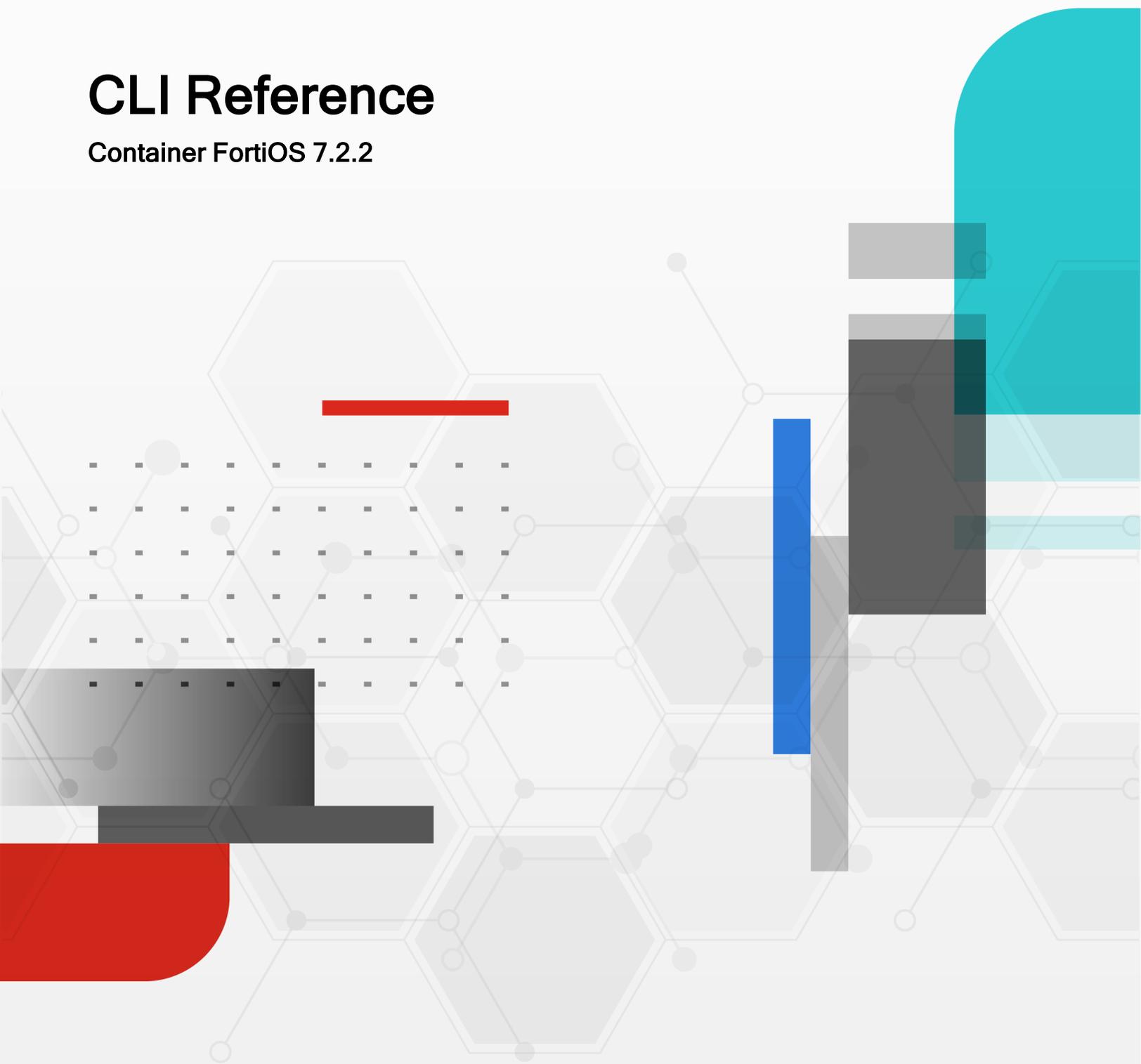


CLI Reference

Container FortiOS 7.2.2



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



July 25, 2025

Container FortiOS 7.2.2 CLI Reference

87-722-976874-20250725

TABLE OF CONTENTS

Change Log	5
Introduction	6
What's new	7
Using the command line interface	8
Connecting to the CLI	8
Command syntax	8
Notation	8
Optional values and ranges	9
CLI basics	9
Getting help	10
Shortcuts and key commands	10
Command abbreviation	11
Adding and removing options from lists	11
Environment variables	11
Special characters	11
Subcommands	12
next	13
end	13
Table subcommands	14
Field subcommands	15
CLI command reference	17
config	17
antivirus	18
application	34
firewall	46
ips	112
log	123
report	157
router	158
system	160
user	178
vpn	180
webfilter	190
diagnose	212
diagnose autoupdate versions	212
diagnose debug	212
diagnose router info routing-table all	214
diagnose sniffer packet	214
diagnose sys	215
diagnose test application	216
execute	219
Syntax	219
Commands	219
exit	220

Usage	220
get	220
show	221
sysctl sh	222

Change Log

Date	Change Description
2025-06-10	Initial release.
2025-07-25	Updated to remove unsupported IPv6 commands and settings.

Introduction

This document describes how to use the Container FortiOS command line interface (CLI) and contains references for Container FortiOS CLI commands.

The Container FortiOS CLI is similar to the FortiOS CLI. While much of the command syntax is the same, there are a limited number of commands available, reflecting the available Container FortiOS features.

What's new

The following table lists the CLI changes from the previous version:

Command	Change
<code>config user peer</code>	Command added.
<code>config user peergrp</code>	Command added.
<code>config system dns</code>	Parameters added: <ul style="list-style-type: none">• <code>dns-cache-ttl</code>• <code>fqdn-cache-ttl</code> Parameters removed: <ul style="list-style-type: none">• <code>primary</code>• <code>secondary</code>
<code>config vpn ipsec phase1-interface</code>	Parameter changed: <ul style="list-style-type: none">• <code>peertype</code> Parameters added: <ul style="list-style-type: none">• <code>peer</code>• <code>peergrp</code>
<code>config firewall address</code>	Parameter added: <ul style="list-style-type: none">• <code>cache-ttl</code>
<code>config vpn certificate ca</code>	Parameter changed: <ul style="list-style-type: none">• <code>name</code>

Using the command line interface

This chapter explains how to connect to the CLI and describes the basics of using the CLI to configure and manage a running Container FortiOS container.

This chapter describes:

- [Connecting to the CLI on page 8](#)
- [CLI basics on page 9](#)
- [Command syntax on page 8](#)
- [Subcommands on page 12](#)

Connecting to the CLI

To connect to the running Container FortiOS container:

1. In the host shell, enter the appropriate command for your platform:
 - LXC: `lxc-console -n <container_name>`
 - Docker: `docker exec -it <container_name> /bin/cli`
 - Kubernetes: `kubectl exec --stdin --tty <container_name> /bin/cli`
2. At the prompt, enter the username and password.
The default user is admin and the password is blank. See [config system admin on page 160](#).

Command syntax

When entering a command, the CLI console requires that you use valid syntax and conform to expected input constraints. It rejects invalid commands. Indentation is used to indicate the levels of nested commands.

Each command line consists of a command word, usually followed by configuration data or a specific item that the command uses or affects.

Notation

Brackets, vertical bars, and spaces are used to denote valid syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

All syntax uses the following conventions:

Angle brackets < >	Indicate a variable of the specified data type.
Curly brackets { }	Indicate that a variable or variables are mandatory.
Square brackets []	Indicate that the variable or variables are optional. For example: <code>show system interface [<name_str>]</code> To show the settings for all interfaces, you can enter <code>show system interface</code> To show the settings for the Port1 interface, you can enter <code>show system interface port1</code> .
Vertical bar 	A vertical bar separates alternative, mutually exclusive options. For example: <code>set protocol {ftp sftp}</code> You can enter either <code>set protocol ftp</code> or <code>set protocol sftp</code> .
Space	A space separates non-mutually exclusive options. For example: <code>set allowaccess {ping https ssh snmp http fgfm radius-acct probe-response capwap ftm}</code> You can enter any of the following: <code>set allowaccess ping</code> <code>set allowaccess https ping ssh</code> <code>set allowaccess http https snmp ssh ping</code> In most cases, to make changes to lists that contain options separated by spaces, you need to retype the entire list, including all the options that you want to apply and excluding all the options that you want to remove.

Optional values and ranges

Any field that is optional will use square-brackets. The overall config command will still be valid whether or not the option is configured.

Square-brackets can be used to show that multiple options can be set, even intermixed with ranges. The following example shows a field that can be set to either a specific value or range, or multiple instances:

```
config firewall service custom
  set iprange <range1> [<range2> <range3> ...]
end
```

CLI basics

This section describes the basic features and characteristics of the CLI environment.

Getting help

Press the question mark (?) key to display command help and complete commands.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Enter a command followed by a space and press the question mark (?) key to display a list of the options available for that command and a description of each option.
- Enter a command followed by an option and press the question mark (?) key to display a list of additional options available for that command option combination and a description of each option.
- Enter a question mark after entering a portion of a command to see a list of valid complete commands and their descriptions. If there is only one valid command, it will be automatically filled in.

Shortcuts and key commands

Shortcut key	Action
?	List valid complete or subsequent commands. If multiple commands can complete the command, they are listed with their descriptions.
Tab	Complete the word with the next available match. Press multiple times to cycle through available matches.
Up arrow or Ctrl + P	Recall the previous command. Command memory is limited to the current session.
Down arrow, or Ctrl + N	Recall the next command.
Left or Right arrow	Move the cursor left or right within the command line.
Ctrl + A	Move the cursor to the beginning of the command line.
Ctrl + E	Move the cursor to the end of the command line.
Ctrl + B	Move the cursor backwards one word.
Ctrl + F	Move the cursor forwards one word.
Ctrl + D	Delete the current character.
Ctrl + C	Abort current interactive commands, such as when entering multiple lines. If you are not currently within an interactive command such as <code>config</code> or <code>edit</code> , this closes the CLI connection.
\ then Enter	Continue typing a command on the next line for a multiline command. For each line that you want to continue, terminate it with a backslash (\). To complete the command, enter a space instead of a backslash, and then press <i>Enter</i> .

Command abbreviation

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

For example, the command `diagnose system status` could be abbreviated to `d sy s`.

