyboard layout.	option	-	en-us

Option	Description
ar-101	Arabic (101).
ar-102	Arabic (102).
ar-102-azerty	Arabic (102) AZERTY.
can-mul	Canadian Multilingual Standard.
cz	Czech.
cz-qwerty	Czech (QWERTY).
cz-pr	Czech Programmers.
da	Danish.
nl	Dutch.
de	German.
de-ch	German, Switzerland.
de-ibm	German (IBM).
en-uk	English, United Kingdom.
en-uk-ext	English, United Kingdom Extended.
en-us	English, United States.
en-us-dvorak	English, United States-Dvorak.
es	Spanish.
es-var	Spanish Variation.
fi	Finish.

Parameter	Description	Type	Size	Default

Option	Description
fi-sami	Finnish with Sami.
fr	French.
fr-apple	French, Apple.
fr-ca	French, Canada.
fr-ch	French, Switzerland.
fr-be	French, Belgian.
hr	Croatian.
hu	Hungarian.
hu-101	Hungarian 101-Key.
it	Italian.
it-142	Italian (142).
ja	Japanese.
ko	Korean.
lt	Lithuanian.
lt-ibm	Lithuanian IBM.
lt-std	Lithuanian Standard.
lav-std	Latvian (Standard).
lav-leg	Latvian (Legacy).
mk	Macedonian (FYROM).
mk-std	Macedonia (FYROM) - Standard.
no	Norwegian.
no-sami	Norwegian with Sami.
pol-214	Polish (214).
pol-pr	Polish (Programmers).
pt	Portuguese.
pt-br	Portuguese (Brazilian ABNT).
pt-br-abnt2	Portuguese (Brazilian ABNT2).
ru	Russian.
ru-mne	Russian - Mnemonic.

Parameter	Description	Type	Size	Default
	Option / **Description** *ru-t* — Russian (Typewriter). *sl* — Slovenian. *sv* — Swedish. *sv-sami* — Swedish with Sami. *tuk* — Turkmen. *tur-f* — Turkish F. *tur-q* — Turkish Q. *zh-sym-sg-us* — Chinese (Simplified, Singapore) - US keyboard. *zh-sym-us* — Chinese (Simplified) - US Keyboard. *zh-tr-hk* — Chinese (Traditional, Hong Kong S.A.R.). *zh-tr-mo* — Chinese (Traditional Macao S.A.R.) - US Keyboard. *zh-tr-us* — Chinese (Traditional) - US keyboard.			
security	Security mode for RDP connection.	option	-	rdp
	Option / **Description** *rdp* — Standard RDP encryption. *nla* — Network Level Authentication. *tls* — TLS encryption. *any* — Allow the server to choose the type of security.			
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable
	Option / **Description** *enable* — Enable sending of preconnection ID. *disable* — Disable sending of preconnection ID.			
preconnection-id	The numeric ID of the RDP source .	integer	Minimum value: 0 Maximum value: 4294967295	0
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511	

Parameter	Description	Type	Size	Default
load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511	
restricted-admin	Enable/disable restricted admin mode for RDP.	option	-	disable

Option	Description
enable	Enable restricted admin mode for RDP.
disable	Disable restricted admin mode for RDP.

Parameter	Description	Type	Size	Default
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535	0
logon-user	Logon user.	var-string	Maximum length: 35	
logon-password	Logon password.	password	Not Specified	
color-depth	Color depth per pixel.	option	-	16

Option	Description
32	32bits per pixel.
16	16bits per pixel.
8	8bits per pixel.

Parameter	Description	Type	Size	Default
sso	Single Sign-On.	option	-	disable

Option	Description
disable	Disable SSO.
static	Static SSO.
auto	Auto SSO.

Parameter	Description	Type	Size	Default
sso-credential	Single sign-on credentials.	option	-	sslvpn-login

Option	Description
sslvpn-login	SSL-VPN login.
alternative	Alternative.

Parameter	Description	Type	Size	Default
sso-username	SSO user name.	var-string	Maximum length: 35	
sso-password	SSO password.	password	Not Specified	

Parameter	Description	Type	Size	Default
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-	disable
	Option / **Description** *enable* — Single sign-on credentials are only sent once to remote server. *disable* — Single sign-on credentials are sent to remote server for every HTTP request.			
width	Screen width .	integer	Minimum value: 0 Maximum value: 65535	0
height	Screen height .	integer	Minimum value: 0 Maximum value: 65535	0

config form-data

Parameter	Description	Type	Size	Default
value	Value.	var-string	Maximum length: 63	

config vpn ssl web user-group-bookmark

Configure SSL-VPN user group bookmark.

```
config vpn ssl web user-group-bookmark
    Description: Configure SSL-VPN user group bookmark.
    edit <name>
        config bookmarks
            Description: Bookmark table.
            edit <name>
                set apptype [ftp|rdp|...]
                set url {var-string}
                set host {var-string}
                set folder {var-string}
                set domain {var-string}
                set additional-params {var-string}
                set description {var-string}
                set keyboard-layout [ar-101|ar-102|...]
                set security [rdp|nla|...]
                set send-preconnection-id [enable|disable]
                set preconnection-id {integer}
                set preconnection-blob {var-string}
```

```
                set load-balancing-info {var-string}
                set restricted-admin [enable|disable]
                set port {integer}
                set logon-user {var-string}
                set logon-password {password}
                set color-depth [32|16|...]
                set sso [disable|static|...]
                config form-data
                    Description: Form data.
                    edit <name>
                        set value {var-string}
                    next
                end
                set sso-credential [sslvpn-login|alternative]
                set sso-username {var-string}
                set sso-password {password}
                set sso-credential-sent-once [enable|disable]
                set width {integer}
                set height {integer}
            next
        end
    next
end
```

config bookmarks

Parameter	Description	Type	Size	Default
apptype	Application type.	option	-	web

Option	Description
ftp	FTP.
rdp	RDP.
sftp	SFTP.
smb	SMB/CIFS.
ssh	SSH.
telnet	Telnet.
vnc	VNC.
web	HTTP/HTTPS.

url	URL parameter.	var-string	Maximum length: 128
host	Host name/IP parameter.	var-string	Maximum length: 128
folder	Network shared file folder parameter.	var-string	Maximum length: 128

Parameter	Description	Type	Size	Default
domain	Login domain.	var-string	Maximum length: 128	
additional-params	Additional parameters.	var-string	Maximum length: 128	
description	Description.	var-string	Maximum length: 128	
keyboard-layout	Keyboard layout.	option	-	en-us

Option	Description
ar-101	Arabic (101).
ar-102	Arabic (102).
ar-102-azerty	Arabic (102) AZERTY.
can-mul	Canadian Multilingual Standard.
cz	Czech.
cz-qwerty	Czech (QWERTY).
cz-pr	Czech Programmers.
da	Danish.
nl	Dutch.
de	German.
de-ch	German, Switzerland.
de-ibm	German (IBM).
en-uk	English, United Kingdom.
en-uk-ext	English, United Kingdom Extended.
en-us	English, United States.
en-us-dvorak	English, United States-Dvorak.
es	Spanish.
es-var	Spanish Variation.
fi	Finish.
fi-sami	Finnish with Sami.
fr	French.
fr-apple	French, Apple.
fr-ca	French, Canada.

Parameter	Description	Type	Size	Default

Option	Description
fr-ch	French, Switzerland.
fr-be	French, Belgian.
hr	Croatian.
hu	Hungarian.
hu-101	Hungarian 101-Key.
it	Italian.
it-142	Italian (142).
ja	Japanese.
ko	Korean.
lt	Lithuanian.
lt-ibm	Lithuanian IBM.
lt-std	Lithuanian Standard.
lav-std	Latvian (Standard).
lav-leg	Latvian (Legacy).
mk	Macedonian (FYROM).
mk-std	Macedonia (FYROM) - Standard.
no	Norwegian.
no-sami	Norwegian with Sami.
pol-214	Polish (214).
pol-pr	Polish (Programmers).
pt	Portuguese.
pt-br	Portuguese (Brazilian ABNT).
pt-br-abnt2	Portuguese (Brazilian ABNT2).
ru	Russian.
ru-mne	Russian - Mnemonic.
ru-t	Russian (Typewriter).
sl	Slovenian.
sv	Swedish.
sv-sami	Swedish with Sami.

Parameter	Description	Type	Size	Default
	Option / **Description** *tuk* — Turkmen. *tur-f* — Turkish F. *tur-q* — Turkish Q. *zh-sym-sg-us* — Chinese (Simplified, Singapore) - US keyboard. *zh-sym-us* — Chinese (Simplified) - US Keyboard. *zh-tr-hk* — Chinese (Traditional, Hong Kong S.A.R.). *zh-tr-mo* — Chinese (Traditional Macao S.A.R.) - US Keyboard. *zh-tr-us* — Chinese (Traditional) - US keyboard.			
security	Security mode for RDP connection.	option	-	rdp
	Option / **Description** *rdp* — Standard RDP encryption. *nla* — Network Level Authentication. *tls* — TLS encryption. *any* — Allow the server to choose the type of security.			
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable
	Option / **Description** *enable* — Enable sending of preconnection ID. *disable* — Disable sending of preconnection ID.			
preconnection-id	The numeric ID of the RDP source .	integer	Minimum value: 0 Maximum value: 4294967295	0
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511	
load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511	
restricted-admin	Enable/disable restricted admin mode for RDP.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable restricted admin mode for RDP. *disable* — Disable restricted admin mode for RDP.			
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535	0
logon-user	Logon user.	var-string	Maximum length: 35	
logon-password	Logon password.	password	Not Specified	
color-depth	Color depth per pixel.	option	-	16
	Option / **Description** *32* — 32bits per pixel. *16* — 16bits per pixel. *8* — 8bits per pixel.			
sso	Single Sign-On.	option	-	disable
	Option / **Description** *disable* — Disable SSO. *static* — Static SSO. *auto* — Auto SSO.			
sso-credential	Single sign-on credentials.	option	-	sslvpn-login
	Option / **Description** *sslvpn-login* — SSL-VPN login. *alternative* — Alternative.			
sso-username	SSO user name.	var-string	Maximum length: 35	
sso-password	SSO password.	password	Not Specified	
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Single sign-on credentials are only sent once to remote server. *disable* / Single sign-on credentials are sent to remote server for every HTTP request.			
width	Screen width .	integer	Minimum value: 0 Maximum value: 65535	0
height	Screen height .	integer	Minimum value: 0 Maximum value: 65535	0

config form-data

Parameter	Description	Type	Size	Default
value	Value.	var-string	Maximum length: 63	

waf

This section includes syntax for the following commands:

config waf main-class

Hidden table for datasource.

```
config waf main-class
    Description: Hidden table for datasource.
    edit <id>
        set name {string}
    next
end
```

config waf main-class

Parameter	Description	Type	Size	Default
name	Main signature class name.	string	Maximum length: 127	

config waf profile

Configure Web application firewall configuration.

```
config waf profile
    Description: Configure Web application firewall configuration.
    edit <name>
        set external [disable|enable]
        set extended-log [enable|disable]
        config signature
            Description: WAF signatures.
            config main-class
                Description: Main signature class.
                edit <id>
                    set status [enable|disable]
                    set action [allow|block|...]
```

```
                    set log [enable|disable]
                    set severity [high|medium|...]
                next
            end
            set disabled-sub-class <id1>, <id2>, ...
            set disabled-signature <id1>, <id2>, ...
            set credit-card-detection-threshold {integer}
            config custom-signature
                Description: Custom signature.
                edit <name>
                    set status [enable|disable]
                    set action [allow|block|...]
                    set log [enable|disable]
                    set severity [high|medium|...]
                    set direction [request|response]
                    set case-sensitivity [disable|enable]
                    set pattern {string}
                    set target {option1}, {option2}, ...
                next
            end
        end
        config constraint
            Description: WAF HTTP protocol restrictions.
            config header-length
                Description: HTTP header length in request.
                set status [enable|disable]
                set length {integer}
                set action [allow|block]
                set log [enable|disable]
                set severity [high|medium|...]
            end
            config content-length
                Description: HTTP content length in request.
                set status [enable|disable]
                set length {integer}
                set action [allow|block]
                set log [enable|disable]
                set severity [high|medium|...]
            end
            config param-length
                Description: Maximum length of parameter in URL, HTTP POST request or HTTP
body.
                set status [enable|disable]
                set length {integer}
                set action [allow|block]
                set log [enable|disable]
                set severity [high|medium|...]
            end
            config line-length
                Description: HTTP line length in request.
                set status [enable|disable]
                set length {integer}
                set action [allow|block]
                set log [enable|disable]
                set severity [high|medium|...]
            end
```

```
            config url-param-length
                Description: Maximum length of parameter in URL.
                set status [enable|disable]
                set length {integer}
                set action [allow|block]
                set log [enable|disable]
                set severity [high|medium|...]
            end
            config version
                Description: Enable/disable HTTP version check.
                set status [enable|disable]
                set action [allow|block]
                set log [enable|disable]
                set severity [high|medium|...]
            end
            config method
                Description: Enable/disable HTTP method check.
                set status [enable|disable]
                set action [allow|block]
                set log [enable|disable]
                set severity [high|medium|...]
            end
            config hostname
                Description: Enable/disable hostname check.
                set status [enable|disable]
                set action [allow|block]
                set log [enable|disable]
                set severity [high|medium|...]
            end
            config malformed
                Description: Enable/disable malformed HTTP request check.
                set status [enable|disable]
                set action [allow|block]
                set log [enable|disable]
                set severity [high|medium|...]
            end
            config max-cookie
                Description: Maximum number of cookies in HTTP request.
                set status [enable|disable]
                set max-cookie {integer}
                set action [allow|block]
                set log [enable|disable]
                set severity [high|medium|...]
            end
            config max-header-line
                Description: Maximum number of HTTP header line.
                set status [enable|disable]
                set max-header-line {integer}
                set action [allow|block]
                set log [enable|disable]
                set severity [high|medium|...]
            end
            config max-url-param
                Description: Maximum number of parameters in URL.
                set status [enable|disable]
                set max-url-param {integer}
```

```
            set action [allow|block]
            set log [enable|disable]
            set severity [high|medium|...]
        end
        config max-range-segment
            Description: Maximum number of range segments in HTTP range line.
            set status [enable|disable]
            set max-range-segment {integer}
            set action [allow|block]
            set log [enable|disable]
            set severity [high|medium|...]
        end
        config exception
            Description: HTTP constraint exception.
            edit <id>
                set pattern {string}
                set regex [enable|disable]
                set address {string}
                set header-length [enable|disable]
                set content-length [enable|disable]
                set param-length [enable|disable]
                set line-length [enable|disable]
                set url-param-length [enable|disable]
                set version [enable|disable]
                set method [enable|disable]
                set hostname [enable|disable]
                set malformed [enable|disable]
                set max-cookie [enable|disable]
                set max-header-line [enable|disable]
                set max-url-param [enable|disable]
                set max-range-segment [enable|disable]
            next
        end
    end
    config method
        Description: Method restriction.
        set status [enable|disable]
        set log [enable|disable]
        set severity [high|medium|...]
        set default-allowed-methods {option1}, {option2}, ...
        config method-policy
            Description: HTTP method policy.
            edit <id>
                set pattern {string}
                set regex [enable|disable]
                set address {string}
                set allowed-methods {option1}, {option2}, ...
            next
        end
    end
    config address-list
        Description: Address block and allow lists.
        set status [enable|disable]
        set blocked-log [enable|disable]
        set severity [high|medium|...]
        set trusted-address <name1>, <name2>, ...
```

```
            set blocked-address <name1>, <name2>, ...
        end
        config url-access
            Description: URL access list.
            edit <id>
                set address {string}
                set action [bypass|permit|...]
                set log [enable|disable]
                set severity [high|medium|...]
                config access-pattern
                    Description: URL access pattern.
                    edit <id>
                        set srcaddr {string}
                        set pattern {string}
                        set regex [enable|disable]
                        set negate [enable|disable]
                    next
                end
            next
        end
        set comment {var-string}
    next
end
```