Adding and removing options from lists

When configuring a list, the `set` command will remove the previous configuration.

For example, if a user group currently includes members A, B, and C, the command `set member D` will remove members A, B, and C. To avoid removing the existing members from the group, the command `set members A B C D` must be used.

To avoid this issue, the following commands are available:

append	Add an option to an existing list. For example, <code>append member D</code> adds user D to the user group without removing any of the existing members.
select	Clear all of the options except for those specified. For example, <code>select member B</code> removes all member from the group except for member B.
unselect	Remove an option from an existing list. For example, <code>unselect member C</code> removes only member C from the group, without affecting the other members.

Environment variables

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

\$USERFROM	The management access type (<code>ssh</code> , <code>jsconsole</code> , and so on) and the IPv4 address of the administrator that configured the item.
\$USERNAME	The account name of the administrator that configured the item.
\$SerialNum	The Container FortiOS serial number.

For example, to set the Container FortiOS host name to its serial number, use the following CLI command:

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

Special characters

The following characters cannot be used in most CLI commands: `<`, `>`, `(`, `)`, `#`, `'`, and `"`

If one of those characters, or a space, needs to be entered as part of a string, it can be entered by using a special command, enclosing the entire string in quotes, or preceding it with an escape character (backslash, \).

To enter a question mark (?) or a tab, *Ctrl + V* or *Ctrl + Shift + -* (depending on the method being used to access the CLI) must be entered first.



Question marks and tabs cannot be copied into the CLI Console or some SSH clients. They must be typed in.

Character	Keys
?	Ctrl + V or Ctrl + Shift + - then ?
Tab	Ctrl + V then Tab
Space (as part of a string value, not to end the string)	Enclose the string in single or double quotation marks: "Security Administrator" or 'Security Administrator'. Precede the space with a backslash: Security\ Administrator.
' (as part of a string value, not to begin or end the string)	\'
" (as part of a string value, not to begin or end the string)	\"
\	\\

Subcommands

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

```
config system fortiguard
```

the command prompt becomes:

```
(fortiguard)#
```

Applicable subcommands are available until you exit the command, or descend an additional level into another subcommand. Subcommand scope is indicated by indentation.

For example, the `edit` subcommand is only available in commands that affects tables, and the next subcommand is available only in the `edit` subcommand:

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

```
    next
end
```

The available subcommands vary by command. From a command prompt under the `config` command, subcommands that affect tables and fields could be available.

next

The `next` command is used to maintain a hierarchy and flow to CLI commands. It is at the same indentation level as the preceding `edit` command, to mark where a table entry finishes.

The following example shows the `next` command used in the subcommand entries:

```
config application list
  edit default
    config entries
      edit 1
        set action pass
      next
```

After configuring table entry `<1>` then entering `next`, the `<1>` table entry is saved and the console returns to the `entries` prompt:

```
(entries) #
```

You can now create more table entries as needed, or enter `end` to save the table and return to the `default` table element prompt.

end

The `end` command is used to maintain a hierarchy and flow to CLI commands.

The following example shows the same command and subcommand as the `next` command example, except `end` has been entered instead of `next` after the subcommand:

```
config application list
  edit default
    config entries
      edit 1
        set action pass
      end
```

Entering `end` will save the `<1>` table entry and the table, and exit the `entries` subcommand entirely. The console returns to the `default` table element prompt:

```
(default) #
```

Table subcommands

edit <table_row>

Create or edit a table value.

In objects such as security policies, <table_row> is a sequence number. To create a new table entry without accidentally editing an existing entry, enter `edit 0`. The CLI will confirm that creation of entry 0, but will assign the next unused number when the entry is saved after entering `end` or `next`.

For example, to create a new firewall policy, enter the following commands:

```
config firewall policy
  edit 0
  ...
  next
end
```

To edit an existing policy, enter the following commands:

```
config firewall policy
  edit 27
  ...
  next
end
```

The `edit` subcommand changes the command prompt to the name of the table value that is being edited, such as `(27) #`.

delete <table_row>

Delete a table value.

For example, to delete firewall policy 27, enter the following commands:

```
config firewall policy
  delete 27
end
```

purge

Clear all table values.

The `purge` command cannot be undone. To restore purged table values, the configuration must be restored from a backup.

move

Move an ordered table value.

In the firewall policy table, this is equivalent to dragging a policy into a new position. It does not change the policy's ID number.

For example, to move policy 27 to policy 30, enter the following commands:

```
config firewall policy
  move 27 to 30
end
```

The `move` subcommand is only available in tables where the order of the table entries matters.

clone <table_row> to <table_row>	<p>Make a clone of a table entry.</p> <p>For example, to create firewall policy 30 as a clone of policy 27, enter the following commands:</p> <pre>config firewall policy clone 27 to 30 end</pre> <p>The clone subcommand may not be available for all tables.</p>
rename <table_row> to <table_row>	<p>Rename a table entry.</p> <p>For example to rename an administrator from Fry to Leela, enter the following commands:</p> <pre>config system admin rename Fry to Leela end</pre> <p>The rename subcommand is only available in tables where the entries can be renamed.</p>
get	<p>List the current table entries.</p> <p>For example, to view the existing firewall policy table entries, enter the following commands:</p> <pre>config firewall policy get</pre>
show	<p>Show the configuration. Only table entries that are not set to default values are shown.</p>
end	<p>Save the configuration and exit the current config command.</p>



Purging the system interface or system admin tables does not reset default table values. You may be unable to connect to or log in to Container FortiOS.

Field subcommands

set <field> <value>	<p>Modify the value of a field.</p> <p>For example, the command set fsso enable sets the fsso field to the value enable.</p>
unset	<p>Set the field to its default value.</p>
clear	<p>Clear all the options from a multi-option table value.</p>
get	<p>List the configuration of the current table entry, including default and customized values.</p>

show	Show the configuration. Only values that are not set to default values are shown.
next	Save changes to the table entry and exit the <code>edit</code> command so that you can configure the next table entry.
abort	Exit the command without saving.
end	Save the configuration and exit the current <code>config</code> command.

CLI command reference

The following primary commands are available in Container FortiOS:

- [config on page 17](#)
- [diagnose on page 212](#)
- [execute on page 219](#)
- [exit on page 220](#)
- [get on page 220](#)
- [show on page 221](#)
- [sysctl sh on page 222](#)

config

Configure and manage Container FortiOS.

- [antivirus on page 18](#)
- [application on page 34](#)
- [firewall on page 46](#)
- [ips on page 112](#)
- [log on page 123](#)
- [report on page 157](#)
- [router on page 158](#)
- [system on page 160](#)
- [vpn on page 180](#)
- [webfilter on page 190](#)

antivirus

This section includes syntax for the following commands:

- [config antivirus profile on page 18](#)
- [config antivirus settings on page 32](#)

config antivirus profile

Configure AntiVirus profiles.

Syntax

```
config antivirus profile
  edit <name>
    set av-block-log [enable|disable]
    set av-virus-log [enable|disable]
    config cifs
      Description: Configure CIFS AntiVirus options.
      set archive-block {option1}, {option2}, ...
      set archive-log {option1}, {option2}, ...
      set av-scan [disable|block|...]
      set emulator [enable|disable]
    end
    set comment {var-string}
    set extended-log [enable|disable]
    config ftp
      Description: Configure FTP AntiVirus options.
      set archive-block {option1}, {option2}, ...
      set archive-log {option1}, {option2}, ...
      set av-scan [disable|block|...]
      set emulator [enable|disable]
    end
    config http
      Description: Configure HTTP AntiVirus options.
      set archive-block {option1}, {option2}, ...
      set archive-log {option1}, {option2}, ...
      set av-scan [disable|block|...]
      set emulator [enable|disable]
    end
    config imap
      Description: Configure IMAP AntiVirus options.
      set archive-block {option1}, {option2}, ...
      set archive-log {option1}, {option2}, ...
      set av-scan [disable|block|...]
      set emulator [enable|disable]
      set executables [default|virus]
    end
  end
```

```

config mapi
  Description: Configure MAPI AntiVirus options.
  set archive-block {option1}, {option2}, ...
  set archive-log {option1}, {option2}, ...
  set av-scan [disable|block|...]
  set emulator [enable|disable]
  set executables [default|virus]
end
config nntp
  Description: Configure NNTP AntiVirus options.
  set archive-block {option1}, {option2}, ...
  set archive-log {option1}, {option2}, ...
  set av-scan [disable|block|...]
  set emulator [enable|disable]
end
config pop3
  Description: Configure POP3 AntiVirus options.
  set archive-block {option1}, {option2}, ...
  set archive-log {option1}, {option2}, ...
  set av-scan [disable|block|...]
  set emulator [enable|disable]
  set executables [default|virus]
end
set replacemsg-group {string}
config smtp
  Description: Configure SMTP AntiVirus options.
  set archive-block {option1}, {option2}, ...
  set archive-log {option1}, {option2}, ...
  set av-scan [disable|block|...]
  set emulator [enable|disable]
  set executables [default|virus]
end
config ssh
  Description: Configure SFTP and SCP AntiVirus options.
  set archive-block {option1}, {option2}, ...
  set archive-log {option1}, {option2}, ...
  set av-scan [disable|block|...]
  set emulator [enable|disable]
end
next
end

```

Parameters

Parameter	Description	Type	Size	Default
av-block-log	Enable/disable logging for AntiVirus file blocking.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
av-virus-log	Enable/disable AntiVirus logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
comment	Comment.	var-string	Maximum length: 255							
extended-log	Enable/disable extended logging for antivirus.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
name	Profile name.	string	Maximum length: 35							
replacemsg-group	Replacement message group customized for this profile.	string	Maximum length: 35							

config cifs

Parameter	Description	Type	Size	Default																		
archive-block	Select the archive types to block.	option	-																			
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Block encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Block corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Block partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Block multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Block nested archives that exceed uncompressed nest limit.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Block mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Block exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Block scan timeout.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Block mail bomb archives.	<i>fileslimit</i>	Block exceeded archive files limit.	<i>timeout</i>	Block scan timeout.			
Option	Description																					
<i>encrypted</i>	Block encrypted archives.																					
<i>corrupted</i>	Block corrupted archives.																					
<i>partiallycorrupted</i>	Block partially corrupted archives.																					
<i>multipart</i>	Block multipart archives.																					
<i>nested</i>	Block nested archives that exceed uncompressed nest limit.																					
<i>mailbomb</i>	Block mail bomb archives.																					
<i>fileslimit</i>	Block exceeded archive files limit.																					
<i>timeout</i>	Block scan timeout.																					