config waf profile

Parameter	Description	Type	Size	Default
external	Disable/Enable external HTTP Inspection.	option	-	disable
	Option / **Description** *disable* — Disable external inspection. *enable* — Enable external inspection.			
extended-log	Enable/disable extended logging.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
comment	Comment.	var-string	Maximum length: 1023	

config signature

Parameter	Description	Type	Size	Default
disabled-sub-class <id>	Disabled signature subclasses. Signature subclass ID.	integer	Minimum value: 0 Maximum value: 4294967295	
disabled-signature <id>	Disabled signatures. Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295	
credit-card-detection-threshold	The minimum number of Credit cards to detect violation.	integer	Minimum value: 0 Maximum value: 128	3

config main-class

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
action	Action.	option	-	allow
	Option / **Description** *allow* — Allow. *block* — Block. *erase* — Erase credit card numbers.			
log	Enable/disable logging.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
severity	Severity.	option	-	medium

Parameter	Description	Type	Size	Default
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.			

config custom-signature

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
action	Action.	option	-	allow
	Option **Description** *allow* Allow. *block* Block. *erase* Erase credit card numbers.			
log	Enable/disable logging.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
severity	Severity.	option	-	medium
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.			
direction	Traffic direction.	option	-	request
	Option **Description** *request* Match HTTP request.			

Parameter	Description	Type	Size	Default
	Option / **Description** *response* — Match HTTP response.			
case-sensitivity	Case sensitivity in pattern.	option	-	disable
	Option / **Description** *disable* — Case insensitive in pattern. *enable* — Case sensitive in pattern.			
pattern	Match pattern.	string	Maximum length: 511	
target	Match HTTP target.	option	-	
	Option / **Description** *arg* — HTTP arguments. *arg-name* — Names of HTTP arguments. *req-body* — HTTP request body. *req-cookie* — HTTP request cookies. *req-cookie-name* — HTTP request cookie names. *req-filename* — HTTP request file name. *req-header* — HTTP request headers. *req-header-name* — HTTP request header names. *req-raw-uri* — Raw URI of HTTP request. *req-uri* — URI of HTTP request. *resp-body* — HTTP response body. *resp-hdr* — HTTP response headers. *resp-status* — HTTP response status.			

config header-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
length	Length of HTTP header in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192
action	Action.	option	-	allow
	Option / **Description** *allow* — Allow. *block* — Block.			
log	Enable/disable logging.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
severity	Severity.	option	-	medium
	Option / **Description** *high* — High severity. *medium* — Medium severity. *low* — Low severity.			

config content-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			

Parameter	Description	Type	Size	Default
length	Length of HTTP content in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	67108864
action	Action.	option	-	allow
	Option / **Description** *allow* — Allow. *block* — Block.			
log	Enable/disable logging.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
severity	Severity.	option	-	medium
	Option / **Description** *high* — High severity. *medium* — Medium severity. *low* — Low severity.			

config param-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
length	Maximum length of parameter in URL, HTTP POST request or HTTP body in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192
action	Action.	option	-	allow

Parameter	Description	Type	Size	Default
	Option **Description** *allow* Allow. *block* Block.			
log	Enable/disable logging.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
severity	Severity.	option	-	medium
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.			

config line-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
length	Length of HTTP line in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	1024
action	Action.	option	-	allow
	Option **Description** *allow* Allow. *block* Block.			
log	Enable/disable logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
severity	Severity.	option	-	medium
	Option / **Description** *high* / High severity. *medium* / Medium severity. *low* / Low severity.			

config url-param-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
length	Maximum length of URL parameter in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192
action	Action.	option	-	allow
	Option / **Description** *allow* / Allow. *block* / Block.			
log	Enable/disable logging.	option	-	disable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
severity	Severity.	option	-	medium

Parameter	Description	Type	Size	Default
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.			

config version

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
action	Action.	option	-	allow
	Option **Description** *allow* Allow. *block* Block.			
log	Enable/disable logging.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
severity	Severity.	option	-	medium
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.			

config method

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
action	Action.	option	-	allow
	Option / **Description** *allow* — Allow. *block* — Block.			
log	Enable/disable logging.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
severity	Severity.	option	-	medium
	Option / **Description** *high* — High severity. *medium* — Medium severity. *low* — Low severity.			

config method

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
log	Enable/disable logging.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
severity	Severity.	option	-	medium

Parameter	Description	Type	Size	Default
	Option / **Description** *high* — High severity *medium* — medium severity *low* — low severity			
default-allowed-methods	Methods.	option	-	
	Option / **Description** *get* — HTTP GET method. *post* — HTTP POST method. *put* — HTTP PUT method. *head* — HTTP HEAD method. *connect* — HTTP CONNECT method. *trace* — HTTP TRACE method. *options* — HTTP OPTIONS method. *delete* — HTTP DELETE method. *others* — Other HTTP methods.			

config hostname

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
action	Action.	option	-	allow
	Option / **Description** *allow* — Allow. *block* — Block.			
log	Enable/disable logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
severity	Severity.	option	-	medium
	Option / **Description** *high* — High severity. *medium* — Medium severity. *low* — Low severity.			

config malformed

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
action	Action.	option	-	allow
	Option / **Description** *allow* — Allow. *block* — Block.			
log	Enable/disable logging.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
severity	Severity.	option	-	medium
	Option / **Description** *high* — High severity. *medium* — Medium severity. *low* — Low severity.			

config max-cookie

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
max-cookie	Maximum number of cookies in HTTP request (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	16
action	Action.	option	-	allow
	Option / **Description** *allow* — Allow. *block* — Block.			
log	Enable/disable logging.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
severity	Severity.	option	-	medium
	Option / **Description** *high* — High severity. *medium* — Medium severity. *low* — Low severity.			

config max-header-line

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			

Parameter	Description	Type	Size	Default
max-header-line	Maximum number HTTP header lines (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	32
action	Action.	option	-	allow
	Option / **Description** *allow* — Allow. *block* — Block.			
log	Enable/disable logging.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
severity	Severity.	option	-	medium
	Option / **Description** *high* — High severity. *medium* — Medium severity. *low* — Low severity.			

config max-url-param

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
max-url-param	Maximum number of parameters in URL (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	16
action	Action.	option	-	allow

Parameter	Description	Type	Size	Default
	Option **Description** *allow* Allow. *block* Block.			
log	Enable/disable logging.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
severity	Severity.	option	-	medium
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.			

config max-range-segment

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
max-range-segment	Maximum number of range segments in HTTP range line (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	5
action	Action.	option	-	allow
	Option **Description** *allow* Allow. *block* Block.			
log	Enable/disable logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
severity	Severity.	option	-	medium
	Option / **Description** *high* — High severity. *medium* — Medium severity. *low* — Low severity.			

config exception

Parameter	Description	Type	Size	Default
pattern	URL pattern.	string	Maximum length: 511	
regex	Enable/disable regular expression based pattern match.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
address	Host address.	string	Maximum length: 79	
header-length	HTTP header length in request.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
content-length	HTTP content length in request.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
param-length	Maximum length of parameter in URL, HTTP POST request or HTTP body.	option	-	disable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
line-length	HTTP line length in request.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
url-param-length	Maximum length of parameter in URL.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
version	Enable/disable HTTP version check.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
method	Enable/disable HTTP method check.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
hostname	Enable/disable hostname check.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
malformed	Enable/disable malformed HTTP request check.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			

Parameter	Description	Type	Size	Default
max-cookie	Maximum number of cookies in HTTP request.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
max-header-line	Maximum number of HTTP header line.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
max-url-param	Maximum number of parameters in URL.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
max-range-segment	Maximum number of range segments in HTTP range line.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

config method

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
action	Action.	option	-	allow
log	Enable/disable logging.	option	-	disable
severity	Severity.	option	-	medium

config method

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
log	Enable/disable logging.	option	-	disable
severity	Severity.	option	-	medium
default-allowed-methods	Methods.	option	-	

config method-policy

Parameter	Description	Type	Size	Default
pattern	URL pattern.	string	Maximum length: 511	
regex	Enable/disable regular expression based pattern match.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
address	Host address.	string	Maximum length: 79	
allowed-methods	Allowed Methods.	option	-	

Option	Description
get	HTTP GET method.
post	HTTP POST method.
put	HTTP PUT method.
head	HTTP HEAD method.
connect	HTTP CONNECT method.
trace	HTTP TRACE method.
options	HTTP OPTIONS method.
delete	HTTP DELETE method.
others	Other HTTP methods.

config address-list

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
blocked-log	Enable/disable logging on blocked addresses.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
severity	Severity.	option	-	medium
	Option / **Description** *high* — High severity. *medium* — Medium severity. *low* — Low severity.			
trusted-address <name>	Trusted address. Address name.	string	Maximum length: 79	
blocked-address <name>	Blocked address. Address name.	string	Maximum length: 79	

config url-access

Parameter	Description	Type	Size	Default
address	Host address.	string	Maximum length: 79	
action	Action.	option	-	permit
	Option / **Description** *bypass* — Allow the HTTP request, also bypass further WAF scanning. *permit* — Allow the HTTP request, and continue further WAF scanning. *block* — Block HTTP request.			

Parameter	Description	Type	Size	Default
log	Enable/disable logging.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
severity	Severity.	option	-	medium
	Option / **Description** *high* — High severity. *medium* — Medium severity. *low* — Low severity.			

config access-pattern

Parameter	Description	Type	Size	Default
srcaddr	Source address.	string	Maximum length: 79	
pattern	URL pattern.	string	Maximum length: 511	
regex	Enable/disable regular expression based pattern match.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
negate	Enable/disable match negation.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			

config waf signature

Hidden table for datasource.

```
config waf signature
    Description: Hidden table for datasource.
    edit <id>
```

```
        set desc {string}
    next
end
```

config waf signature

Parameter	Description	Type	Size	Default
desc	Signature description.	string	Maximum length: 511	

config waf sub-class

Hidden table for datasource.

```
config waf sub-class
    Description: Hidden table for datasource.
    edit <id>
        set name {string}
    next
end
```

config waf sub-class

Parameter	Description	Type	Size	Default
name	Signature subclass name.	string	Maximum length: 127	

wanopt

This section includes syntax for the following commands:

config wanopt auth-group

Configure WAN optimization authentication groups.

```
config wanopt auth-group
    Description: Configure WAN optimization authentication groups.
    edit <name>
        set auth-method [cert|psk]
        set psk {password}
        set cert {string}
        set peer-accept [any|defined|...]
        set peer {string}
    next
end
```

config wanopt auth-group

Parameter	Description	Type	Size	Default
auth-method	Select certificate or pre-shared key authentication for this authentication group.	option	-	cert
	Option / **Description** *cert* — Certificate authentication. *psk* — Pre-shared secret key authentication.			
psk	Pre-shared key used by the peers in this authentication group.	password	Not Specified	
cert	Name of certificate to identify this peer.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
peer-accept	Determine if this auth group accepts, any peer, a list of defined peers, or just one peer.	option	-	any

Option	Description
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.

peer	If peer-accept is set to one, select the name of one peer to add to this authentication group. The peer must have added with the wanopt peer command.	string	Maximum length: 35	

config wanopt cache-service

Designate cache-service for wan-optimization and webcache.

```
config wanopt cache-service
    Description: Designate cache-service for wan-optimization and webcache.
    set prefer-scenario [balance|prefer-speed|...]
    set collaboration [enable|disable]
    set device-id {string}
    set acceptable-connections [any|peers]
    config dst-peer
        Description: Modify cache-service destination peer list.
        edit <device-id>
            set auth-type {integer}
            set encode-type {integer}
            set priority {integer}
            set ip {ipv4-address-any}
        next
    end
    config src-peer
        Description: Modify cache-service source peer list.
        edit <device-id>
            set auth-type {integer}
            set encode-type {integer}
            set priority {integer}
            set ip {ipv4-address-any}
        next
    end
end
```

config wanopt cache-service

Parameter	Description	Type	Size	Default
prefer-scenario	Set the preferred cache behavior towards the balance between latency and hit-ratio.	option	-	prefer-speed
	Option / **Description** *balance* — Balance between speed and cache hit ratio. *prefer-speed* — Prefer response speed at the expense of increased cache bypasses. *prefer-cache* — Prefer improving hit-ratio through increasing latency tolerance.			
collaboration	Enable/disable cache-collaboration between cache-service clusters.	option	-	disable
	Option / **Description** *enable* — Enable cache cache-collaboration. *disable* — Disable cache cache-collaboration.			
device-id	Set identifier for this cache device.	string	Maximum length: 35	default_dev_id
acceptable-connections	Set strategy when accepting cache collaboration connection.	option	-	any
	Option / **Description** *any* — We can accept any cache-collaboration connection. *peers* — We can only accept connections that are already in src-peers.			

config dst-peer

Parameter	Description	Type	Size	Default
auth-type	Set authentication type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
encode-type	Set encode type for this peer.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default
priority	Set priority for this peer.	integer	Minimum value: 0 Maximum value: 255	1
ip	Set cluster IP address of this peer.	ipv4-address-any	Not Specified	0.0.0.0

config src-peer

Parameter	Description	Type	Size	Default
auth-type	Set authentication type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
encode-type	Set encode type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
priority	Set priority for this peer.	integer	Minimum value: 0 Maximum value: 255	1
ip	Set cluster IP address of this peer.	ipv4-address-any	Not Specified	0.0.0.0

config wanopt content-delivery-network-rule

Configure WAN optimization content delivery network rules.

```
config wanopt content-delivery-network-rule
    Description: Configure WAN optimization content delivery network rules.
    edit <name>
        set comment {var-string}
        set status [enable|disable]
        set host-domain-name-suffix <name1>, <name2>, ...
        set category [vcache|youtube]
        set request-cache-control [enable|disable]
        set response-cache-control [enable|disable]
        set response-expires [enable|disable]
        set updateserver [enable|disable]
        config rules
```

```
            Description: WAN optimization content delivery network rule entries.
            edit <name>
                set match-mode [all|any]
                set skip-rule-mode [all|any]
                config match-entries
                    Description: List of entries to match.
                    edit <id>
                        set target [path|parameter|...]
                        set pattern <string1>, <string2>, ...
                    next
                end
                config skip-entries
                    Description: List of entries to skip.
                    edit <id>
                        set target [path|parameter|...]
                        set pattern <string1>, <string2>, ...
                    next
                end
                config content-id
                    Description: Content ID settings.
                    set target [path|parameter|...]
                    set start-str {string}
                    set start-skip {integer}
                    set start-direction [forward|backward]
                    set end-str {string}
                    set end-skip {integer}
                    set end-direction [forward|backward]
                    set range-str {string}
                end
            next
        end
    next
end
```

config wanopt content-delivery-network-rule

Parameter	Description	Type	Size	Default
comment	Comment about this CDN-rule.	var-string	Maximum length: 255	
status	Enable/disable WAN optimization content delivery network rules.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
host-domain-name-suffix <name>	Suffix portion of the fully qualified domain name. For example, fortinet.com in "www.fortinet.com". Suffix portion of the fully qualified domain name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
category	Content delivery network rule category.	option	-	vcache

Option	Description
vcache	Vcache content delivery network.
youtube	Youtube content delivery network.

Parameter	Description	Type	Size	Default
request-cache-control	Enable/disable HTTP request cache control.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
response-cache-control	Enable/disable HTTP response cache control.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
response-expires	Enable/disable HTTP response cache expires.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
updateserver	Enable/disable update server.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

config rules

Parameter	Description	Type	Size	Default
match-mode	Match criteria for collecting content ID.	option	-	all

Parameter	Description	Type	Size	Default
	Option / **Description** *all* — Must match all of the match entries. *any* — Must match any of the match entries.			
skip-rule-mode	Skip mode when evaluating skip-rules.	option	-	all
	Option / **Description** *all* — Must match all skip entries. *any* — Must match any skip entries.			

config match-entries

Parameter	Description	Type	Size	Default
target	Option in HTTP header or URL parameter to match.	option	-	path
	Option / **Description** *path* — Match with the URL path. *parameter* — Match with the URL parameters. *referrer* — Match with the Referrer option in HTTP header. *youtube-map* — Match Youtube content-id collection. *youtube-id* — Match Youtube content-id. *youku-id* — Match Youku content-id.			
pattern `<string>`	Pattern string for matching target (Referrer or URL pattern). For example, a, a*c, *a*, a*c*e, and *. Pattern strings.	string	Maximum length: 79	

config skip-entries

Parameter	Description	Type	Size	Default
target	Option in HTTP header or URL parameter to match.	option	-	path
	Option / **Description** *path* — Match with the URL path. *parameter* — Match with the URL parameters. *referrer* — Match with the Referrer option in HTTP header.			

Parameter	Description	Type	Size	Default
	Option / **Description** *youtube-map* / Match Youtube content-id collection. *youtube-id* / Match Youtube content-id. *youku-id* / Match Youku content-id.			
pattern <string>	Pattern string for matching target (Referrer or URL pattern). For example, a, a*c, *a*, a*c*e, and *. Pattern strings.	string	Maximum length: 79	

config content-id

Parameter	Description	Type	Size	Default
target	Option in HTTP header or URL parameter to match.	option	-	path
	Option / **Description** *path* / Match with the URL path. *parameter* / Match with the URL parameters. *referrer* / Match with the Referrer option in HTTP header. *youtube-map* / Match Youtube content-id collection. *youtube-id* / Match Youtube content-id. *youku-id* / Match Youku content-id. *hls-manifest* / Match with HLS manifest. *dash-manifest* / Match with DASH manifest. *hls-fragment* / Match HLS stream fragment. *dash-fragment* / Match DASH stream fragment.			
start-str	String from which to start search.	string	Maximum length: 35	
start-skip	Number of characters in URL to skip after start-str has been matched.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-direction	Search direction from start-str match.	option	-	forward

Parameter	Description	Type	Size	Default
	Option / **Description** *forward* / Forward direction. *backward* / Backward direction.			
end-str	String from which to end search.	string	Maximum length: 35	
end-skip	Number of characters in URL to skip after end-str has been matched.	integer	Minimum value: 0 Maximum value: 4294967295	0
end-direction	Search direction from end-str match.	option	-	forward
	Option / **Description** *forward* / Forward direction. *backward* / Backward direction.			
range-str	Name of content ID within the start string and end string.	string	Maximum length: 35	

config wanopt peer

Configure WAN optimization peers.

```
config wanopt peer
    Description: Configure WAN optimization peers.
    edit <peer-host-id>
        set ip {ipv4-address-any}
    next
end
```

config wanopt peer

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

config wanopt profile

Configure WAN optimization profiles.

```
config wanopt profile
    Description: Configure WAN optimization profiles.
    edit <name>
        set transparent [enable|disable]
        set comments {var-string}
        set auth-group {string}
        config http
            Description: Enable/disable HTTP WAN Optimization and configure HTTP WAN
Optimization features.
            set status [enable|disable]
            set secure-tunnel [enable|disable]
            set byte-caching [enable|disable]
            set ssl [enable|disable]
            set prefer-chunking [dynamic|fix]
            set protocol-opt [protocol|tcp]
            set tunnel-sharing [shared|express-shared|...]
            set log-traffic [enable|disable]
        end
        config cifs
            Description: Enable/disable CIFS (Windows sharing) WAN Optimization and
configure CIFS WAN Optimization features.
            set status [enable|disable]
            set secure-tunnel [enable|disable]
            set byte-caching [enable|disable]
            set prefer-chunking [dynamic|fix]
            set protocol-opt [protocol|tcp]
            set tunnel-sharing [shared|express-shared|...]
            set log-traffic [enable|disable]
        end
        config mapi
            Description: Enable/disable MAPI email WAN Optimization and configure MAPI WAN
Optimization features.
            set status [enable|disable]
            set secure-tunnel [enable|disable]
            set byte-caching [enable|disable]
            set tunnel-sharing [shared|express-shared|...]
            set log-traffic [enable|disable]
        end
        config ftp
            Description: Enable/disable FTP WAN Optimization and configure FTP WAN
Optimization features.
            set status [enable|disable]
            set secure-tunnel [enable|disable]
            set byte-caching [enable|disable]
            set ssl [enable|disable]
            set prefer-chunking [dynamic|fix]
            set protocol-opt [protocol|tcp]
            set tunnel-sharing [shared|express-shared|...]
            set log-traffic [enable|disable]
        end
        config tcp
```

```
            Description: Enable/disable TCP WAN Optimization and configure TCP WAN
Optimization features.
            set status [enable|disable]
            set secure-tunnel [enable|disable]
            set byte-caching [enable|disable]
            set byte-caching-opt [mem-only|mem-disk]
            set tunnel-sharing [shared|express-shared|...]
            set log-traffic [enable|disable]
            set port {user}
            set ssl [enable|disable]
            set ssl-port {user}
        end
    next
end
```

config wanopt profile

Parameter	Description	Type	Size	Default
transparent	Enable/disable transparent mode.	option	-	enable

Option	Description
enable	Determine if WAN Optimization changes client packet source addresses. Affects the routing configuration on the server network.
disable	Disable transparent mode. Client packets source addresses are changed to the source address of the FortiProxy internal interface. Similar to source NAT.

comments	Comment.	var-string	Maximum length: 255	
auth-group	Optionally add an authentication group to restrict access to the WAN Optimization tunnel to peers in the authentication group.	string	Maximum length: 35	

config http

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization.	option	-	disable

Option	Description
enable	Enable WAN Optimization.
disable	Disable WAN Optimization.

secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable SSL-secured tunnelling. *disable* — Disable SSL-secured tunnelling.			
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	enable
	Option / **Description** *enable* — Enable byte-caching. *disable* — Disable byte-caching.			
ssl	Enable/disable SSL/TLS offloading (hardware acceleration) for traffic in this tunnel.	option	-	disable
	Option / **Description** *enable* — Enable SSL/TLS offloading. *disable* — Disable SSL/TLS offloading.			
prefer-chunking	Select dynamic or fixed-size data chunking for WAN Optimization.	option	-	fix
	Option / **Description** *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.			
protocol-opt	Select protocol specific optimization or generic TCP optimization.	option	-	protocol
	Option / **Description** *protocol* — Using protocol-specific optimization. *tcp* — Using generic TCP optimization.			
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private
	Option / **Description** *shared* — For profiles that accept nonaggressive and non-interactive protocols. *express-shared* — For profiles that accept interactive protocols such as Telnet.			

Parameter	Description	Type	Size	Default
	Option / **Description** *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.			
log-traffic	Enable/disable logging. **Option** / **Description** *enable* — Enable logging. *disable* — Disable logging.	option	-	enable

config cifs

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization. **Option** / **Description** *enable* — Enable WAN Optimization. *disable* — Disable WAN Optimization.	option	-	disable
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810). **Option** / **Description** *enable* — Enable SSL-secured tunnelling. *disable* — Disable SSL-secured tunnelling.	option	-	disable
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache. **Option** / **Description** *enable* — Enable byte-caching. *disable* — Disable byte-caching.	option	-	enable
prefer-chunking	Select dynamic or fixed-size data chunking for WAN Optimization.	option	-	fix

Parameter	Description	Type	Size	Default
	Option / **Description** *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.			
protocol-opt	Select protocol specific optimization or generic TCP optimization.	option	-	protocol
	Option / **Description** *protocol* — Using protocol-specific optimization. *tcp* — Using generic TCP optimization.			
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private
	Option / **Description** *shared* — For profiles that accept nonaggressive and non-interactive protocols. *express-shared* — For profiles that accept interactive protocols such as Telnet. *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.			
log-traffic	Enable/disable logging.	option	-	enable
	Option / **Description** *enable* — Enable logging. *disable* — Disable logging.			

config mapi

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization.	option	-	disable
	Option / **Description** *enable* — Enable WAN Optimization. *disable* — Disable WAN Optimization.			

Parameter	Description	Type	Size	Default
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable

Option	Description
enable	Enable SSL-secured tunnelling.
disable	Disable SSL-secured tunnelling.

Parameter	Description	Type	Size	Default
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	enable

Option	Description
enable	Enable byte-caching.
disable	Disable byte-caching.

Parameter	Description	Type	Size	Default
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private

Option	Description
shared	For profiles that accept nonaggressive and non-interactive protocols.
express-shared	For profiles that accept interactive protocols such as Telnet.
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.

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

Option	Description
enable	Enable logging.
disable	Disable logging.

config ftp

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization.	option	-	disable

Option	Description
enable	Enable WAN Optimization.
disable	Disable WAN Optimization.

Parameter	Description	Type	Size	Default
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable

Option	Description
enable	Enable SSL-secured tunnelling.
disable	Disable SSL-secured tunnelling.

Parameter	Description	Type	Size	Default
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	enable

Option	Description
enable	Enable byte-caching.
disable	Disable byte-caching.

Parameter	Description	Type	Size	Default
ssl	Enable/disable SSL/TLS offloading (hardware acceleration) for traffic in this tunnel.	option	-	disable

Option	Description
enable	Enable SSL/TLS offloading.
disable	Disable SSL/TLS offloading.