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

config ftp

Parameter	Description	Type	Size	Default						
archive-block	Select the archive types to block.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Block encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Block corrupted archives.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.			
Option	Description									
<i>encrypted</i>	Block encrypted archives.									
<i>corrupted</i>	Block corrupted archives.									

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

config http

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

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.			
Option	Description									
<i>enable</i>	Enable the virus emulator.									
<i>disable</i>	Disable the virus emulator.									

config imap

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

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>block</i></td> <td>Block the virus infected files.</td> </tr> <tr> <td><i>monitor</i></td> <td>Log the virus infected files.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the virus infected files.	<i>monitor</i>	Log the virus infected files.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the virus infected files.											
<i>monitor</i>	Log the virus infected files.											
emulator	Enable/disable the virus emulator.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.					
Option	Description											
<i>enable</i>	Enable the virus emulator.											
<i>disable</i>	Disable the virus emulator.											
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Perform standard AntiVirus scanning of Windows executable files.</td> </tr> <tr> <td><i>virus</i></td> <td>Treat Windows executables as viruses.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.					
Option	Description											
<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.											
<i>virus</i>	Treat Windows executables as viruses.											

config mapi

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

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Log encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Log corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Log partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Log multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Log nested archives that exceed uncompressed nest limit.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Log mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Log exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Log scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Log archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>fileslimit</i>	Log exceeded archive files limit.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Log encrypted archives.																							
<i>corrupted</i>	Log corrupted archives.																							
<i>partiallycorrupted</i>	Log partially corrupted archives.																							
<i>multipart</i>	Log multipart archives.																							
<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																							
<i>mailbomb</i>	Log mail bomb archives.																							
<i>fileslimit</i>	Log exceeded archive files limit.																							
<i>timeout</i>	Log scan timeout.																							
<i>unhandled</i>	Log archives that FortiOS cannot open.																							
av-scan	Enable AntiVirus scan service.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>block</i></td> <td>Block the virus infected files.</td> </tr> <tr> <td><i>monitor</i></td> <td>Log the virus infected files.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the virus infected files.	<i>monitor</i>	Log the virus infected files.															
Option	Description																							
<i>disable</i>	Disable.																							
<i>block</i>	Block the virus infected files.																							
<i>monitor</i>	Log the virus infected files.																							
emulator	Enable/disable the virus emulator.	option	-	enable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.																	
Option	Description																							
<i>enable</i>	Enable the virus emulator.																							
<i>disable</i>	Disable the virus emulator.																							
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Perform standard AntiVirus scanning of Windows executable files.</td> </tr> <tr> <td><i>virus</i></td> <td>Treat Windows executables as viruses.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.																	
Option	Description																							
<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.																							
<i>virus</i>	Treat Windows executables as viruses.																							

config nntp

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

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

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.			
Option	Description									
<i>enable</i>	Enable the virus emulator.									
<i>disable</i>	Disable the virus emulator.									

config pop3

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

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>block</i></td> <td>Block the virus infected files.</td> </tr> <tr> <td><i>monitor</i></td> <td>Log the virus infected files.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the virus infected files.	<i>monitor</i>	Log the virus infected files.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the virus infected files.											
<i>monitor</i>	Log the virus infected files.											
emulator	Enable/disable the virus emulator.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.					
Option	Description											
<i>enable</i>	Enable the virus emulator.											
<i>disable</i>	Disable the virus emulator.											
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Perform standard AntiVirus scanning of Windows executable files.</td> </tr> <tr> <td><i>virus</i></td> <td>Treat Windows executables as viruses.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.					
Option	Description											
<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.											
<i>virus</i>	Treat Windows executables as viruses.											

config smtp

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

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Log encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Log corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Log partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Log multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Log nested archives that exceed uncompressed nest limit.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Log mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Log exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Log scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Log archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>fileslimit</i>	Log exceeded archive files limit.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Log encrypted archives.																							
<i>corrupted</i>	Log corrupted archives.																							
<i>partiallycorrupted</i>	Log partially corrupted archives.																							
<i>multipart</i>	Log multipart archives.																							
<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																							
<i>mailbomb</i>	Log mail bomb archives.																							
<i>fileslimit</i>	Log exceeded archive files limit.																							
<i>timeout</i>	Log scan timeout.																							
<i>unhandled</i>	Log archives that FortiOS cannot open.																							
av-scan	Enable AntiVirus scan service.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>block</i></td> <td>Block the virus infected files.</td> </tr> <tr> <td><i>monitor</i></td> <td>Log the virus infected files.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the virus infected files.	<i>monitor</i>	Log the virus infected files.															
Option	Description																							
<i>disable</i>	Disable.																							
<i>block</i>	Block the virus infected files.																							
<i>monitor</i>	Log the virus infected files.																							
emulator	Enable/disable the virus emulator.	option	-	enable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.																	
Option	Description																							
<i>enable</i>	Enable the virus emulator.																							
<i>disable</i>	Disable the virus emulator.																							
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Perform standard AntiVirus scanning of Windows executable files.</td> </tr> <tr> <td><i>virus</i></td> <td>Treat Windows executables as viruses.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.																	
Option	Description																							
<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.																							
<i>virus</i>	Treat Windows executables as viruses.																							

config ssh

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

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

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.			
Option	Description									
<i>enable</i>	Enable the virus emulator.									
<i>disable</i>	Disable the virus emulator.									

config antivirus settings

Configure AntiVirus settings.

Syntax

```
config antivirus settings
  set grayware [enable|disable]
  set machine-learning-detection [enable|monitor|...]
  set override-timeout {integer}
  set use-extreme-db [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default								
grayware	Enable/disable grayware detection when an AntiVirus profile is applied to traffic.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable grayware detection.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable grayware detection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable grayware detection.	<i>disable</i>	Disable grayware detection.					
Option	Description											
<i>enable</i>	Enable grayware detection.											
<i>disable</i>	Disable grayware detection.											
machine-learning-detection	Use machine learning based malware detection.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable machine learning based malware detection.</td> </tr> <tr> <td><i>monitor</i></td> <td>Enable machine learning based malware detection for monitoring only.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable machine learning based malware detection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable machine learning based malware detection.	<i>monitor</i>	Enable machine learning based malware detection for monitoring only.	<i>disable</i>	Disable machine learning based malware detection.			
Option	Description											
<i>enable</i>	Enable machine learning based malware detection.											
<i>monitor</i>	Enable machine learning based malware detection for monitoring only.											
<i>disable</i>	Disable machine learning based malware detection.											
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								

Parameter	Description	Type	Size	Default						
use-extreme-db	Enable/disable the use of Extreme AVDB.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable extreme AVDB.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable extreme AVDB.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable extreme AVDB.	<i>disable</i>	Disable extreme AVDB.			
Option	Description									
<i>enable</i>	Enable extreme AVDB.									
<i>disable</i>	Disable extreme AVDB.									

application

This section includes syntax for the following commands:

- [config application group on page 34](#)
- [config application list on page 35](#)
- [config application name on page 44](#)

config application group

Configure firewall application groups.

Syntax

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

Parameters

Parameter	Description	Type	Size	Default
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
behavior	Application behavior filter.	user	Not Specified	all
category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default												
comment	Comment	var-string	Maximum length: 255													
name	Application group name.	string	Maximum length: 63													
popularity	Application popularity filter.	option	-	1 2 3 4 5												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Popularity level 1.</td> </tr> <tr> <td>2</td> <td>Popularity level 2.</td> </tr> <tr> <td>3</td> <td>Popularity level 3.</td> </tr> <tr> <td>4</td> <td>Popularity level 4.</td> </tr> <tr> <td>5</td> <td>Popularity level 5.</td> </tr> </tbody> </table>	Option	Description	1	Popularity level 1.	2	Popularity level 2.	3	Popularity level 3.	4	Popularity level 4.	5	Popularity level 5.			
Option	Description															
1	Popularity level 1.															
2	Popularity level 2.															
3	Popularity level 3.															
4	Popularity level 4.															
5	Popularity level 5.															
protocols	Application protocol filter.	user	Not Specified	all												
risk <level>	<p>Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).</p> <p>Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).</p>	integer	Minimum value: 0 Maximum value: 4294967295													
technology	Application technology filter.	user	Not Specified	all												
type	Application group type.	option	-	application												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>application</i></td> <td>Application ID.</td> </tr> <tr> <td><i>filter</i></td> <td>Application filter.</td> </tr> </tbody> </table>	Option	Description	<i>application</i>	Application ID.	<i>filter</i>	Application filter.									
Option	Description															
<i>application</i>	Application ID.															
<i>filter</i>	Application filter.															
vendor	Application vendor filter.	user	Not Specified	all												

config application list

Configure application control lists.

Syntax

```

config application list
  edit <name>
    set app-replacemsg [disable|enable]
    set comment {var-string}
    set control-default-network-services [disable|enable]
  
```