Parameter	Description	Type	Size	Default
prefer-chunking	Select dynamic or fixed-size data chunking for WAN Optimization.	option	-	fix

Option	Description
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.

Parameter	Description	Type	Size	Default
protocol-opt	Select protocol specific optimization or generic TCP optimization.	option	-	protocol

Option	Description
protocol	Using protocol-specific optimization.
tcp	Using generic TCP optimization.

Parameter	Description	Type	Size	Default
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private

Parameter	Description	Type	Size	Default
	Option / **Description** *shared* — For profiles that accept nonaggressive and non-interactive protocols. *express-shared* — For profiles that accept interactive protocols such as Telnet. *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.			
log-traffic	Enable/disable logging.	option	-	enable
	Option / **Description** *enable* — Enable logging. *disable* — Disable logging.			

config tcp

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization.	option	-	disable
	Option / **Description** *enable* — Enable WAN Optimization. *disable* — Disable WAN Optimization.			
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable
	Option / **Description** *enable* — Enable SSL-secured tunnelling. *disable* — Disable SSL-secured tunnelling.			
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	disable
	Option / **Description** *enable* — Enable byte-caching. *disable* — Disable byte-caching.			

Parameter	Description	Type	Size	Default
byte-caching-opt	Select whether TCP byte-caching uses system memory only or both memory and disk space.	option	-	mem-only
	Option / **Description** *mem-only* — Byte caching with memory only. *mem-disk* — Byte caching with memory and disk.			
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private
	Option / **Description** *shared* — For profiles that accept nonaggressive and non-interactive protocols. *express-shared* — For profiles that accept interactive protocols such as Telnet. *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.			
log-traffic	Enable/disable logging.	option	-	enable
	Option / **Description** *enable* — Enable logging. *disable* — Disable logging.			
port	Port numbers or port number ranges for TCP. Only packets with a destination port number that matches this port number or range are accepted by this profile.	user	Not Specified	
ssl	Enable/disable SSL/TLS offloading (hardware acceleration) for traffic in this tunnel.	option	-	disable
	Option / **Description** *enable* — Enable SSL/TLS offloading. *disable* — Disable SSL/TLS offloading.			
ssl-port	Port numbers or port number ranges on which to expect HTTPS traffic for SSL/TLS offloading.	user	Not Specified	

config wanopt remote-storage

Configure a remote cache device as Web cache storage.

```
config wanopt remote-storage
    Description: Configure a remote cache device as Web cache storage.
    set status [disable|enable]
    set local-cache-id {string}
    set remote-cache-id {string}
    set remote-cache-ip {ipv4-address-any}
end
```

config wanopt remote-storage

Parameter	Description	Type	Size	Default
status	Enable/disable using remote device as Web cache storage.	option	-	disable
	Option / **Description** *disable* — Use local disks as Web cache storage. *enable* — Use a remote device as Web cache storage.			
local-cache-id	ID that this device uses to connect to the remote device.	string	Maximum length: 35	
remote-cache-id	ID of the remote device to which the device connects.	string	Maximum length: 35	
remote-cache-ip	IP address of the remote device to which the device connects.	ipv4-address-any	Not Specified	0.0.0.0

config wanopt settings

Configure WAN optimization settings.

```
config wanopt settings
    Description: Configure WAN optimization settings.
    set host-id {string}
    set tunnel-ssl-algorithm {option}
    set auto-detect-algorithm [simple|diff-req-resp]
    set tunnel-optimization [memory-usage|balanced|...]
end
```

config wanopt settings

Parameter	Description	Type	Size	Default
host-id	Local host ID (must also be entered in the remote FortiProxy's peer list).	string	Maximum length: 35	default-id
tunnel-ssl-algorithm	Relative strength of encryption algorithms accepted during tunnel negotiation.	option	-	low
	Option / **Description** *low* — Low encryption algorithms accepted in tunnel negotiation.			
auto-detect-algorithm	Auto detection algorithms used in tunnel negotiations.	option	-	simple
	Option / **Description** *simple* — Use the same TCP option value in SYN/SYNACK packets. Backward compatible. *diff-req-resp* — Use different TCP option values in SYN/SYNACK packets to avoid false positive detection.			
tunnel-optimization	WANOpt tunnel optimization option.	option	-	balanced
	Option / **Description** *memory-usage* — Optimize tunnel for low system memory usage. *balanced* — Optimize tunnel to balance between system memory usage and throughput. *throughput* — Optimize tunnel for throughput.			

web-proxy

This section includes syntax for the following commands:

config web-proxy debug-url

Configure debug URL addresses.

```
config web-proxy debug-url
    Description: Configure debug URL addresses.
    edit <name>
        set url-pattern {string}
        set status [enable|disable]
        set exact [enable|disable]
    next
end
```

config web-proxy debug-url

Parameter	Description	Type	Size	Default
url-pattern	URL exemption pattern.	string	Maximum length: 511	
status	Enable/disable this URL exemption.	option	-	enable

Option	Description
enable	Enable this URL exemption.
disable	Disable this URL exemption.

Parameter	Description	Type	Size	Default
exact	Enable/disable matching the exact path.	option	-	enable

Option	Description
enable	Enable matching the exact path.
disable	Disable matching the exact path.

config web-proxy dynamic-bypass

Configure dynamic bypass settings.

```
config web-proxy dynamic-bypass
    Description: Configure dynamic bypass settings.
    set status [enable|disable]
    set errors {option1}, {option2}, ...
    set total-max {integer}
    set server-max {integer}
    set timeout {integer}
end
```

config web-proxy dynamic-bypass

Parameter	Description	Type	Size	Default
status	Enable/disable dynamic bypass.	option	-	disable

Option	Description
enable	Enable dynamic bypass.
disable	Disable dynamic bypass.

Parameter	Description	Type	Size	Default
errors	Configure bypass errors.	option	-	

Option	Description
connect-error	Connect error.
receive-error	HTTP response is not received.
non-http	HTTP protocol is not detected.
400	HTTP response code is 400.
401	HTTP response code is 401.
403	HTTP response code is 403.

Parameter	Description	Type	Size	Default
	Option / **Description** *405* — HTTP response code is 405. *406* — HTTP response code is 406. *500* — HTTP response code is 500. *502* — HTTP response code is 502. *503* — HTTP response code is 503. *504* — HTTP response code is 504.			
total-max	Maximum numbers of entries in dynamic bypass list .	integer	Minimum value: 10 Maximum value: 50000	5000
server-max	Maximum numbers of entries in dynamic bypass list belongs to one server, all requests to this server will be bypassed once server-max is reached .	integer	Minimum value: 1 Maximum value: 255	16
timeout	Maximum time .	integer	Minimum value: 1 Maximum value: 21600	60

config web-proxy explicit-proxy

Configure explicit Web proxy settings.

```
config web-proxy explicit-proxy
    Description: Configure explicit Web proxy settings.
    edit <name>
        set status [enable|disable]
        set interface {string}
        set ftp-over-http [enable|disable]
        set socks [enable|disable]
        set http-incoming-port {user}
        set https-incoming-port {user}
        set ftp-incoming-port {user}
        set socks-incoming-port {user}
        set incoming-ip {ipv4-address-any}
        set ipv6-status [enable|disable]
        set incoming-ip6 {ipv6-address}
        set pref-dns-result [ipv4|ipv6]
        set unknown-http-version [reject|best-effort]
```

```
        set realm {string}
        set sec-default-action [accept|deny]
        set pac-file-server-status [enable|disable]
        set pac-file-url {user}
        set pac-file-server-port {user}
        set pac-file-name {string}
        set pac-file-data {user}
        set ssl-algorithm {option}
        set return-to-sender [enable|disable]
        set detect-https-in-http-request [enable|disable]
        set learn-dst-from-sni [enable|disable]
    next
end
```

config web-proxy explicit-proxy

Parameter	Description	Type	Size	Default
status	Enable/disable the explicit Web proxy for HTTP and HTTPS session.	option	-	disable
	Option / **Description** *enable* — Enable the explicit web proxy. *disable* — Disable the explicit web proxy.			
interface	interface name	string	Maximum length: 15	
ftp-over-http	Enable to proxy FTP-over-HTTP sessions sent from a web browser.	option	-	disable
	Option / **Description** *enable* — Enable FTP-over-HTTP sessions. *disable* — Disable FTP-over-HTTP sessions.			
socks	Enable/disable the SOCKS proxy.	option	-	disable
	Option / **Description** *enable* — Enable the SOCKS proxy. *disable* — Disable the SOCKS proxy.			
http-incoming-port	Accept incoming HTTP requests on one or more ports .	user	Not Specified	
https-incoming-port	Accept incoming HTTPS requests on one or more ports .	user	Not Specified	

Parameter	Description	Type	Size	Default
ftp-incoming-port	Accept incoming FTP-over-HTTP requests on one or more ports .	user	Not Specified	
socks-incoming-port	Accept incoming SOCKS proxy requests on one or more ports .	user	Not Specified	
incoming-ip	Restrict the explicit HTTP proxy to only accept sessions from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	0.0.0.0
ipv6-status	Enable/disable allowing an IPv6 web proxy destination in policies and all IPv6 related entries in this command.	option	-	disable
	Option / **Description** *enable* — Enable allowing an IPv6 web proxy destination. *disable* — Disable allowing an IPv6 web proxy destination.			
incoming-ip6	Restrict the explicit web proxy to only accept sessions from this IPv6 address. An interface must have this IPv6 address.	ipv6-address	Not Specified	::
pref-dns-result	Prefer resolving addresses using the configured IPv4 or IPv6 DNS server .	option	-	ipv4
	Option / **Description** *ipv4* — Prefer the IPv4 DNS server. *ipv6* — Prefer the IPv6 DNS server.			
unknown-http-version	How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.	option	-	reject
	Option / **Description** *reject* — Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1. *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.			
realm	Authentication realm used to identify the explicit web proxy (maximum of 63 characters).	string	Maximum length: 63	default
sec-default-action	Accept or deny explicit web proxy sessions when no web proxy firewall policy exists.	option	-	deny

Parameter	Description	Type	Size	Default
	Option / **Description** *accept* — Accept requests. All explicit web proxy traffic is accepted whether there is an explicit web proxy policy or not. *deny* — Deny requests unless there is a matching explicit web proxy policy.			
pac-file-server-status	Enable/disable Proxy Auto-Configuration (PAC) for users of this explicit proxy profile.	option	-	disable
	Option / **Description** *enable* — Enable Proxy Auto-Configuration (PAC). *disable* — Disable Proxy Auto-Configuration (PAC).			
pac-file-url	PAC file access URL.	user	Not Specified	
pac-file-server-port	Port number that PAC traffic from client web browsers uses to connect to the explicit web proxy .	user	Not Specified	
pac-file-name	Pac file name.	string	Maximum length: 63	proxy.pac
pac-file-data	PAC file contents enclosed in quotes (maximum of 256K bytes).	user	Not Specified	
ssl-algorithm	Relative strength of encryption algorithms accepted in HTTPS deep scan: high, medium, or low.	option	-	low
	Option / **Description** *low* — Low encryption algorithms accepted in HTTPS deep scan.			
return-to-sender	Enable/disable return-to-sender.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
detect-https-in-http-request	Enable/disable detecting SSL in HTTP request line.	option	-	disable
	Option / **Description** *enable* — Enable detecting SSL in HTTP request line. *disable* — Disable detecting SSL in HTTP request line.			

Parameter	Description	Type	Size	Default
learn-dst-from-sni	Enable/disable learning destination from SNI in client hello.	option	-	disable

Option	Description
enable	Enable learning destination from SNI in client hello.
disable	Disable learning destination from SNI in client hello.

config web-proxy forward-server-group

Configure a forward server group consisting or multiple forward servers. Supports failover and load balancing.

```
config web-proxy forward-server-group
    Description: Configure a forward server group consisting or multiple forward servers.
Supports failover and load balancing.
    edit <name>
        set affinity [enable|disable]
        set ldb-method [weighted|least-session|...]
        set group-down-option [block|pass]
        config server-list
            Description: Add web forward servers to a list to form a server group.
Optionally assign weights to each server.
            edit <name>
                set weight {integer}
            next
        end
    next
end
```

config web-proxy forward-server-group

Parameter	Description	Type	Size	Default
affinity	Enable/disable affinity, attaching a source-ip's traffic to the assigned forwarding server until the forward-server-affinity-timeout is reached (under web-proxy global).	option	-	enable

Option	Description
enable	Enable affinity.
disable	Disable affinity.

ldb-method	Load balance method: weighted or least-session.	option	-	weighted

Parameter	Description	Type	Size	Default
	Option / **Description** *weighted* — Load balance traffic to forward servers based on assigned weights. Weights are ratios of total number of sessions. *least-session* — Send new sessions to the server with lowest session count. *active-passive* — Send new sessions to the next active server in the list. Servers are selected with highest weight first and then in order as they are configured. Traffic switches back to the first server upon failure recovery.			
group-down-option	Action to take when all of the servers in the forward server group are down: block sessions until at least one server is back up or pass sessions to their destination.	option	-	block
	Option / **Description** *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

Parameter	Description	Type	Size	Default
weight	Optionally assign a weight of the forwarding server for weighted load balancing .	integer	Minimum value: 1 Maximum value: 100	10

config web-proxy forward-server

Configure forward-server addresses.

```
config web-proxy forward-server
    Description: Configure forward-server addresses.
    edit <name>
        set addr-type [ip|fqdn]
        set ip {ipv4-address-any}
        set fqdn {string}
        set port {integer}
        set comment {string}
        set masquerade [enable|disable]
        set healthcheck [disable|enable]
        set monitor {string}
        set server-down-option [block|pass]
        set username {string}
```

```
        set password {password}
    next
end
```

config web-proxy forward-server

Parameter	Description	Type	Size	Default
addr-type	Address type of the forwarding proxy server: IP or FQDN.	option	-	ip
	Option / **Description** *ip* — Use an IP address for the forwarding proxy server. *fqdn* — Use the FQDN for the forwarding proxy server.			
ip	Forward proxy server IP address.	ipv4-address-any	Not Specified	0.0.0.0
fqdn	Forward server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255	
port	Port number that the forwarding server expects to receive HTTP sessions on .	integer	Minimum value: 1 Maximum value: 65535	3128
comment	Comment.	string	Maximum length: 63	
masquerade	set webproxy to use device address to connect proxy server.	option	-	enable
	Option / **Description** *enable* — Enable using device address to connect proxy server. *disable* — Disable using device address to connect proxy server.			
healthcheck	Enable/disable forward server health checking. Attempts to connect through the remote forwarding server to a destination to verify that the forwarding server is operating normally.	option	-	disable
	Option / **Description** *disable* — Disable health checking. *enable* — Enable health checking.			

Parameter	Description	Type	Size	Default
monitor	URL for forward server health check monitoring .	string	Maximum length: 255	http://www.google.com
server-down-option	Action to take when the forward server is found to be down: block sessions until the server is back up or pass sessions to their destination.	option	-	block
	Option / **Description** *block* — Block sessions until the server is back up. *pass* — Pass sessions to their destination bypassing the forward server.			
username	HTTP authentication user name.	string	Maximum length: 64	
password	HTTP authentication password.	password	Not Specified	

config web-proxy global

Configure Web proxy global settings.

```
config web-proxy global
    Description: Configure Web proxy global settings.
    set ssl-cert {string}
    set ssl-ca-cert {string}
    set fast-policy-match [enable|disable]
    set ldap-user-cache [enable|disable]
    set use-dynamic-pkey [enable|disable]
    set proxy-fqdn {string}
    set max-request-length {integer}
    set max-message-length {integer}
    set strict-web-check [enable|disable]
    set forward-proxy-auth [enable|disable]
    set forward-server-affinity-timeout {integer}
    set webproxy-profile {string}
    set learn-client-ip [enable|disable]
    set learn-client-ip-from-header {option1}, {option2}, ...
    set learn-client-ip-srcaddr <name1>, <name2>, ...
    set learn-client-ip-srcaddr6 <name1>, <name2>, ...
    set src-affinity-exempt-addr {ipv4-address-any}
    set src-affinity-exempt-addr6 {ipv6-address}
    set strict-guest [enable|disable]
    set https-replacement-message [enable|disable]
    set message-upon-server-error [enable|disable]
    set trace-auth-no-rsp [enable|disable]
    set log-policy-pending [enable|disable]
    set explicit-outgoing-ip {ipv4-address-any}
    set explicit-outgoing-ip6 {ipv6-address}
```

```
    set realm {string}
end
```

config web-proxy global

Parameter	Description	Type	Size	Default
ssl-cert	SSL certificate for SSL interception.	string	Maximum length: 35	default-server-cert
ssl-ca-cert	SSL CA certificate for SSL interception.	string	Maximum length: 35	default-ca
fast-policy-match	Enable/disable fast matching algorithm for explicit and transparent proxy policy.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
ldap-user-cache	Enable/disable ldap user cache for explicit and transparent proxy user.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
use-dynamic-pkey	Enable/disable use dynamic private key in the resigned cert.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
proxy-fqdn	Fully Qualified Domain Name to connect to the explicit web proxy.	string	Maximum length: 255	default.fqdn
max-request-length	Maximum length of HTTP request line .	integer	Minimum value: 2 Maximum value: 64	8
max-message-length	Maximum length of HTTP message, not including body .	integer	Minimum value: 16 Maximum value: 256	32

Parameter	Description	Type	Size	Default
strict-web-check	Enable/disable strict web checking to block web sites that send incorrect headers that don't conform to HTTP 1.1.	option	-	disable
	Option / **Description** *enable* — Enable strict web checking. *disable* — Disable strict web checking.			
forward-proxy-auth	Enable/disable forwarding proxy authentication headers.	option	-	disable
	Option / **Description** *enable* — Enable forwarding proxy authentication headers. *disable* — Disable forwarding proxy authentication headers.			
forward-server-affinity-timeout	Period of time before the source IP's traffic is no longer assigned to the forwarding server .	integer	Minimum value: 6 Maximum value: 60	30
webproxy-profile	Name of the web proxy profile to apply when explicit proxy traffic is allowed by default and traffic is accepted that does not match an explicit proxy policy.	string	Maximum length: 63	
learn-client-ip	Enable/disable learning the client's IP address from headers.	option	-	disable
	Option / **Description** *enable* — Enable learning the client's IP address from headers. *disable* — Disable learning the client's IP address from headers.			
learn-client-ip-from-header	Learn client IP address from the specified headers.	option	-	
	Option / **Description** *true-client-ip* — Learn the client IP address from the True-Client-IP header. *x-real-ip* — Learn the client IP address from the X-Real-IP header. *x-forwarded-for* — Learn the client IP address from the X-Forwarded-For header.			
learn-client-ip-srcaddr `<name>`	Source address name (srcaddr or srcaddr6 must be set). Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
learn-client-ip-srcaddr6 <name>	IPv6 Source address name (srcaddr or srcaddr6 must be set). Address name.	string	Maximum length: 79	
src-affinity-exempt-addr	IPv4 source addresses to exempt proxy affinity.	ipv4-address-any	Not Specified	
src-affinity-exempt-addr6	IPv6 source addresses to exempt proxy affinity.	ipv6-address	Not Specified	
strict-guest	Enable/disable strict guest user checking by the explicit web proxy.	option	-	disable
	Option / **Description** *enable* — Enable strict guest user checking. *disable* — Disable strict guest user checking.			
https-replacement-message	Default action to enable or disable return replacement message for HTTPS requests.	option	-	enable
	Option / **Description** *enable* — Display a replacement message for HTTPS requests. *disable* — Do not display a replacement message for HTTPS requests.			
message-upon-server-error	Enable/disable return of replacement message upon server error detection.	option	-	enable
	Option / **Description** *enable* — Display a replacement message when a server error is detected. *disable* — Do not display a replacement message when a server error is detected.			
trace-auth-no-rsp	Enable/disable logging timed-out authentication requests.	option	-	disable
	Option / **Description** *enable* — Enable logging timed-out authentication requests. *disable* — Disable logging timed-out authentication requests.			
log-policy-pending	Enable/disable logging sessions that are pending on policy matching.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable logging sessions that are pending on policy matching. *disable* / Disable logging sessions that are pending on policy matching.			
explicit-outgoing-ip	Outgoing HTTP requests by explicit webproxy will have this IP address as their source address. An interface must have this IP address.	ipv4-address-any	Not Specified	
explicit-outgoing-ip6	Outgoing HTTP requests by explicit webproxy will leave this IP. An interface must have this IP address.	ipv6-address	Not Specified	
realm	Authentication realm.	string	Maximum length: 63	default

config web-proxy isolator-server

Configure forward-server addresses.

```
config web-proxy isolator-server
    Description: Configure forward-server addresses.
    edit <name>
        set addr-type [ip|fqdn]
        set ip {ipv4-address-any}
        set fqdn {string}
        set port {integer}
        set comment {string}
        set masquerade [enable|disable]
    next
end
```

config web-proxy isolator-server

Parameter	Description	Type	Size	Default
addr-type	Address type of the forwarding proxy server: IP or FQDN.	option	-	ip
	Option / **Description** *ip* / Use an IP address for the forwarding proxy server. *fqdn* / Use the FQDN for the forwarding proxy server.			
ip	Forward proxy server IP address.	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
fqdn	Forward server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255	
port	Port number that the forwarding server expects to receive HTTP sessions on .	integer	Minimum value: 1 Maximum value: 65535	3128
comment	Comment.	string	Maximum length: 63	
masquerade	set webproxy to use device address to connect proxy server.	option	-	enable

Option	Description
enable	Enable using device address to connect proxy server.
disable	Disable using device address to connect proxy server.

config web-proxy pac-policy

Configure explicit Web proxy pac policy.

```
config web-proxy pac-policy
    Description: Configure explicit Web proxy pac policy.
    edit <policyid>
        set status [enable|disable]
        set srcaddr <name1>, <name2>, ...
        set srcaddr6 <name1>, <name2>, ...
        set dstaddr <name1>, <name2>, ...
        set pac-file-name {string}
        set pac-file-data {user}
        set comments {var-string}
    next
end
```

config web-proxy pac-policy

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

Option	Description
enable	Enable policy.

Parameter	Description	Type	Size	Default
	Option: *disable* — Description: Disable policy.			
srcaddr <name>	Source address objects. Address name.	string	Maximum length: 79	
srcaddr6 <name>	Source address6 objects. Address name.	string	Maximum length: 79	
dstaddr <name>	Destination address objects. Address name.	string	Maximum length: 79	
pac-file-name	Pac file name.	string	Maximum length: 63	proxy.pac
pac-file-data	PAC file contents enclosed in quotes (maximum of 256K bytes).	user	Not Specified	
comments	Optional comments.	var-string	Maximum length: 1023	

config web-proxy profile

Configure web proxy profiles.

```
config web-proxy profile
    Description: Configure web proxy profiles.
    edit <name>
        set max-cache-object-size {integer}
        set header-client-ip [pass|add|...]
        set header-via-request [pass|add|...]
        set header-via-response [pass|add|...]
        set header-x-forwarded-for [pass|add|...]
        set header-x-forwarded-client-cert [pass|add|...]
        set header-front-end-https [pass|add|...]
        set header-x-authenticated-user [pass|add|...]
        set header-x-authenticated-groups [pass|add|...]
        set strip-encoding [enable|disable]
        set log-header-change [enable|disable]
        config headers
            Description: Configure HTTP forwarded requests headers.
            edit <id>
                set name {string}
                set dstaddr <name1>, <name2>, ...
                set dstaddr6 <name1>, <name2>, ...
                set action [add-to-request|add-to-response|...]
                set content {string}
                set base64-encoding [disable|enable]
                set add-option [append|new-on-not-found|...]
                set protocol {option1}, {option2}, ...
```

```
            next
        end
    next
end
```

config web-proxy profile

Parameter	Description	Type	Size	Default
max-cache-object-size	Maximum cacheable object size in KB . When the value is set to 0, the max cache object size will be max-object-size under webcache settings.	integer	Minimum value: 0 Maximum value: 3984384	0
header-client-ip	Action to take on the HTTP client-IP header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	Option / **Description** *pass* — Forward the same HTTP header. *add* — Add the HTTP header. *remove* — Remove the HTTP header.			
header-via-request	Action to take on the HTTP via header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	Option / **Description** *pass* — Forward the same HTTP header. *add* — Add the HTTP header. *remove* — Remove the HTTP header.			
header-via-response	Action to take on the HTTP via header in forwarded responses: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	Option / **Description** *pass* — Forward the same HTTP header. *add* — Add the HTTP header. *remove* — Remove the HTTP header.			
header-x-forwarded-for	Action to take on the HTTP x-forwarded-for header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass

Parameter	Description	Type	Size	Default
	Option / **Description** *pass* — Forward the same HTTP header. *add* — Add the HTTP header. *remove* — Remove the HTTP header.			
header-x-forwarded-client-cert	Action to take on the HTTP x-forwarded-client-cert header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	Option / **Description** *pass* — Forward the same HTTP header. *add* — Add the HTTP header. *remove* — Remove the HTTP header.			
header-front-end-https	Action to take on the HTTP front-end-HTTPS header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	Option / **Description** *pass* — Forward the same HTTP header. *add* — Add the HTTP header. *remove* — Remove the HTTP header.			
header-x-authenticated-user	Action to take on the HTTP x-authenticated-user header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	Option / **Description** *pass* — Forward the same HTTP header. *add* — Add the HTTP header. *remove* — Remove the HTTP header.			
header-x-authenticated-groups	Action to take on the HTTP x-authenticated-groups header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	Option / **Description** *pass* — Forward the same HTTP header.			

Parameter	Description	Type	Size	Default
	Option / **Description** *add* — Add the HTTP header. *remove* — Remove the HTTP header.			
strip-encoding	Enable/disable stripping unsupported encoding from the request header.	option	-	disable
	Option / **Description** *enable* — Enable stripping of unsupported encoding from the request header. *disable* — Disable stripping of unsupported encoding from the request header.			
log-header-change	Enable/disable logging HTTP header changes.	option	-	disable
	Option / **Description** *enable* — Enable Enable/disable logging HTTP header changes. *disable* — Disable Enable/disable logging HTTP header changes.			

config headers

Parameter	Description	Type	Size	Default
name	HTTP forwarded header name.	string	Maximum length: 79	
dstaddr <name>	Destination address and address group names. Address name.	string	Maximum length: 79	
dstaddr6 <name>	Destination address and address group names (IPv6). Address name.	string	Maximum length: 79	
action	Action when the HTTP header is forwarded.	option	-	add-to-request
	Option / **Description** *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.			

Parameter	Description	Type	Size	Default
content	HTTP header content.	string	Maximum length: 511	
base64-encoding	Enable/disable use of base64 encoding of HTTP content.	option	-	disable

Option	Description
disable	Disable use of base64 encoding of HTTP content.
enable	Enable use of base64 encoding of HTTP content.

Parameter	Description	Type	Size	Default
add-option	Configure options to append content to existing HTTP header or add new HTTP header.	option	-	new

Option	Description
append	Append content to existing HTTP header or create new header if HTTP header is not found.
new-on-not-found	Create new header only if existing HTTP header is not found.
new	Create new header regardless if existing HTTP header is found or not.