```

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

```

```

set options {option1}, {option2}, ...
set other-application-action [pass|block]
set other-application-log [disable|enable]
set p2p-block-list {option1}, {option2}, ...
set replacemsg-group {string}
set unknown-application-action [pass|block]
set unknown-application-log [disable|enable]
next
end

```

Parameters

Parameter	Description	Type	Size	Default						
app-replacemsg	Enable/disable replacement messages for blocked applications.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable replacement messages for blocked applications.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable replacement messages for blocked applications.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable replacement messages for blocked applications.	<i>enable</i>	Enable replacement messages for blocked applications.			
Option	Description									
<i>disable</i>	Disable replacement messages for blocked applications.									
<i>enable</i>	Enable replacement messages for blocked applications.									
comment	comments	var-string	Maximum length: 255							
control-default-network-services	Enable/disable enforcement of protocols over selected ports.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable protocol enforcement over selected ports.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable protocol enforcement over selected ports.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable protocol enforcement over selected ports.	<i>enable</i>	Enable protocol enforcement over selected ports.			
Option	Description									
<i>disable</i>	Disable protocol enforcement over selected ports.									
<i>enable</i>	Enable protocol enforcement over selected ports.									
deep-app-inspection	Enable/disable deep application inspection.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable deep application inspection.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable deep application inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable deep application inspection.	<i>enable</i>	Enable deep application inspection.			
Option	Description									
<i>disable</i>	Disable deep application inspection.									
<i>enable</i>	Enable deep application inspection.									
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-	disable						

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable default application port enforcement.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable default application port enforcement.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable default application port enforcement.	<i>enable</i>	Enable default application port enforcement.									
Option	Description															
<i>disable</i>	Disable default application port enforcement.															
<i>enable</i>	Enable default application port enforcement.															
extended-log	Enable/disable extended logging.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
force-inclusion-ssl-di-sigs	Enable/disable forced inclusion of SSL deep inspection signatures.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable forced inclusion of signatures which normally require SSL deep inspection.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable forced inclusion of signatures which normally require SSL deep inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable forced inclusion of signatures which normally require SSL deep inspection.	<i>enable</i>	Enable forced inclusion of signatures which normally require SSL deep inspection.									
Option	Description															
<i>disable</i>	Disable forced inclusion of signatures which normally require SSL deep inspection.															
<i>enable</i>	Enable forced inclusion of signatures which normally require SSL deep inspection.															
name	List name.	string	Maximum length: 35													
options	Basic application protocol signatures allowed by default.	option	-	allow-dns												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow-dns</i></td> <td>Allow DNS.</td> </tr> <tr> <td><i>allow-icmp</i></td> <td>Allow ICMP.</td> </tr> <tr> <td><i>allow-http</i></td> <td>Allow generic HTTP web browsing.</td> </tr> <tr> <td><i>allow-ssl</i></td> <td>Allow generic SSL communication.</td> </tr> <tr> <td><i>allow-quic</i></td> <td>Allow QUIC.</td> </tr> </tbody> </table>	Option	Description	<i>allow-dns</i>	Allow DNS.	<i>allow-icmp</i>	Allow ICMP.	<i>allow-http</i>	Allow generic HTTP web browsing.	<i>allow-ssl</i>	Allow generic SSL communication.	<i>allow-quic</i>	Allow QUIC.			
Option	Description															
<i>allow-dns</i>	Allow DNS.															
<i>allow-icmp</i>	Allow ICMP.															
<i>allow-http</i>	Allow generic HTTP web browsing.															
<i>allow-ssl</i>	Allow generic SSL communication.															
<i>allow-quic</i>	Allow QUIC.															
other-application-action	Action for other applications.	option	-	pass												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Allow sessions matching an application in this application list.</td> </tr> <tr> <td><i>block</i></td> <td>Block sessions matching an application in this application list.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Allow sessions matching an application in this application list.	<i>block</i>	Block sessions matching an application in this application list.									
Option	Description															
<i>pass</i>	Allow sessions matching an application in this application list.															
<i>block</i>	Block sessions matching an application in this application list.															

Parameter	Description	Type	Size	Default								
other-application-log	Enable/disable logging for other applications.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging for other applications.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging for other applications.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging for other applications.	<i>enable</i>	Enable logging for other applications.					
Option	Description											
<i>disable</i>	Disable logging for other applications.											
<i>enable</i>	Enable logging for other applications.											
p2p-block-list	P2P applications to be blocklisted.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>skype</i></td> <td>Skype.</td> </tr> <tr> <td><i>edonkey</i></td> <td>Edonkey.</td> </tr> <tr> <td><i>bittorrent</i></td> <td>Bit torrent.</td> </tr> </tbody> </table>	Option	Description	<i>skype</i>	Skype.	<i>edonkey</i>	Edonkey.	<i>bittorrent</i>	Bit torrent.			
Option	Description											
<i>skype</i>	Skype.											
<i>edonkey</i>	Edonkey.											
<i>bittorrent</i>	Bit torrent.											
replacemsg-group	Replacement message group.	string	Maximum length: 35									
unknown-application-action	Pass or block traffic from unknown applications.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Pass or allow unknown applications.</td> </tr> <tr> <td><i>block</i></td> <td>Drop or block unknown applications.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Pass or allow unknown applications.	<i>block</i>	Drop or block unknown applications.					
Option	Description											
<i>pass</i>	Pass or allow unknown applications.											
<i>block</i>	Drop or block unknown applications.											
unknown-application-log	Enable/disable logging for unknown applications.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging for unknown applications.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging for unknown applications.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging for unknown applications.	<i>enable</i>	Enable logging for unknown applications.					
Option	Description											
<i>disable</i>	Disable logging for unknown applications.											
<i>enable</i>	Enable logging for unknown applications.											

config default-network-services

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

Parameter	Description	Type	Size	Default																								
port	Port number.	integer	Minimum value: 0 Maximum value: 65535	0																								
services	Network protocols.	option	-																									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>http</i></td> <td>HTTP.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH.</td> </tr> <tr> <td><i>telnet</i></td> <td>TELNET.</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP.</td> </tr> <tr> <td><i>dns</i></td> <td>DNS.</td> </tr> <tr> <td><i>smtp</i></td> <td>SMTP.</td> </tr> <tr> <td><i>pop3</i></td> <td>POP3.</td> </tr> <tr> <td><i>imap</i></td> <td>IMAP.</td> </tr> <tr> <td><i>snmp</i></td> <td>SNMP.</td> </tr> <tr> <td><i>nntp</i></td> <td>NNTP.</td> </tr> <tr> <td><i>https</i></td> <td>HTTPS.</td> </tr> </tbody> </table>	Option	Description	<i>http</i>	HTTP.	<i>ssh</i>	SSH.	<i>telnet</i>	TELNET.	<i>ftp</i>	FTP.	<i>dns</i>	DNS.	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>imap</i>	IMAP.	<i>snmp</i>	SNMP.	<i>nntp</i>	NNTP.	<i>https</i>	HTTPS.			
Option	Description																											
<i>http</i>	HTTP.																											
<i>ssh</i>	SSH.																											
<i>telnet</i>	TELNET.																											
<i>ftp</i>	FTP.																											
<i>dns</i>	DNS.																											
<i>smtp</i>	SMTP.																											
<i>pop3</i>	POP3.																											
<i>imap</i>	IMAP.																											
<i>snmp</i>	SNMP.																											
<i>nntp</i>	NNTP.																											
<i>https</i>	HTTPS.																											
violation-action	Action for protocols not in the allowlist for selected port.	option	-	block																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Allow protocols not in the allowlist for selected port.</td> </tr> <tr> <td><i>monitor</i></td> <td>Monitor protocols not in the allowlist for selected port.</td> </tr> <tr> <td><i>block</i></td> <td>Block protocols not in the allowlist for selected port.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Allow protocols not in the allowlist for selected port.	<i>monitor</i>	Monitor protocols not in the allowlist for selected port.	<i>block</i>	Block protocols not in the allowlist for selected port.																			
Option	Description																											
<i>pass</i>	Allow protocols not in the allowlist for selected port.																											
<i>monitor</i>	Monitor protocols not in the allowlist for selected port.																											
<i>block</i>	Block protocols not in the allowlist for selected port.																											

config entries

Parameter	Description	Type	Size	Default								
action	Pass or block traffic, or reset connection for traffic from this application.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Pass or allow matching traffic.</td> </tr> <tr> <td><i>block</i></td> <td>Block or drop matching traffic.</td> </tr> <tr> <td><i>reset</i></td> <td>Reset sessions for matching traffic.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Pass or allow matching traffic.	<i>block</i>	Block or drop matching traffic.	<i>reset</i>	Reset sessions for matching traffic.			
Option	Description											
<i>pass</i>	Pass or allow matching traffic.											
<i>block</i>	Block or drop matching traffic.											
<i>reset</i>	Reset sessions for matching traffic.											

Parameter	Description	Type	Size	Default						
application <id>	ID of allowed applications. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295							
behavior	Application behavior filter.	user	Not Specified	all						
category <id>	Category ID list. Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295							
exclusion <id>	ID of excluded applications. Excluded application IDs.	integer	Minimum value: 0 Maximum value: 4294967295							
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
log	Enable/disable logging for this application list.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging.	<i>enable</i>	Enable logging.			
Option	Description									
<i>disable</i>	Disable logging.									
<i>enable</i>	Enable logging.									
log-packet	Enable/disable packet logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable packet logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable packet logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable packet logging.	<i>enable</i>	Enable packet logging.			
Option	Description									
<i>disable</i>	Disable packet logging.									
<i>enable</i>	Enable packet logging.									
per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35							
popularity	Application popularity filter.	option	-	1 2 3 4 5						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>1</i></td> <td>Popularity level 1.</td> </tr> <tr> <td><i>2</i></td> <td>Popularity level 2.</td> </tr> </tbody> </table>	Option	Description	<i>1</i>	Popularity level 1.	<i>2</i>	Popularity level 2.			
Option	Description									
<i>1</i>	Popularity level 1.									
<i>2</i>	Popularity level 2.									

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>Popularity level 3.</td> </tr> <tr> <td>4</td> <td>Popularity level 4.</td> </tr> <tr> <td>5</td> <td>Popularity level 5.</td> </tr> </tbody> </table>	Option	Description	3	Popularity level 3.	4	Popularity level 4.	5	Popularity level 5.			
Option	Description											
3	Popularity level 3.											
4	Popularity level 4.											
5	Popularity level 5.											
protocols	Application protocol filter.	user	Not Specified	all								
quarantine	Quarantine method.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Quarantine is disabled.</td> </tr> <tr> <td><i>attacker</i></td> <td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.					
Option	Description											
<i>none</i>	Quarantine is disabled.											
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.											
quarantine-expiry	Duration of quarantine. Requires quarantine set to attacker.	user	Not Specified	5m								
quarantine-log	Enable/disable quarantine logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable quarantine logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable quarantine logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable quarantine logging.	<i>enable</i>	Enable quarantine logging.					
Option	Description											
<i>disable</i>	Disable quarantine logging.											
<i>enable</i>	Enable quarantine logging.											
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								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>periodical</i></td> <td>Allow configured number of packets every rate-duration.</td> </tr> <tr> <td><i>continuous</i></td> <td>Block packets once the rate is reached.</td> </tr> </tbody> </table>	Option	Description	<i>periodical</i>	Allow configured number of packets every rate-duration.	<i>continuous</i>	Block packets once the rate is reached.					
Option	Description											
<i>periodical</i>	Allow configured number of packets every rate-duration.											
<i>continuous</i>	Block packets once the rate is reached.											
rate-track	Track the packet protocol field.	option	-	none								

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>none</td> </tr> <tr> <td><i>src-ip</i></td> <td>Source IP.</td> </tr> <tr> <td><i>dest-ip</i></td> <td>Destination IP.</td> </tr> <tr> <td><i>dhcp-client-mac</i></td> <td>DHCP client.</td> </tr> <tr> <td><i>dns-domain</i></td> <td>DNS domain.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	none	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.	<i>dhcp-client-mac</i>	DHCP client.	<i>dns-domain</i>	DNS domain.			
Option	Description															
<i>none</i>	none															
<i>src-ip</i>	Source IP.															
<i>dest-ip</i>	Destination IP.															
<i>dhcp-client-mac</i>	DHCP client.															
<i>dns-domain</i>	DNS domain.															
risk <level>	<p>Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).</p> <p>Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).</p>	integer	Minimum value: 0 Maximum value: 4294967295													
session-ttl	Session TTL.	integer	Minimum value: 0 Maximum value: 4294967295	0												
shaper	Traffic shaper.	string	Maximum length: 35													
shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35													
technology	Application technology filter.	user	Not Specified	all												
vendor	Application vendor filter.	user	Not Specified	all												

config parameters

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

config members

Parameter	Description	Type	Size	Default
id	Parameter.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Parameter name.	string	Maximum length: 31	
value	Parameter value.	string	Maximum length: 199	

config application name

Configure application signatures. Read-only.

This table cannot be edited.

Syntax