Parameter	Description	Type	Size	Default
protocol	Configure protocol(s) to take add-option action on (HTTP, HTTPS, or both).	option	-	https http

Option	Description
https	Perform add-option action on HTTPS.
http	Perform add-option action on HTTP.

config web-proxy url-list

URLs for web proxy.

```
config web-proxy url-list
    Description: URLs for web proxy.
    edit <name>
        set comment {var-string}
        config entries
            Description: URL list entries.
            edit <id>
                set status [enable|disable]
                set url {string}
                set type [simple|wildcard]
            next
        end
```

```
    next
end
```

config web-proxy url-list

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

config entries

Parameter	Description	Type	Size	Default
status	Enable/disable the entry.	option	-	enable
	Option / **Description** *enable* / Enable The URL. *disable* / Disable The URL.			
url	URL.	string	Maximum length: 511	
type	URL type (simple, wildcard).	option	-	simple
	Option / **Description** *simple* / Simple URL string. *wildcard* / Wildcard URL string (only '*').			

config web-proxy url-match

URLs to be exempted from caching and/or to be redirected to forward server.

```
config web-proxy url-match
    Description: URLs to be exempted from caching and/or to be redirected to forward server.
    edit <name>
        set status [enable|disable]
        set type [simple|wildcard|...]
        set url-pattern {string}
        set url-list {string}
        set forward-server {string}
        set cache-exemption [enable|disable]
        set comment {var-string}
    next
end
```

config web-proxy url-match

Parameter	Description	Type	Size	Default
status	Enable/disable URLs to be exempted from caching and/or to be redirected to forward server.	option	-	enable
	Option / **Description** *enable* — Enable exempting the matching URLs. *disable* — Disable exempting the matching URLs.			
type	URL type (simple, wildcard, list).	option	-	simple
	Option / **Description** *simple* — Simple URL string. *wildcard* — Wildcard URL string (only '*'). *list* — URL list.			
url-pattern	URL pattern to be exempted from caching and/or to be redirected to forward server.	string	Maximum length: 511	
url-list	URL list to be exempted from caching and/or to be redirected to forward server.	string	Maximum length: 63	
forward-server	Forward server name.	string	Maximum length: 63	
cache-exemption	Enable/disable exempting this URL pattern from caching.	option	-	disable
	Option / **Description** *enable* — Enable exempting this URL pattern from caching. *disable* — Disable exempting this URL pattern from caching.			
comment	Comment.	var-string	Maximum length: 255	

config web-proxy wisp

Configure Websense Integrated Services Protocol (WISP) servers.

```
config web-proxy wisp
    Description: Configure Websense Integrated Services Protocol (WISP) servers.
    edit <name>
        set comment {var-string}
        set outgoing-ip {ipv4-address-any}
```

```
        set server-ip {ipv4-address-any}
        set server-port {integer}
        set max-connections {integer}
        set timeout {integer}
    next
end
```

config web-proxy wisp

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
outgoing-ip	WISP outgoing IP address.	ipv4-address-any	Not Specified	0.0.0.0
server-ip	WISP server IP address.	ipv4-address-any	Not Specified	0.0.0.0
server-port	WISP server port .	integer	Minimum value: 1 Maximum value: 65535	15868
max-connections	Maximum number of web proxy WISP connections .	integer	Minimum value: 4 Maximum value: 4096	64
timeout	Period of time before WISP requests time out .	integer	Minimum value: 1 Maximum value: 15	5

webcache

This section includes syntax for the following commands:

config webcache prefetch

Configure cache prefetch.

```
config webcache prefetch
    Description: Configure cache prefetch.
    edit <name>
        set url {string}
        set crawl-depth {integer}
        set ignore-robots [enable|disable]
        set interval {integer}
        set start-delay {integer}
        set repeat {integer}
        set user {string}
        set password {password}
        set user-agent <name1>, <name2>, ...
    next
end
```

config webcache prefetch

Parameter	Description	Type	Size	Default
url	URL of the target.	string	Maximum length: 1023	
crawl-depth	Depth to crawl the whole url.	integer	Minimum value: 0 Maximum value: 16	0
ignore-robots	Ignore robots.txt specification.	option	-	disable

Option	Description
enable	Ignore robots.txt config while crawling the url.

Parameter	Description	Type	Size	Default
	Option **Description** *disable* Obey robots.txt config while crawling the url.			
interval	Time interval (in seconds) to fetch the url.	integer	Minimum value: 0 Maximum value: 608400	43200
start-delay	Delay period to start the fetching (in secondss).	integer	Minimum value: 0 Maximum value: 2422800	0
repeat	How many times repeat to fetch the url .	integer	Minimum value: 0 Maximum value: 4294967295	0
user	Username for the Web resource.	string	Maximum length: 64	
password	Password for the Web resource.	password	Not Specified	
user-agent <name>	User agents can be used by this prefetch. User agent.	string	Maximum length: 79	

config webcache reverse-cache-server

Configure reverse cache server.

```
config webcache reverse-cache-server
    Description: Configure reverse cache server.
    edit <name>
        set ip {ipv4-address-any}
        set port {integer}
        set status [enable|disable]
        set priority {integer}
    next
end
```

config webcache reverse-cache-server

Parameter	Description	Type	Size	Default
ip	Server IP address.	ipv4-address-any	Not Specified	0.0.0.0
port	Server port.	integer	Minimum value: 1 Maximum value: 65535	80
status	Enable/disable the cache server.	option	-	enable
	Option / **Description** *enable* — Enable the reverse-cache-server. *disable* — Disable the reverse-cache-server.			
priority	Priority of the cache server (reserved).	integer	Minimum value: 0 Maximum value: 15	0

config webcache settings

Configure global Web cache settings.

```
config webcache settings
    Description: Configure global Web cache settings.
    set max-object-size {integer}
    set neg-resp-time {integer}
    set fresh-factor {integer}
    set max-ttl {integer}
    set min-ttl {integer}
    set default-ttl {integer}
    set ignore-ims [enable|disable]
    set ignore-conditional [enable|disable]
    set ignore-pnc [enable|disable]
    set ignore-ie-reload [enable|disable]
    set cache-expired [enable|disable]
    set cache-cookie [enable|disable]
    set reval-pnc [enable|disable]
    set always-revalidate [enable|disable]
    set cache-by-default [enable|disable]
    set host-validate [enable|disable]
    set add-x-cache [enable|disable]
    set x-cache-message {string}
    set external [enable|disable]
```

```
    set crawler-user-agent {string}
end
```

config webcache settings

Parameter	Description	Type	Size	Default
max-object-size	Maximum cacheable object size in kB . All objects that exceed this are delivered to the client but not stored in the web cache.	integer	Minimum value: 1 Maximum value: 2147483	512000
neg-resp-time	Time in minutes to cache negative responses or errors .	integer	Minimum value: 0 Maximum value: 4294967295	0
fresh-factor	Frequency that the server is checked to see if any objects have expired . The higher the fresh factor, the less often the checks occur.	integer	Minimum value: 1 Maximum value: 100	100
max-ttl	Maximum time an object can stay in the web cache without checking to see if it has expired on the server .	integer	Minimum value: 1 Maximum value: 5256000	7200
min-ttl	Minimum time an object can stay in the web cache without checking to see if it has expired on the server .	integer	Minimum value: 1 Maximum value: 5256000	5
default-ttl	Default object expiry time . This only applies to those objects that do not have an expiry time set by the web server.	integer	Minimum value: 1 Maximum value: 5256000	1440
ignore-ims	Enable/disable ignoring the if-modified-since (IMS) header.	option	-	disable

Option	Description
enable	Enable ignoring the if-modified-since (IMS) header.
disable	Disable ignoring the if-modified-since (IMS) header.

Parameter	Description	Type	Size	Default
ignore-conditional	Enable/disable controlling the behavior of cache-control HTTP 1.1 header values.	option	-	disable

Option	Description
enable	Enable ignoring cache-control HTTP 1.1 header values.
disable	Disable ignoring cache-control HTTP 1.1 header values.

Parameter	Description	Type	Size	Default
ignore-pnc	Enable/disable ignoring the pragma no-cache (PNC) header.	option	-	disable

Option	Description
enable	Enable ignoring the pragma no-cache (PNC) header.
disable	Disable ignoring the pragma no-cache (PNC) header.

Parameter	Description	Type	Size	Default
ignore-ie-reload	Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.	option	-	enable

Option	Description
enable	Enable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.
disable	Disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.

Parameter	Description	Type	Size	Default
cache-expired	Enable/disable caching type-1 objects that are already expired on arrival.	option	-	disable

Option	Description
enable	Enable caching type-1 objects that have expired.
disable	Disable caching type-1 objects that have expired.

Parameter	Description	Type	Size	Default
cache-cookie	Enable/disable caching cookies. Since cookies contain information for or about individual users, they not usually cached..	option	-	disable

Option	Description
enable	Cache cookies.
disable	Do not cache cookies.

Parameter	Description	Type	Size	Default
reval-pnc	Enable/disable revalidation of pragma-no-cache (PNC) to address bandwidth concerns.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable revalidation of pragma-no-cache (PNC). *disable* — Disable revalidation of pragma-no-cache (PNC).			
always-revalidate	Enable/disable revalidation of requested cached objects, which have content on the server, before serving it to the client.	option	-	disable
	Option / **Description** *enable* — Enable revalidation of requested cached objects. *disable* — Disable revalidation of requested cached objects.			
cache-by-default	Enable/disable caching content that lacks explicit caching policies from the server.	option	-	disable
	Option / **Description** *enable* — Enable caching content that lacks explicit caching policies. *disable* — Disable caching content that lacks explicit caching policies.			
host-validate	Enable/disable validating "Host:" with original server IP.	option	-	disable
	Option / **Description** *enable* — Enable validating "Host:" with original server IP. *disable* — Disable validating "Host:" with original server IP.			
add-x-cache	Enable/disable appending local "X-Cache: HIT/MISS" information when http-request is cacheable.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
x-cache-message	Config customized x-cache header message .	string	Maximum length: 400	
external	Enable/disable external Web caching.	option	-	disable
	Option / **Description** *enable* — Enable external Web caching *disable* — Disable external Web caching			

Parameter	Description	Type	Size	Default
crawler-user-agent	The user agent that the web crawler will use.	string	Maximum length: 255	fpx

config webcache user-agent

Configure reverse cache user agent.

```
config webcache user-agent
    Description: Configure reverse cache user agent.
    edit <name>
        set value {string}
    next
end
```

config webcache user-agent

Parameter	Description	Type	Size	Default
value	User agent of the URL.	string	Maximum length: 255	

webfilter

This section includes syntax for the following commands:

config webfilter categories

List the FortiGuard Web Filter category descriptions.

```
config webfilter categories
    Description: List the FortiGuard Web Filter category descriptions.
end
```

config webfilter content-header

Configure content types used by Web filter.

```
config webfilter content-header
    Description: Configure content types used by Web filter.
    edit <id>
        set name {string}
        set comment {var-string}
        config entries
            Description: Configure content types used by web filter.
            edit <pattern>
                set action [block|allow|...]
                set category {user}
```

```
            next
        end
    next
end
```

config webfilter content-header

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

config entries

Parameter	Description	Type	Size	Default
action	Action to take for this content type.	option	-	allow

Option	Description
block	Block content type.
allow	Allow content type.
exempt	Exempt content type.

Parameter	Description	Type	Size	Default
category	Categories that this content type applies to.	user	Not Specified	all

config webfilter content

Configure Web filter banned word table.

```
config webfilter content
    Description: Configure Web filter banned word table.
    edit <id>
        set name {string}
        set comment {var-string}
        config entries
            Description: Configure banned word entries.
            edit <name>
                set pattern-type [wildcard|regexp]
                set status [enable|disable]
                set lang [western|simch|...]
                set score {integer}
                set action [block|exempt]
            next
```

```
        end
    next
end
```

config webfilter content

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

config entries

Parameter	Description	Type	Size	Default
pattern-type	Banned word pattern type: wildcard pattern or Perl regular expression.	option	-	wildcard

Option	Description
wildcard	Wildcard pattern.
regexp	Perl regular expression.