```
config application name
  edit <name>
    get
  next
end
```

Parameters

Parameter	Description	Type	Size	Default
behavior	Application behavior.	user	Not Specified	
category	Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
id	Application ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Application name.	string	Maximum length: 63	

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

firewall

This section includes syntax for the following commands:

- [config firewall address on page 46](#)
- [config firewall addrgrp on page 47](#)
- [config firewall central-snat-map on page 48](#)
- [config firewall policy on page 50](#)
- [config firewall profile-protocol-options on page 53](#)
- [config firewall schedule group on page 75](#)
- [config firewall schedule onetime on page 75](#)
- [config firewall schedule recurring on page 76](#)
- [config firewall security-policy on page 77](#)
- [config firewall service category on page 81](#)
- [config firewall service custom on page 82](#)
- [config firewall service group on page 84](#)
- [config firewall ssl-ssh-profile on page 85](#)
- [config firewall vip on page 109](#)
- [config firewall wildcard-fqdn custom on page 111](#)

config firewall address

Configure IPv4 addresses.

Syntax

```
config firewall address
  edit <name>
    set cache-ttl {integer}
    set comment {var-string}
    set end-ip {ipv4-address-any}
    set fqdn {string}
    set start-ip {ipv4-address-any}
    set subnet {ipv4-classnet-any}
    set type [ipmask|iprange]
  next
end
```

Parameters

Parameter	Description	Type	Size	Default
cache-ttl	Defines the minimal TTL of individual IP addresses in FQDN cache measured in seconds.	integer	Minimum value: 0 Maximum value: 86400	0
comment	Comment.	var-string	Maximum length: 255	
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	
name	Address name.	string	Maximum length: 79	
start-ip	First IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0
subnet	IP address and subnet mask of address.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
type	Type of address.	option	-	ipmask

Option	Description
<i>ipmask</i>	Standard IPv4 address with subnet mask.
<i>iprange</i>	Range of IPv4 addresses between two specified addresses (inclusive).

config firewall addrgrp

Configure IPv4 address groups.

Syntax

```
config firewall addrgrp
  edit <name>
    set category [default|ztna-ems-tag|...]
    set comment {var-string}
    set exclude [enable|disable]
    set exclude-member <name1>, <name2>, ...
    set member <name1>, <name2>, ...
```

```

set type [default|folder]
next
end

```

Parameters

Parameter	Description	Type	Size	Default								
category	Address group category.	option	-	default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Default address group category (cannot be used as ztna-ems-tag/ztna-geo-tag in policy).</td> </tr> <tr> <td><i>ztna-ems-tag</i></td> <td>Members must be ztna-ems-tag group or ems-tag address, can be used as ztna-ems-tag in policy.</td> </tr> <tr> <td><i>ztna-geo-tag</i></td> <td>Members must be ztna-geo-tag group or geographic address, can be used as ztna-geo-tag in policy.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Default address group category (cannot be used as ztna-ems-tag/ztna-geo-tag in policy).	<i>ztna-ems-tag</i>	Members must be ztna-ems-tag group or ems-tag address, can be used as ztna-ems-tag in policy.	<i>ztna-geo-tag</i>	Members must be ztna-geo-tag group or geographic address, can be used as ztna-geo-tag in policy.			
Option	Description											
<i>default</i>	Default address group category (cannot be used as ztna-ems-tag/ztna-geo-tag in policy).											
<i>ztna-ems-tag</i>	Members must be ztna-ems-tag group or ems-tag address, can be used as ztna-ems-tag in policy.											
<i>ztna-geo-tag</i>	Members must be ztna-geo-tag group or geographic address, can be used as ztna-geo-tag in policy.											
comment	Comment.	var-string	Maximum length: 255									
exclude	Enable/disable address exclusion.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable address exclusion.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable address exclusion.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable address exclusion.	<i>disable</i>	Disable address exclusion.					
Option	Description											
<i>enable</i>	Enable address exclusion.											
<i>disable</i>	Disable address exclusion.											
exclude-member <name>	Address exclusion member. Address name.	string	Maximum length: 79									
member <name>	Address objects contained within the group. Address name.	string	Maximum length: 79									
name	Address group name.	string	Maximum length: 79									
type	Address group type.	option	-	default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Default address group type (address may belong to multiple groups).</td> </tr> <tr> <td><i>folder</i></td> <td>Address folder group (members may not belong to any other group).</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Default address group type (address may belong to multiple groups).	<i>folder</i>	Address folder group (members may not belong to any other group).					
Option	Description											
<i>default</i>	Default address group type (address may belong to multiple groups).											
<i>folder</i>	Address folder group (members may not belong to any other group).											

config firewall central-snat-map

Configure IPv4 central SNAT policies.

Syntax

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

config firewall central-snat-map

Parameter	Description	Type	Size	Default						
comments	Comment.	var-string	Maximum length: 1023							
dst-addr <name>	IPv4 Destination address. Address name.	string	Maximum length: 79							
dstintf <name>	Destination interface name from available interfaces. Interface name.	string	Maximum length: 79							
nat	Enable/disable source NAT.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable source NAT.</td></tr><tr><td><i>enable</i></td><td>Enable source NAT.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable source NAT.	<i>enable</i>	Enable source NAT.			
Option	Description									
<i>disable</i>	Disable source NAT.									
<i>enable</i>	Enable source NAT.									
nat-ippool <name>	Name of the IP pools to be used to translate addresses from available IP Pools. IP pool name.	string	Maximum length: 79							
nat-port	Translated port or port range (1 to 65535, 0 means any port).	user	Not Specified							
orig-addr <name>	IPv4 Original address. Address name.	string	Maximum length: 79							
orig-port	Original TCP port (1 to 65535, 0 means any port).	user	Not Specified							

Parameter	Description	Type	Size	Default						
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
protocol	Integer value for the protocol type.	integer	Minimum value: 0 Maximum value: 255	0						
srcintf <name>	Source interface name from available interfaces. Interface name.	string	Maximum length: 79							
status	Enable/disable the active status of this policy.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this policy.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.		
Option	Description									
<i>enable</i>	Enable this policy.									
<i>disable</i>	Disable this policy.									
type	IPv4 source NAT.	option	-	ipv4						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipv4</i></td> <td>Perform IPv4 source NAT.</td> </tr> </tbody> </table>		Option	Description	<i>ipv4</i>	Perform IPv4 source NAT.				
Option	Description									
<i>ipv4</i>	Perform IPv4 source NAT.									

config firewall policy

Configure policies.

Syntax

```

config firewall policy
  edit <policyid>
    set action [accept|deny]
    set application-list {string}
    set av-profile {string}
    set comments {var-string}
    set custom-log-fields <field-id1>, <field-id2>, ...
    set dstaddr <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set ips-sensor {string}
    set logtraffic [all|utm|...]
    set name {string}
    set nat [enable|disable]
    set profile-group {string}
    set profile-protocol-options {string}
    set profile-type [single|group]

```

```

set service <name1>, <name2>, ...
set srcaddr <name1>, <name2>, ...
set srcintf <name1>, <name2>, ...
set ssl-ssh-profile {string}
set status [enable|disable]
set utm-status [enable|disable]
set webfilter-profile {string}
next
end

```

Parameters

Parameter	Description	Type	Size	Default								
action	Policy action (accept/deny).	option	-	accept								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accept</i></td> <td>Allows session that match the firewall policy.</td> </tr> <tr> <td><i>deny</i></td> <td>Blocks sessions that match the firewall policy.</td> </tr> </tbody> </table>	Option	Description	<i>accept</i>	Allows session that match the firewall policy.	<i>deny</i>	Blocks sessions that match the firewall policy.					
Option	Description											
<i>accept</i>	Allows session that match the firewall policy.											
<i>deny</i>	Blocks sessions that match the firewall policy.											
application-list	Name of an existing Application list.	string	Maximum length: 35									
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35									
comments	Comment.	var-string	Maximum length: 1023									
custom-log-fields <field-id>	Custom fields to append to log messages for this policy. Custom log field.	string	Maximum length: 35									
dstaddr <name>	Destination IPv4 address and address group names. Address name.	string	Maximum length: 79									
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79									
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35									
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>all</i></td> <td>Log all sessions accepted or denied by this policy.</td> </tr> <tr> <td><i>utm</i></td> <td>Log traffic that has a security profile applied to it.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable all logging for this policy.</td> </tr> </tbody> </table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.			
Option	Description											
<i>all</i>	Log all sessions accepted or denied by this policy.											
<i>utm</i>	Log traffic that has a security profile applied to it.											
<i>disable</i>	Disable all logging for this policy.											

Parameter	Description	Type	Size	Default						
name	Policy name.	string	Maximum length: 35							
nat	Enable/disable source NAT.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
policyid	Policy ID.	integer	Minimum value: 1 Maximum value: 65535	1						
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						
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>single</i></td> <td>Do not allow security profile groups.</td> </tr> <tr> <td><i>group</i></td> <td>Allow security profile groups.</td> </tr> </tbody> </table>	Option	Description	<i>single</i>	Do not allow security profile groups.	<i>group</i>	Allow security profile groups.			
Option	Description									
<i>single</i>	Do not allow security profile groups.									
<i>group</i>	Allow security profile groups.									
service <name>	Service and service group names. Service and service group names.	string	Maximum length: 79							
srcaddr <name>	Source IPv4 address and address group names. Address name.	string	Maximum length: 79							
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79							
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	no-inspection						
status	Enable or disable this policy.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
utm-status	Enable to add one or more security profiles (AV, IPS, etc.) to the firewall policy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35							

config firewall profile-protocol-options

Configure protocol options.

Syntax

```

config firewall profile-protocol-options
  edit <name>
    config cifs
      Description: Configure CIFS protocol options.
      set domain-controller {string}
      set options {option1}, {option2}, ...
      set oversize-limit {integer}
      set scan-bzip2 [enable|disable]
      set server-credential-type [none|credential-replication|...]
    config server-keytab
      Description: Server keytab.
      edit <principal>
        set keytab {string}
      next
    end
    set status [enable|disable]
    set tcp-window-maximum {integer}
    set tcp-window-minimum {integer}
    set tcp-window-size {integer}
    set tcp-window-type [system|static|...]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
  end
  set comment {var-string}
  config dns
    Description: Configure DNS protocol options.
    set status [enable|disable]
  end
  config ftp
    Description: Configure FTP protocol options.
    set comfort-amount {integer}

```

```

set comfort-interval {integer}
set inspect-all [enable|disable]
set options {option1}, {option2}, ...
set oversize-limit {integer}
set scan-bzip2 [enable|disable]
set ssl-offloaded [no|yes]
set status [enable|disable]
set stream-based-uncompressed-limit {integer}
set tcp-window-maximum {integer}
set tcp-window-minimum {integer}
set tcp-window-size {integer}
set tcp-window-type [system|static|...]
set uncompressed-nest-limit {integer}
set uncompressed-oversize-limit {integer}
end
config http
  Description: Configure HTTP protocol options.
  set block-page-status-code {integer}
  set comfort-amount {integer}
  set comfort-interval {integer}
  set inspect-all [enable|disable]
  set options {option1}, {option2}, ...
  set oversize-limit {integer}
  set post-lang {option1}, {option2}, ...
  set proxy-after-tcp-handshake [enable|disable]
  set range-block [disable|enable]
  set retry-count {integer}
  set scan-bzip2 [enable|disable]
  set ssl-offloaded [no|yes]
  set status [enable|disable]
  set stream-based-uncompressed-limit {integer}
  set streaming-content-bypass [enable|disable]
  set strip-x-forwarded-for [disable|enable]
  set switching-protocols [bypass|block]
  set tcp-window-maximum {integer}
  set tcp-window-minimum {integer}
  set tcp-window-size {integer}
  set tcp-window-type [system|static|...]
  set tunnel-non-http [enable|disable]
  set uncompressed-nest-limit {integer}
  set uncompressed-oversize-limit {integer}
  set unknown-http-version [reject|tunnel|...]
end
config imap
  Description: Configure IMAP protocol options.
  set inspect-all [enable|disable]
  set options {option1}, {option2}, ...
  set oversize-limit {integer}
  set proxy-after-tcp-handshake [enable|disable]
  set scan-bzip2 [enable|disable]
  set ssl-offloaded [no|yes]
  set status [enable|disable]

```