Parameter	Description	Type	Size	Default
status	Enable/disable banned word.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
lang	Language of banned word.	option	-	western

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

Parameter	Description	Type	Size	Default
	Option / **Description** *spanish* / Spanish. *cyrillic* / Cyrillic.			
score	Score, to be applied every time the word appears on a web page .	integer	Minimum value: 0 Maximum value: 4294967295	10
action	Block or exempt word when a match is found.	option	-	block
	Option / **Description** *block* / Block matches. *exempt* / Exempt matches.			

config webfilter fortiguard

Configure FortiGuard Web Filter service.

```
config webfilter fortiguard
    Description: Configure FortiGuard Web Filter service.
    set cache-mode [ttl|db-ver]
    set cache-prefix-match [enable|disable]
    set cache-mem-percent {integer}
    set ovrd-auth-port-http {integer}
    set ovrd-auth-port-https {integer}
    set ovrd-auth-port-https-flow {integer}
    set ovrd-auth-port-warning {integer}
    set ovrd-auth-https [enable|disable]
    set warn-auth-https [enable|disable]
    set close-ports [enable|disable]
    set request-packet-size-limit {integer}
    set embed-image [enable|disable]
end
```

config webfilter fortiguard

Parameter	Description	Type	Size	Default
cache-mode	Cache entry expiration mode.	option	-	ttl

Parameter	Description	Type	Size	Default
	Option / **Description** *ttl* — Expire cache items by time-to-live. *db-ver* — Expire cache items when the server DB version changes.			
cache-prefix-match	Enable/disable prefix matching in the cache.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
cache-mem-percent	Maximum percentage of available memory allocated to caching .	integer	Minimum value: 1 Maximum value: 15	2
ovrd-auth-port-http	Port to use for FortiGuard Web Filter HTTP override authentication.	integer	Minimum value: 0 Maximum value: 65535	8008
ovrd-auth-port-https	Port to use for FortiGuard Web Filter HTTPS override authentication in proxy mode.	integer	Minimum value: 0 Maximum value: 65535	8010
ovrd-auth-port-https-flow	Port to use for FortiGuard Web Filter HTTPS override authentication in flow mode.	integer	Minimum value: 0 Maximum value: 65535	8015
ovrd-auth-port-warning	Port to use for FortiGuard Web Filter Warning override authentication.	integer	Minimum value: 0 Maximum value: 65535	8020
ovrd-auth-https	Enable/disable use of HTTPS for override authentication.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			

Parameter	Description	Type	Size	Default
warn-auth-https	Enable/disable use of HTTPS for warning and authentication.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
close-ports	Close ports used for HTTP/HTTPS override authentication and disable user overrides.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
request-packet-size-limit	Limit size of URL request packets sent to FortiGuard server .	integer	Minimum value: 576 Maximum value: 10000	0
embed-image	Enable/disable embedding images into replacement messages .	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			

config webfilter ftgd-local-cat

Configure FortiGuard Web Filter local categories.

```
config webfilter ftgd-local-cat
    Description: Configure FortiGuard Web Filter local categories.
    edit <desc>
        set status [enable|disable]
        set id {integer}
    next
end
```

config webfilter ftgd-local-cat

Parameter	Description	Type	Size	Default
status	Enable/disable the local category.	option	-	enable
	Option / **Description** *enable* — Enable the local category. *disable* — Disable the local category.			
id	Local category ID.	integer	Minimum value: 140 Maximum value: 191	0

config webfilter ftgd-local-rating

Configure local FortiGuard Web Filter local ratings.

```
config webfilter ftgd-local-rating
    Description: Configure local FortiGuard Web Filter local ratings.
    edit <url>
        set status [enable|disable]
        set comment {var-string}
        set rating {user}
    next
end
```

config webfilter ftgd-local-rating

Parameter	Description	Type	Size	Default
status	Enable/disable local rating.	option	-	enable
	Option / **Description** *enable* — Enable local rating. *disable* — Disable local rating.			
comment	Comment.	var-string	Maximum length: 255	
rating	Local rating.	user	Not Specified	

config webfilter ftgd-statistics

Display rating cache and daemon statistics.

```
config webfilter ftgd-statistics
    Description: Display rating cache and daemon statistics.
end
```

config webfilter ips-urlfilter-cache-setting

Configure IPS URL filter cache settings.

```
config webfilter ips-urlfilter-cache-setting
    Description: Configure IPS URL filter cache settings.
    set dns-retry-interval {integer}
    set extended-ttl {integer}
end
```

config webfilter ips-urlfilter-cache-setting

Parameter	Description	Type	Size	Default
dns-retry-interval	Retry interval. Refresh DNS faster than TTL to capture multiple IPs for hosts. 0 means use DNS server's TTL only.	integer	Minimum value: 0 Maximum value: 2147483	0
extended-ttl	Extend time to live beyond reported by DNS. Use of 0 means use DNS server's TTL.	integer	Minimum value: 0 Maximum value: 2147483	0

config webfilter ips-urlfilter-setting

Configure IPS URL filter settings.

```
config webfilter ips-urlfilter-setting
    Description: Configure IPS URL filter settings.
    set device {string}
    set distance {integer}
    set gateway {ipv4-address}
    set geo-filter {var-string}
end
```

config webfilter ips-urlfilter-setting

Parameter	Description	Type	Size	Default
device	Interface for this route.	string	Maximum length: 35	
distance	Administrative distance for this route.	integer	Minimum value: 1 Maximum value: 255	1
gateway	Gateway IP address for this route.	ipv4-address	Not Specified	0.0.0.0
geo-filter	Filter based on geographical location. Route will NOT be installed if the resolved IP address belongs to the country in the filter.	var-string	Maximum length: 255	

config webfilter ips-urlfilter-setting6

Configure IPS URL filter settings for IPv6.

```
config webfilter ips-urlfilter-setting6
    Description: Configure IPS URL filter settings for IPv6.
    set device {string}
    set distance {integer}
    set gateway6 {ipv6-address}
    set geo-filter {var-string}
end
```

config webfilter ips-urlfilter-setting6

Parameter	Description	Type	Size	Default
device	Interface for this route.	string	Maximum length: 35	
distance	Administrative distance for this route.	integer	Minimum value: 1 Maximum value: 255	1
gateway6	Gateway IPv6 address for this route.	ipv6-address	Not Specified	::
geo-filter	Filter based on geographical location. Route will NOT be installed if the resolved IPv6 address belongs to the country in the filter.	var-string	Maximum length: 255	

config webfilter override-usr

Display list of user overrides.

```
config webfilter override-usr
    Description: Display list of user overrides.
end
```

config webfilter override

Configure FortiGuard Web Filter administrative overrides.

```
config webfilter override
    Description: Configure FortiGuard Web Filter administrative overrides.
    edit <id>
        set status [enable|disable]
        set scope [user|user-group|...]
        set ip {ipv4-address}
        set user {string}
        set user-group {string}
        set old-profile {string}
        set new-profile {string}
        set ip6 {ipv6-address}
        set expires {user}
        set initiator {string}
    next
end
```

config webfilter override

Parameter	Description	Type	Size	Default
status	Enable/disable override rule.	option	-	disable

Option	Description
enable	Enable override rule.
disable	Disable override rule.

Parameter	Description	Type	Size	Default
scope	Override either the specific user, user group, IPv4 address, or IPv6 address.	option	-	user

Option	Description
user	Override the specified user.
user-group	Override the specified user group.
ip	Override the specified IP address.

Parameter	Description	Type	Size	Default
	Option **Description** *ip6* Override the specified IPv6 address.			
ip	IPv4 address which the override applies.	ipv4-address	Not Specified	0.0.0.0
user	Name of the user which the override applies.	string	Maximum length: 64	
user-group	Specify the user group for which the override applies.	string	Maximum length: 63	
old-profile	Name of the web filter profile which the override applies.	string	Maximum length: 35	
new-profile	Name of the new web filter profile used by the override.	string	Maximum length: 35	
ip6	IPv6 address which the override applies.	ipv6-address	Not Specified	::
expires	Override expiration date and time, from 5 minutes to 365 from now (format: yyyy/mm/dd hh:mm:ss).	user	Not Specified	1969/12/31 16:00:00
initiator	Initiating user of override (read-only setting).	string	Maximum length: 64	

config webfilter profile

Configure Web filter profiles.

```
config webfilter profile
    Description: Configure Web filter profiles.
    edit <name>
        set comment {var-string}
        set replacemsg-group {string}
        set options {option1}, {option2}, ...
        set https-replacemsg [enable|disable]
        set ovrd-perm {option1}, {option2}, ...
        set post-action [normal|block]
        config override
            Description: Web Filter override settings.
            set ovrd-cookie [allow|deny]
            set ovrd-scope [user|user-group|...]
            set profile-type [list|radius]
            set ovrd-dur-mode [constant|ask]
            set ovrd-dur {user}
            set profile-attribute [User-Name|NAS-IP-Address|...]
            set ovrd-user-group <name1>, <name2>, ...
            set profile <name1>, <name2>, ...
```

```
        end
        config web
            Description: Web content filtering settings.
            set bword-threshold {integer}
            set bword-table {integer}
            set urlfilter-table {integer}
            set content-header-list {integer}
            set blocklist [enable|disable]
            set allowlist {option1}, {option2}, ...
            set safe-search {option1}, {option2}, ...
            set youtube-restrict [none|strict|...]
            set vimeo-restrict {string}
            set log-search [enable|disable]
            set keyword-match <pattern1>, <pattern2>, ...
        end
        config ftgd-wf
            Description: FortiGuard Web Filter settings.
            set options {option1}, {option2}, ...
            set exempt-quota {user}
            set ovrd {user}
            config filters
                Description: FortiGuard filters.
                edit <id>
                    set category {integer}
                    set action [block|authenticate|...]
                    set warn-duration {user}
                    set auth-usr-grp <name1>, <name2>, ...
                    set log [enable|disable]
                    set override-replacemsg {string}
                    set warning-prompt [per-domain|per-category]
                    set warning-duration-type [session|timeout]
                next
            end
            config quota
                Description: FortiGuard traffic quota settings.
                edit <id>
                    set category {user}
                    set type [time|traffic]
                    set unit [B|KB|...]
                    set value {integer}
                    set duration {user}
                    set override-replacemsg {string}
                next
            end
            set max-quota-timeout {integer}
            set rate-javascript-urls [disable|enable]
            set rate-css-urls [disable|enable]
            set rate-crl-urls [disable|enable]
        end
        config antiphish
            Description: AntiPhishing profile.
            set status [enable|disable]
            set default-action [exempt|log|...]
            set check-uri [enable|disable]
            set check-basic-auth [enable|disable]
            set check-username-only [enable|disable]
```

```
            set max-body-len {integer}
            config inspection-entries
                Description: AntiPhishing entries.
                edit <name>
                    set fortiguard-category {user}
                    set action [exempt|log|...]
                next
            end
            config custom-patterns
                Description: Custom username and password regex patterns.
                edit <pattern>
                    set category [username|password]
                    set type [regex|literal]
                next
            end
            set authentication [domain-controller|ldap]
            set domain-controller {string}
            set ldap {string}
        end
        set wisp [enable|disable]
        set wisp-servers <name1>, <name2>, ...
        set wisp-algorithm [primary-secondary|round-robin|...]
        set log-all-url [enable|disable]
        set web-content-log [enable|disable]
        set web-filter-activex-log [enable|disable]
        set web-filter-command-block-log [enable|disable]
        set web-filter-cookie-log [enable|disable]
        set web-filter-applet-log [enable|disable]
        set web-filter-jscript-log [enable|disable]
        set web-filter-js-log [enable|disable]
        set web-filter-vbs-log [enable|disable]
        set web-filter-unknown-log [enable|disable]
        set web-filter-referer-log [enable|disable]
        set web-filter-cookie-removal-log [enable|disable]
        set web-url-log [enable|disable]
        set web-invalid-domain-log [enable|disable]
        set web-ftgd-err-log [enable|disable]
        set web-ftgd-quota-usage [enable|disable]
        set extended-log [enable|disable]
        set web-extended-all-action-log [enable|disable]
        set web-antiphishing-log [enable|disable]
    next
end
```

config webfilter profile

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
replacemsg-group	Replacement message group.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
options	Options.	option	-	

Option	Description
activexfilter	ActiveX filter.
cookiefilter	Cookie filter.
javafilter	Java applet filter.
block-invalid-url	Block sessions contained an invalid domain name.
jscript	Javascript block.
js	JS block.
vbs	VB script block.
unknown	Unknown script block.
intrinsic	Intrinsic script block.
wf-referer	Referring block.
wf-cookie	Cookie block.
per-user-bal	Per-user block/allow list filter

Parameter	Description	Type	Size	Default
https-replacemsg	Enable replacement messages for HTTPS.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
ovrd-perm	Permitted override types.	option	-	

Option	Description
bannedword-override	Banned word override.
urlfilter-override	URL filter override.
fortiguard-wf-override	FortiGuard Web Filter override.
contenttype-check-override	Content-type header override.

Parameter	Description	Type	Size	Default
post-action	Action taken for HTTP POST traffic.	option	-	normal

Parameter	Description	Type	Size	Default
	Option / **Description** *normal* — Normal, POST requests are allowed. *block* — POST requests are blocked.			
wisp	Enable/disable web proxy WISP.	option	-	disable
	Option / **Description** *enable* — Enable web proxy WISP. *disable* — Disable web proxy WISP.			
wisp-servers <name>	WISP servers. Server name.	string	Maximum length: 79	
wisp-algorithm	WISP server selection algorithm.	option	-	auto-learning
	Option / **Description** *primary-secondary* — Select the first healthy server in order. *round-robin* — Select the next healthy server. *auto-learning* — Select the lightest loading healthy server.			
log-all-url	Enable/disable logging all URLs visited.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
web-content-log	Enable/disable logging logging blocked web content.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
web-filter-activex-log	Enable/disable logging ActiveX.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			

Parameter	Description	Type	Size	Default
web-filter-command-block-log	Enable/disable logging blocked commands.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
web-filter-cookie-log	Enable/disable logging cookie filtering.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
web-filter-applet-log	Enable/disable logging Java applets.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
web-filter-jscript-log	Enable/disable logging JScripts.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
web-filter-js-log	Enable/disable logging Java scripts.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
web-filter-vbs-log	Enable/disable logging VBS scripts.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			

Parameter	Description	Type	Size	Default
web-filter-unknown-log	Enable/disable logging unknown scripts.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
web-filter-referer-log	Enable/disable logging referrers.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
web-filter-cookie-removal-log	Enable/disable logging blocked cookies.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
web-url-log	Enable/disable logging URL filtering.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
web-invalid-domain-log	Enable/disable logging invalid domain names.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
web-ftgd-err-log	Enable/disable logging rating errors.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
web-ftgd-quota-usage	Enable/disable logging daily quota usage.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
extended-log	Enable/disable extended logging for web filtering.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
web-extended-all-action-log	Enable/disable extended any filter action logging for web filtering.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
web-antiphishing-log	Enable/disable logging of AntiPhishing checks.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

config override

Parameter	Description	Type	Size	Default
ovrd-cookie	Allow/deny browser-based (cookie) overrides.	option	-	deny

Option	Description
allow	Allow browser-based (cookie) override.
deny	Deny browser-based (cookie) override.

Parameter	Description	Type	Size	Default
ovrd-scope	Override scope.	option	-	user

Parameter	Description	Type	Size	Default
	Option / **Description** *user* — Override for the user. *user-group* — Override for the user's group. *ip* — Override for the initiating IP. *browser* — Create browser-based (cookie) override. *ask* — Prompt for scope when initiating an override.			
profile-type	Override profile type.	option	-	list
	Option / **Description** *list* — Profile chosen from list. *radius* — Profile determined by RADIUS server.			
ovrd-dur-mode	Override duration mode.	option	-	constant
	Option / **Description** *constant* — Constant mode. *ask* — Prompt for duration when initiating an override.			
ovrd-dur	Override duration.	user	Not Specified	15m
profile-attribute	Profile attribute to retrieve from the RADIUS server.	option	-	Login-LAT-Service
	Option / **Description** *User-Name* — Use this attribute. *NAS-IP-Address* — Use this attribute. *Framed-IP-Address* — Use this attribute. *Framed-IP-Netmask* — Use this attribute. *Filter-Id* — Use this attribute. *Login-IP-Host* — Use this attribute. *Reply-Message* — Use this attribute.			

Parameter	Description	Type	Size	Default
	Option / **Description** *Callback-Number* — Use this attribute. *Callback-Id* — Use this attribute. *Framed-Route* — Use this attribute. *Framed-IPX-Network* — Use this attribute. *Class* — Use this attribute. *Called-Station-Id* — Use this attribute. *Calling-Station-Id* — Use this attribute. *NAS-Identifier* — Use this attribute. *Proxy-State* — Use this attribute. *Login-LAT-Service* — Use this attribute. *Login-LAT-Node* — Use this attribute. *Login-LAT-Group* — Use this attribute. *Framed-AppleTalk-Zone* — Use this attribute. *Acct-Session-Id* — Use this attribute. *Acct-Multi-Session-Id* — Use this attribute.			
ovrd-user-group `<name>`	User groups with permission to use the override. User group name.	string	Maximum length: 79	
profile `<name>`	Web filter profile with permission to create overrides. Web profile.	string	Maximum length: 79	

config web

Parameter	Description	Type	Size	Default
bword-threshold	Banned word score threshold.	integer	Minimum value: 0 Maximum value: 2147483647	10
bword-table	Banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
urlfilter-table	URL filter table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
content-header-list	Content header list.	integer	Minimum value: 0 Maximum value: 4294967295	0
blocklist	Enable/disable automatic addition of URLs detected by FortiSandbox to blocklist.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

allowlist	FortiGuard allowlist settings.	option	-	

Option	Description
exempt-av	Exempt antivirus.
exempt-webcontent	Exempt web content.
exempt-activex-java-cookie	Exempt ActiveX-JAVA-Cookie.
exempt-dlp	Exempt DLP.
exempt-rangeblock	Exempt RangeBlock.

Parameter	Description	Type	Size	Default
	Option / **Description** *extended-log-others* — Support extended log.			
safe-search	Safe search type.	option	-	
	Option / **Description** *url* — Insert safe search string into URL. *header* — Insert safe search header.			
youtube-restrict	YouTube EDU filter level.	option	-	none
	Option / **Description** *none* — Full access for YouTube. *strict* — Strict access for YouTube. *moderate* — Moderate access for YouTube.			
vimeo-restrict	Set Vimeo-restrict ("7" = don't show mature content, "134" = don't show unrated and mature content). A value of cookie "content_rating".	string	Maximum length: 63	
log-search	Enable/disable logging all search phrases.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
keyword-match `<pattern>`	Search keywords to log when match is found. Pattern/keyword to search for.	string	Maximum length: 79	

config ftgd-wf

Parameter	Description	Type	Size	Default
options	Options for FortiGuard Web Filter.	option	-	ftgd-disable
	Option / **Description** *error-allow* — Allow web pages with a rating error to pass through. *rate-server-ip* — Rate the server IP in addition to the domain name.			

Parameter	Description	Type	Size	Default
	Option / **Description** *connect-request-bypass* — Bypass connection which has CONNECT request. *ftgd-disable* — Disable FortiGuard scanning.			
exempt-quota	Do not stop quota for these categories.	user	Not Specified	17
ovrd	Allow web filter profile overrides.	user	Not Specified	
max-quota-timeout	Maximum FortiGuard quota used by single page view in seconds (excludes streams).	integer	Minimum value: 1 Maximum value: 86400	300
rate-javascript-urls	Enable/disable rating JavaScript by URL.	option	-	enable
	Option / **Description** *disable* — Disable rating JavaScript by URL. *enable* — Enable rating JavaScript by URL.			
rate-css-urls	Enable/disable rating CSS by URL.	option	-	enable
	Option / **Description** *disable* — Disable rating CSS by URL. *enable* — Enable rating CSS by URL.			
rate-crl-urls	Enable/disable rating CRL by URL.	option	-	enable
	Option / **Description** *disable* — Disable rating CRL by URL. *enable* — Enable rating CRL by URL.			

config filters

Parameter	Description	Type	Size	Default
category	Categories and groups the filter examines.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default
action	Action to take for matches.	option	-	monitor
	Option / **Description** *block* — Block access. *authenticate* — Authenticate user before allowing access. *monitor* — Allow access while logging the action. *warning* — Allow access after warning the user.			
warn-duration	Duration of warnings.	user	Not Specified	5m
auth-usr-grp <name>	Groups with permission to authenticate. User group name.	string	Maximum length: 79	
log	Enable/disable logging.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
override-replacemsg	Override replacement message.	string	Maximum length: 28	
warning-prompt	Warning prompts in each category or each domain.	option	-	per-category
	Option / **Description** *per-domain* — Per-domain warnings. *per-category* — Per-category warnings.			
warning-duration-type	Re-display warning after closing browser or after a timeout.	option	-	timeout
	Option / **Description** *session* — After session ends. *timeout* — After timeout occurs.			

config quota

Parameter	Description	Type	Size	Default
category	FortiGuard categories to apply quota to (category action must be set to monitor).	user	Not Specified	

Parameter	Description	Type	Size	Default
type	Quota type.	option	-	time
	Option / **Description** *time* — Use a time-based quota. *traffic* — Use a traffic-based quota.			
unit	Traffic quota unit of measurement.	option	-	MB
	Option / **Description** *B* — Quota in bytes. *KB* — Quota in kilobytes. *MB* — Quota in megabytes. *GB* — Quota in gigabytes.			
value	Traffic quota value.	integer	Minimum value: 1 Maximum value: 4294967295	1024
duration	Duration of quota.	user	Not Specified	5m
override-replacemsg	Override replacement message.	string	Maximum length: 28	

config antiphish

Parameter	Description	Type	Size	Default
status	Toggle AntiPhishing functionality.	option	-	disable
	Option / **Description** *enable* — Enable AntiPhishing functionality. *disable* — Disable AntiPhishing functionality.			
default-action	Action to be taken when there is no matching rule.	option	-	exempt
	Option / **Description** *exempt* — Exempt requests from matching. *log* — Log all matched requests. *block* — Block all matched requests.			

Parameter	Description	Type	Size	Default
check-uri	Enable/disable checking of GET URI parameters for known credentials.	option	-	disable

Option	Description
enable	Enable checking of GET URI for username and password fields.
disable	Disable checking of GET URI for username and password fields.

Parameter	Description	Type	Size	Default
check-basic-auth	Enable/disable checking of HTTP Basic Auth field for known credentials.	option	-	disable

Option	Description
enable	Enable checking of HTTP Basic Auth field for known credentials.
disable	Disable checking of HTTP Basic Auth field for known credentials.

Parameter	Description	Type	Size	Default
check-username-only	Enable/disable username only matching of credentials. Action will be taken for valid usernames regardless of password validity.	option	-	disable

Option	Description
enable	Enable username only credential matches.
disable	Disable username only credential matches.

Parameter	Description	Type	Size	Default
max-body-len	Maximum size of a POST body to check for credentials.	integer	Minimum value: 0 Maximum value: 4294967295	65536
authentication	Authentication methods.	option	-	domain-controller

Option	Description
domain-controller	Domain Controller to verify user credential.
ldap	LDAP to verify user credential.

Parameter	Description	Type	Size	Default
domain-controller	Domain for which to verify received credentials against.	string	Maximum length: 63	
ldap	LDAP server for which to verify received credentials against.	string	Maximum length: 63	

config inspection-entries

Parameter	Description	Type	Size	Default
fortiguard-category	FortiGuard category to match.	user	Not Specified	0
action	Action to be taken upon an AntiPhishing match.	option	-	exempt

Option	Description
exempt	Exempt requests from matching.
log	Log all matched requests.
block	Block all matched requests.

config custom-patterns

Parameter	Description	Type	Size	Default
category	Category that the pattern matches.	option	-	username

Option	Description
username	Pattern matches username fields.
password	Pattern matches password fields.

Parameter	Description	Type	Size	Default
type	Pattern will be treated either as a regex pattern or literal string.	option	-	regex

Option	Description
regex	Pattern will be treated as a regex pattern.
literal	Pattern will be treated as a literal string.

config webfilter search-engine

Configure web filter search engines.

```
config webfilter search-engine
    Description: Configure web filter search engines.
    edit <name>
        set hostname {string}
        set url {string}
        set query {string}
        set safesearch [disable|url|...]
        set charset [utf-8|gb2312]
        set source-url [enable|disable]
        set safesearch-str {string}
```

```
    next
end
```

config webfilter search-engine

Parameter	Description	Type	Size	Default
hostname	Hostname (regular expression).	string	Maximum length: 127	
url	URL (regular expression).	string	Maximum length: 127	
query	Code used to prefix a query (must end with an equals character).	string	Maximum length: 15	
safesearch	Safe search method. You can disable safe search, add the safe search string to URLs, or insert a safe search header.	option	-	disable

Option	Description
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).
translate	Perform URL FortiGuard check on HTTP requests parameter.
yt-pattern	Pattern to match YouTube channel ID.
yt-scan	Perform IPS scan.
yt-video	Pattern to match YouTube video name.
yt-channel	Pattern to match YouTube channel name.

charset	Search engine charset.	option	-	utf-8

Option	Description
utf-8	UTF-8 encoding.
gb2312	GB2312 encoding.

source-url	Enable/disable source url in the image search result.	option	-	disable

Option	Description
enable	Enable source url in image search.
disable	Disable source url in image search.

safesearch-str	Safe search parameter used in the URL.	string	Maximum length: 79	

config webfilter status

Display rating info.

```
config webfilter status
    Description: Display rating info.
    set <refresh-rate> {string}
end
```

config webfilter status

Parameter	Description	Type	Size	Default
<refresh-rate>	Frequency to refresh the server list (sec).	string	Maximum length: -1	

config webfilter urlfilter

Configure URL filter lists.

```
config webfilter urlfilter
    Description: Configure URL filter lists.
    edit <id>
        set name {string}
        set comment {var-string}
        set one-arm-ips-urlfilter [enable|disable]
        set ip-addr-block [enable|disable]
        config entries
            Description: URL filter entries.
            edit <id>
                set url {string}
                set type [simple|regex|...]
                set action [exempt|block|...]
                set antiphish-action [block|log]
                set status [enable|disable]
                set exempt {option1}, {option2}, ...
                set web-proxy-profile {string}
                set referrer-host {string}
                set dns-address-family [ipv4|ipv6|...]
            next
        end
    next
end
```

config webfilter urlfilter

Parameter	Description	Type	Size	Default
name	Name of URL filter list.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	
one-arm-ips-urlfilter	Enable/disable DNS resolver for one-arm IPS URL filter operation.	option	-	disable

Option	Description
enable	Enable DNS resolver for one-arm IPS URL filter operation.
disable	Disable DNS resolver for one-arm IPS URL filter operation.

Parameter	Description	Type	Size	Default
ip-addr-block	Enable/disable blocking URLs when the hostname appears as an IP address.	option	-	disable

Option	Description
enable	Enable blocking URLs when the hostname appears as an IP address.
disable	Disable blocking URLs when the hostname appears as an IP address.

config entries

Parameter	Description	Type	Size	Default
url	URL to be filtered.	string	Maximum length: 511	
type	Filter type (simple, regex, or wildcard).	option	-	simple

Option	Description
simple	Simple URL string.
regex	Regular expression URL string.
wildcard	Wildcard URL string.

Parameter	Description	Type	Size	Default
action	Action to take for URL filter matches.	option	-	exempt

Option	Description
exempt	Exempt matches.
block	Block matches.

Parameter	Description	Type	Size	Default
	Option / **Description** *allow* — Allow matches (no log). *monitor* — Allow matches (with log).			
antiphish-action	Action to take for AntiPhishing matches.	option	-	block
	Option / **Description** *block* — Block matches. *log* — Allow matches with log.			
status	Enable/disable this URL filter.	option	-	enable
	Option / **Description** *enable* — Enable this URL filter. *disable* — Disable this URL filter.			
exempt	If action is set to exempt, select the security profile operations that exempt URLs skip. Separate multiple options with a space.	option	-	av web-content activex-java-cookie dlp fortiguard range-block antiphish all
	Option / **Description** *av* — AntiVirus scanning. *web-content* — Web filter content matching. *activex-java-cookie* — ActiveX, Java, and cookie filtering. *dlp* — DLP scanning. *fortiguard* — FortiGuard web filtering. *range-block* — Range block feature. *pass* — Pass single connection from all. *antiphish* — AntiPhish credential checking. *all* — Exempt from all security profiles.			

Parameter	Description	Type	Size	Default
web-proxy-profile	Web proxy profile.	string	Maximum length: 63	
referrer-host	Referrer host name.	string	Maximum length: 255	
dns-address-family	Resolve IPv4 address, IPv6 address, or both from DNS server.	option	-	ipv4

Option	Description
ipv4	Resolve IPv4 address from DNS server.
ipv6	Resolve IPv6 address from DNS server.
both	Resolve both IPv4 and IPv6 addresses from DNS server.

www.fortinet.com