```

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

```

```

    set status [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
config ssh
  Description: Configure SFTP and SCP protocol options.
  set comfort-amount {integer}
  set comfort-interval {integer}
  set options {option1}, {option2}, ...
  set oversize-limit {integer}
  set scan-bzip2 [enable|disable]
  set ssl-offloaded [no|yes]
  set stream-based-uncompressed-limit {integer}
  set tcp-window-maximum {integer}
  set tcp-window-minimum {integer}
  set tcp-window-size {integer}
  set tcp-window-type [system|static|...]
  set uncompressed-nest-limit {integer}
  set uncompressed-oversize-limit {integer}
end
set switching-protocols-log [disable|enable]
next
end

```

config firewall profile-protocol-options

Parameter	Description	Type	Size	Default						
comment	Optional comments.	var-string	Maximum length: 255							
name	Name.	string	Maximum length: 35							
oversize-log	Enable/disable logging for antivirus oversize file blocking.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging for antivirus oversize file blocking.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging for antivirus oversize file blocking.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging for antivirus oversize file blocking.	<i>enable</i>	Enable logging for antivirus oversize file blocking.			
Option	Description									
<i>disable</i>	Disable logging for antivirus oversize file blocking.									
<i>enable</i>	Enable logging for antivirus oversize file blocking.									
replacemsg-group	Name of the replacement message group to be used	string	Maximum length: 35							
rpc-over-http	Enable/disable inspection of RPC over HTTP.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable inspection of RPC over HTTP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable inspection of RPC over HTTP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable inspection of RPC over HTTP.	<i>disable</i>	Disable inspection of RPC over HTTP.			
Option	Description									
<i>enable</i>	Enable inspection of RPC over HTTP.									
<i>disable</i>	Disable inspection of RPC over HTTP.									

Parameter	Description	Type	Size	Default
switching-protocols-log	Enable/disable logging for HTTP/HTTPS switching protocols.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging for HTTP/HTTPS switching protocols.		
	<i>enable</i>	Enable logging for HTTP/HTTPS switching protocols.		

config cifs

Parameter	Description	Type	Size	Default
domain-controller	Domain for which to decrypt CIFS traffic.	string	Maximum length: 63	
options	One or more options that can be applied to the session.	option	-	
	Option	Description		
	<i>oversize</i>	Block oversized file/email.		
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
server-credential-type	CIFS server credential type.	option	-	none
	Option	Description		
	<i>none</i>	Credential derivation not set.		
	<i>credential-replication</i>	Credential derived using Replication account on Domain Controller.		
	<i>credential-keytab</i>	Credential derived using server keytab.		
status	Enable/disable the active status of scanning for this protocol.	option	-	enable

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608								
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072								
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144								
tcp-window-type	TCP window type to use for this protocol.	option	-	system								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>system</i></td> <td>Use system default TCP window size for this protocol (default).</td> </tr> <tr> <td><i>static</i></td> <td>Manually specify TCP window size.</td> </tr> <tr> <td><i>dynamic</i></td> <td>Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.</td> </tr> </tbody> </table>	Option	Description	<i>system</i>	Use system default TCP window size for this protocol (default).	<i>static</i>	Manually specify TCP window size.	<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			
Option	Description											
<i>system</i>	Use system default TCP window size for this protocol (default).											
<i>static</i>	Manually specify TCP window size.											
<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.											
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12								
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10								

config server-keytab

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

config dns

Parameter	Description	Type	Size	Default						
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

config ftp

Parameter	Description	Type	Size	Default						
comfort-amount	Amount of data to send in a transmission for client comforting.	integer	Minimum value: 1 Maximum value: 65535	1						
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						
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>clientcomfort</i></td> <td>Prevent client timeout.</td> </tr> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> <tr> <td><i>splice</i></td> <td>Enable splice mode.</td> </tr> <tr> <td><i>bypass-rest-command</i></td> <td>Bypass REST command.</td> </tr> <tr> <td><i>bypass-mode-command</i></td> <td>Bypass MODE command.</td> </tr> </tbody> </table>	Option	Description	<i>clientcomfort</i>	Prevent client timeout.	<i>oversize</i>	Block oversized file/email.	<i>splice</i>	Enable splice mode.	<i>bypass-rest-command</i>	Bypass REST command.	<i>bypass-mode-command</i>	Bypass MODE command.			
Option	Description															
<i>clientcomfort</i>	Prevent client timeout.															
<i>oversize</i>	Block oversized file/email.															
<i>splice</i>	Enable splice mode.															
<i>bypass-rest-command</i>	Bypass REST command.															
<i>bypass-mode-command</i>	Bypass MODE command.															
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10												
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no</i></td> <td>SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.</td> </tr> <tr> <td><i>yes</i></td> <td>SSL decryption and encryption performed by an external device.</td> </tr> </tbody> </table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.									
Option	Description															
<i>no</i>	SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.															
<i>yes</i>	SSL decryption and encryption performed by an external device.															
status	Enable/disable the active status of scanning for this protocol.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned.	integer	Minimum value: 0 Maximum value: 4294967295	0												

Parameter	Description	Type	Size	Default								
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608								
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072								
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144								
tcp-window-type	TCP window type to use for this protocol.	option	-	system								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>system</i></td> <td>Use system default TCP window size for this protocol (default).</td> </tr> <tr> <td><i>static</i></td> <td>Manually specify TCP window size.</td> </tr> <tr> <td><i>dynamic</i></td> <td>Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.</td> </tr> </tbody> </table>	Option	Description	<i>system</i>	Use system default TCP window size for this protocol (default).	<i>static</i>	Manually specify TCP window size.	<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			
Option	Description											
<i>system</i>	Use system default TCP window size for this protocol (default).											
<i>static</i>	Manually specify TCP window size.											
<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.											
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12								
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10								

config http

Parameter	Description	Type	Size	Default
block-page-status-code	Code number returned for blocked HTTP pages.	integer	Minimum value: 100 Maximum value: 599	403

Parameter	Description	Type	Size	Default														
comfort-amount	Amount of data to send in a transmission for client comforting.	integer	Minimum value: 1 Maximum value: 65535	1														
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														
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.											
Option	Description																	
<i>enable</i>	Enable setting.																	
<i>disable</i>	Disable setting.																	
options	One or more options that can be applied to the session.	option	-															
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>clientcomfort</i></td> <td>Prevent client timeout.</td> </tr> <tr> <td><i>servercomfort</i></td> <td>Prevent server timeout.</td> </tr> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> <tr> <td><i>chunkedbypass</i></td> <td>Bypass chunked transfer encoded sites.</td> </tr> </tbody> </table>	Option	Description	<i>clientcomfort</i>	Prevent client timeout.	<i>servercomfort</i>	Prevent server timeout.	<i>oversize</i>	Block oversized file/email.	<i>chunkedbypass</i>	Bypass chunked transfer encoded sites.							
Option	Description																	
<i>clientcomfort</i>	Prevent client timeout.																	
<i>servercomfort</i>	Prevent server timeout.																	
<i>oversize</i>	Block oversized file/email.																	
<i>chunkedbypass</i>	Bypass chunked transfer encoded sites.																	
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10														
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	-															
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>jisx0201</i></td> <td>Japanese Industrial Standard 0201.</td> </tr> <tr> <td><i>jisx0208</i></td> <td>Japanese Industrial Standard 0208.</td> </tr> <tr> <td><i>jisx0212</i></td> <td>Japanese Industrial Standard 0212.</td> </tr> <tr> <td><i>gb2312</i></td> <td>Guojia Biaozhun 2312 (simplified Chinese).</td> </tr> <tr> <td><i>ksc5601-ex</i></td> <td>Wansung Korean standard 5601.</td> </tr> <tr> <td><i>euc-jp</i></td> <td>Extended Unicode Japanese.</td> </tr> </tbody> </table>	Option	Description	<i>jisx0201</i>	Japanese Industrial Standard 0201.	<i>jisx0208</i>	Japanese Industrial Standard 0208.	<i>jisx0212</i>	Japanese Industrial Standard 0212.	<i>gb2312</i>	Guojia Biaozhun 2312 (simplified Chinese).	<i>ksc5601-ex</i>	Wansung Korean standard 5601.	<i>euc-jp</i>	Extended Unicode Japanese.			
Option	Description																	
<i>jisx0201</i>	Japanese Industrial Standard 0201.																	
<i>jisx0208</i>	Japanese Industrial Standard 0208.																	
<i>jisx0212</i>	Japanese Industrial Standard 0212.																	
<i>gb2312</i>	Guojia Biaozhun 2312 (simplified Chinese).																	
<i>ksc5601-ex</i>	Wansung Korean standard 5601.																	
<i>euc-jp</i>	Extended Unicode Japanese.																	

Parameter	Description	Type	Size	Default																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sjis</i></td> <td>Shift Japanese Industrial Standard.</td> </tr> <tr> <td><i>iso2022-jp</i></td> <td>ISO 2022 Japanese.</td> </tr> <tr> <td><i>iso2022-jp-1</i></td> <td>ISO 2022-1 Japanese.</td> </tr> <tr> <td><i>iso2022-jp-2</i></td> <td>ISO 2022-2 Japanese.</td> </tr> <tr> <td><i>euc-cn</i></td> <td>Extended Unicode Chinese.</td> </tr> <tr> <td><i>ces-gbk</i></td> <td>Extended GB2312 (simplified Chinese).</td> </tr> <tr> <td><i>hz</i></td> <td>Hanzi simplified Chinese.</td> </tr> <tr> <td><i>ces-big5</i></td> <td>Big-5 traditional Chinese.</td> </tr> <tr> <td><i>euc-kr</i></td> <td>Extended Unicode Korean.</td> </tr> <tr> <td><i>iso2022-jp-3</i></td> <td>ISO 2022-3 Japanese.</td> </tr> <tr> <td><i>iso8859-1</i></td> <td>ISO 8859 Part 1 (Western European).</td> </tr> <tr> <td><i>tis620</i></td> <td>Thai Industrial Standard 620.</td> </tr> <tr> <td><i>cp874</i></td> <td>Code Page 874 (Thai).</td> </tr> <tr> <td><i>cp1252</i></td> <td>Code Page 1252 (Western European Latin).</td> </tr> <tr> <td><i>cp1251</i></td> <td>Code Page 1251 (Cyrillic).</td> </tr> </tbody> </table>	Option	Description	<i>sjis</i>	Shift Japanese Industrial Standard.	<i>iso2022-jp</i>	ISO 2022 Japanese.	<i>iso2022-jp-1</i>	ISO 2022-1 Japanese.	<i>iso2022-jp-2</i>	ISO 2022-2 Japanese.	<i>euc-cn</i>	Extended Unicode Chinese.	<i>ces-gbk</i>	Extended GB2312 (simplified Chinese).	<i>hz</i>	Hanzi simplified Chinese.	<i>ces-big5</i>	Big-5 traditional Chinese.	<i>euc-kr</i>	Extended Unicode Korean.	<i>iso2022-jp-3</i>	ISO 2022-3 Japanese.	<i>iso8859-1</i>	ISO 8859 Part 1 (Western European).	<i>tis620</i>	Thai Industrial Standard 620.	<i>cp874</i>	Code Page 874 (Thai).	<i>cp1252</i>	Code Page 1252 (Western European Latin).	<i>cp1251</i>	Code Page 1251 (Cyrillic).			
Option	Description																																			
<i>sjis</i>	Shift Japanese Industrial Standard.																																			
<i>iso2022-jp</i>	ISO 2022 Japanese.																																			
<i>iso2022-jp-1</i>	ISO 2022-1 Japanese.																																			
<i>iso2022-jp-2</i>	ISO 2022-2 Japanese.																																			
<i>euc-cn</i>	Extended Unicode Chinese.																																			
<i>ces-gbk</i>	Extended GB2312 (simplified Chinese).																																			
<i>hz</i>	Hanzi simplified Chinese.																																			
<i>ces-big5</i>	Big-5 traditional Chinese.																																			
<i>euc-kr</i>	Extended Unicode Korean.																																			
<i>iso2022-jp-3</i>	ISO 2022-3 Japanese.																																			
<i>iso8859-1</i>	ISO 8859 Part 1 (Western European).																																			
<i>tis620</i>	Thai Industrial Standard 620.																																			
<i>cp874</i>	Code Page 874 (Thai).																																			
<i>cp1252</i>	Code Page 1252 (Western European Latin).																																			
<i>cp1251</i>	Code Page 1251 (Cyrillic).																																			
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																													
Option	Description																																			
<i>enable</i>	Enable setting.																																			
<i>disable</i>	Disable setting.																																			
range-block	Enable/disable blocking of partial downloads.	option	-	disable																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable range header blocking (allow partial file downloads)</td> </tr> <tr> <td><i>enable</i></td> <td>Enable range header blocking (treat all partial file downloads as full file download)</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable range header blocking (allow partial file downloads)	<i>enable</i>	Enable range header blocking (treat all partial file downloads as full file download)																													
Option	Description																																			
<i>disable</i>	Disable range header blocking (allow partial file downloads)																																			
<i>enable</i>	Enable range header blocking (treat all partial file downloads as full file download)																																			
retry-count	Number of attempts to retry HTTP connection.	integer	Minimum value: 0 Maximum value: 100	0																																

Parameter	Description	Type	Size	Default						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no</i></td> <td>SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.</td> </tr> <tr> <td><i>yes</i></td> <td>SSL decryption and encryption performed by an external device.</td> </tr> </tbody> </table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.			
Option	Description									
<i>no</i>	SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.									
<i>yes</i>	SSL decryption and encryption performed by an external device.									
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned.	integer	Minimum value: 0 Maximum value: 4294967295	0						
streaming-content-bypass	Enable/disable bypassing of streaming content from buffering.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
strip-x-forwarded-for	Enable/disable stripping of HTTP X-Forwarded-For header.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable changing of HTTP X-Forwarded-For header.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable replacement of X-Forwarded-For value with 1.1.1.1.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable changing of HTTP X-Forwarded-For header.	<i>enable</i>	Enable replacement of X-Forwarded-For value with 1.1.1.1.			
Option	Description									
<i>disable</i>	Disable changing of HTTP X-Forwarded-For header.									
<i>enable</i>	Enable replacement of X-Forwarded-For value with 1.1.1.1.									

Parameter	Description	Type	Size	Default								
switching-protocols	Bypass from scanning, or block a connection that attempts to switch protocol.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass connections when switching protocols.</td> </tr> <tr> <td><i>block</i></td> <td>Block connections when switching protocols.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass connections when switching protocols.	<i>block</i>	Block connections when switching protocols.					
Option	Description											
<i>bypass</i>	Bypass connections when switching protocols.											
<i>block</i>	Block connections when switching protocols.											
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608								
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072								
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144								
tcp-window-type	TCP window type to use for this protocol.	option	-	system								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>system</i></td> <td>Use system default TCP window size for this protocol (default).</td> </tr> <tr> <td><i>static</i></td> <td>Manually specify TCP window size.</td> </tr> <tr> <td><i>dynamic</i></td> <td>Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.</td> </tr> </tbody> </table>	Option	Description	<i>system</i>	Use system default TCP window size for this protocol (default).	<i>static</i>	Manually specify TCP window size.	<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			
Option	Description											
<i>system</i>	Use system default TCP window size for this protocol (default).											
<i>static</i>	Manually specify TCP window size.											
<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.											
tunnel-non-http	Configure how to process non-HTTP traffic when a profile configured for HTTP traffic accepts a non-HTTP session. Can occur if an application sends non-HTTP traffic using an HTTP destination port.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.</td> </tr> <tr> <td><i>disable</i></td> <td>Drop or tear down non-HTTP sessions accepted by the profile.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.	<i>disable</i>	Drop or tear down non-HTTP sessions accepted by the profile.					
Option	Description											
<i>enable</i>	Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.											
<i>disable</i>	Drop or tear down non-HTTP sessions accepted by the profile.											

Parameter	Description	Type	Size	Default								
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12								
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10								
unknown-http-version	How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.	option	-	reject								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>reject</i></td> <td>Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.</td> </tr> <tr> <td><i>tunnel</i></td> <td>Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.</td> </tr> <tr> <td><i>best-effort</i></td> <td>Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.</td> </tr> </tbody> </table>	Option	Description	<i>reject</i>	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.	<i>tunnel</i>	Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.	<i>best-effort</i>	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.			
Option	Description											
<i>reject</i>	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.											
<i>tunnel</i>	Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.											
<i>best-effort</i>	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.											

config imap

Parameter	Description	Type	Size	Default						
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fragmail</i></td> <td>Pass fragmented email.</td> </tr> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> </tbody> </table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized file/email.			
Option	Description									
<i>fragmail</i>	Pass fragmented email.									
<i>oversize</i>	Block oversized file/email.									
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10						

Parameter	Description	Type	Size	Default						
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no</i></td> <td>SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.</td> </tr> <tr> <td><i>yes</i></td> <td>SSL decryption and encryption performed by an external device.</td> </tr> </tbody> </table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.			
Option	Description									
<i>no</i>	SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.									
<i>yes</i>	SSL decryption and encryption performed by an external device.									
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10						

config mail-signature

Parameter	Description	Type	Size	Default						
signature	Email signature to be added to outgoing email (if the signature contains spaces, enclose with quotation marks).	string	Maximum length: 1023							
status	Enable/disable adding an email signature to SMTP email messages as they pass through Container FortiOS.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable mail signature.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable mail signature.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable mail signature.	<i>enable</i>	Enable mail signature.			
Option	Description									
<i>disable</i>	Disable mail signature.									
<i>enable</i>	Enable mail signature.									

config mapi

Parameter	Description	Type	Size	Default						
options	One or more options that can be applied to the session.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fragmail</i></td> <td>Pass fragmented email.</td> </tr> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> </tbody> </table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized file/email.			
Option	Description									
<i>fragmail</i>	Pass fragmented email.									
<i>oversize</i>	Block oversized file/email.									
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10

config nntp

Parameter	Description	Type	Size	Default						
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> <tr> <td><i>splice</i></td> <td>Enable splice mode.</td> </tr> </tbody> </table>	Option	Description	<i>oversize</i>	Block oversized file/email.	<i>splice</i>	Enable splice mode.			
Option	Description									
<i>oversize</i>	Block oversized file/email.									
<i>splice</i>	Enable splice mode.									
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10						
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.					
Option	Description									
<i>enable</i>	Enable setting.									

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable setting.					
Option	Description									
<i>disable</i>	Disable setting.									
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10						

config pop3

Parameter	Description	Type	Size	Default						
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fragmail</i></td> <td>Pass fragmented email.</td> </tr> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> </tbody> </table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized file/email.			
Option	Description									
<i>fragmail</i>	Pass fragmented email.									
<i>oversize</i>	Block oversized file/email.									
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10						

Parameter	Description	Type	Size	Default						
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no</i></td> <td>SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.</td> </tr> <tr> <td><i>yes</i></td> <td>SSL decryption and encryption performed by an external device.</td> </tr> </tbody> </table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.			
Option	Description									
<i>no</i>	SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.									
<i>yes</i>	SSL decryption and encryption performed by an external device.									
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10						

config smtp

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

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
options	One or more options that can be applied to the session.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fragmail</i></td> <td>Pass fragmented email.</td> </tr> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> <tr> <td><i>splice</i></td> <td>Enable splice mode.</td> </tr> </tbody> </table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized file/email.	<i>splice</i>	Enable splice mode.			
Option	Description											
<i>fragmail</i>	Pass fragmented email.											
<i>oversize</i>	Block oversized file/email.											
<i>splice</i>	Enable splice mode.											
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10								
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
server-busy	Enable/disable SMTP server busy when server not available.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no</i></td> <td>SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.</td> </tr> <tr> <td><i>yes</i></td> <td>SSL decryption and encryption performed by an external device.</td> </tr> </tbody> </table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.			
Option	Description									
<i>no</i>	SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.									
<i>yes</i>	SSL decryption and encryption performed by an external device.									
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10						

config ssh

Parameter	Description	Type	Size	Default								
comfort-amount	Amount of data to send in a transmission for client comforting.	integer	Minimum value: 1 Maximum value: 65535	1								
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								
options	One or more options that can be applied to the session.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> <tr> <td><i>clientcomfort</i></td> <td>Prevent client timeout.</td> </tr> <tr> <td><i>servercomfort</i></td> <td>Prevent server timeout.</td> </tr> </tbody> </table>	Option	Description	<i>oversize</i>	Block oversized file/email.	<i>clientcomfort</i>	Prevent client timeout.	<i>servercomfort</i>	Prevent server timeout.			
Option	Description											
<i>oversize</i>	Block oversized file/email.											
<i>clientcomfort</i>	Prevent client timeout.											
<i>servercomfort</i>	Prevent server timeout.											

Parameter	Description	Type	Size	Default						
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no</i></td> <td>SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.</td> </tr> <tr> <td><i>yes</i></td> <td>SSL decryption and encryption performed by an external device.</td> </tr> </tbody> </table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.			
Option	Description									
<i>no</i>	SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.									
<i>yes</i>	SSL decryption and encryption performed by an external device.									
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned.	integer	Minimum value: 0 Maximum value: 4294967295	0						
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608						
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072						
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144						
tcp-window-type	TCP window type to use for this protocol.	option	-	system						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>system</i></td> <td>Use system default TCP window size for this protocol (default).</td> </tr> <tr> <td><i>static</i></td> <td>Manually specify TCP window size.</td> </tr> <tr> <td><i>dynamic</i></td> <td>Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.</td> </tr> </tbody> </table>	Option	Description	<i>system</i>	Use system default TCP window size for this protocol (default).	<i>static</i>	Manually specify TCP window size.	<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			
Option	Description											
<i>system</i>	Use system default TCP window size for this protocol (default).											
<i>static</i>	Manually specify TCP window size.											
<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.											
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12								
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10								

config firewall schedule group

Schedule group configuration.

Syntax

```
config firewall schedule group
  edit <name>
    set member <name1>, <name2>, ...
  next
end
```

Parameters

Parameter	Description	Type	Size	Default
member <name>	Schedules added to the schedule group. Schedule name.	string	Maximum length: 79	
name	Schedule group name.	string	Maximum length: 31	

config firewall schedule onetime

Onetime schedule configuration.

Syntax

```
config firewall schedule onetime
  edit <name>
    set end {user}
    set expiration-days {integer}
    set start {user}
  next
end
```

Parameters

Parameter	Description	Type	Size	Default
end	Schedule end date and time, format hh:mm yyyy/mm/dd.	user	Not Specified	
expiration-days	Write an event log message this many days before the schedule expires.	integer	Minimum value: 0 Maximum value: 100	3
name	Onetime schedule name.	string	Maximum length: 31	
start	Schedule start date and time, format hh:mm yyyy/mm/dd.	user	Not Specified	

config firewall schedule recurring

Recurring schedule configuration.

Syntax

```
config firewall schedule recurring
  edit <name>
    set day {option1}, {option2}, ...
    set end {user}
    set start {user}
  next
end
```

Parameters

Parameter	Description	Type	Size	Default
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																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sunday</i></td> <td>Sunday.</td> </tr> <tr> <td><i>monday</i></td> <td>Monday.</td> </tr> <tr> <td><i>tuesday</i></td> <td>Tuesday.</td> </tr> <tr> <td><i>wednesday</i></td> <td>Wednesday.</td> </tr> <tr> <td><i>thursday</i></td> <td>Thursday.</td> </tr> <tr> <td><i>friday</i></td> <td>Friday.</td> </tr> <tr> <td><i>saturday</i></td> <td>Saturday.</td> </tr> <tr> <td><i>none</i></td> <td>None.</td> </tr> </tbody> </table>	Option	Description	<i>sunday</i>	Sunday.	<i>monday</i>	Monday.	<i>tuesday</i>	Tuesday.	<i>wednesday</i>	Wednesday.	<i>thursday</i>	Thursday.	<i>friday</i>	Friday.	<i>saturday</i>	Saturday.	<i>none</i>	None.			
Option	Description																					
<i>sunday</i>	Sunday.																					
<i>monday</i>	Monday.																					
<i>tuesday</i>	Tuesday.																					
<i>wednesday</i>	Wednesday.																					
<i>thursday</i>	Thursday.																					
<i>friday</i>	Friday.																					
<i>saturday</i>	Saturday.																					
<i>none</i>	None.																					
end	Time of day to end the schedule, format hh:mm.	user		Not Specified																		
name	Recurring schedule name.	string		Maximum length: 31																		
start	Time of day to start the schedule, format hh:mm.	user		Not Specified																		

config firewall security-policy

Configure NGFW application policies.

Syntax

```
config firewall security-policy
  edit <policyid>
    set action [accept|deny]
    set app-category <id1>, <id2>, ...
    set app-group <name1>, <name2>, ...
    set application <id1>, <id2>, ...
    set application-list {string}
    set av-profile {string}
    set comments {var-string}
    set custom-log-fields <field-id1>, <field-id2>, ...
    set dstaddr <name1>, <name2>, ...
    set dstaddr-negate [enable|disable]
    set dstintf <name1>, <name2>, ...
    set enforce-default-app-port [enable|disable]
    set fsso-groups <name1>, <name2>, ...
    set groups <name1>, <name2>, ...
    set ips-sensor {string}
    set learning-mode [enable|disable]
    set logtraffic [all|utm|...]
```

```

set name {string}
set profile-group {string}
set profile-protocol-options {string}
set profile-type [single|group]
set schedule {string}
set send-deny-packet [disable|enable]
set service <name1>, <name2>, ...
set service-negate [enable|disable]
set srcaddr <name1>, <name2>, ...
set srcaddr-negate [enable|disable]
set srcintf <name1>, <name2>, ...
set status [enable|disable]
set url-category <id1>, <id2>, ...
set users <name1>, <name2>, ...
set uuid {uuid}
set webfilter-profile {string}
next
end

```

config firewall security-policy

Parameter	Description	Type	Size	Default						
action	Policy action (accept/deny).	option	-	deny						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accept</i></td> <td>Allows session that match the firewall policy.</td> </tr> <tr> <td><i>deny</i></td> <td>Blocks sessions that match the firewall policy.</td> </tr> </tbody> </table>	Option	Description	<i>accept</i>	Allows session that match the firewall policy.	<i>deny</i>	Blocks sessions that match the firewall policy.			
Option	Description									
<i>accept</i>	Allows session that match the firewall policy.									
<i>deny</i>	Blocks sessions that match the firewall policy.									
app-category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295							
app-group <name>	Application group names. Application group names.	string	Maximum length: 79							
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295							
application- list	Name of an existing Application list.	string	Maximum length: 35							
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default						
comments	Comment.	var-string	Maximum length: 1023							
custom-log-fields <field-id>	Custom fields to append to log messages for this policy. Custom log field.	string	Maximum length: 35							
dstaddr <name>	Destination IPv4 address name and address group names. Address name.	string	Maximum length: 79							
dstaddr-negate	When enabled dstaddr/dstaddr6 specifies what the destination address must NOT be.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable destination address negate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable destination address negate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable destination address negate.	<i>disable</i>	Disable destination address negate.			
Option	Description									
<i>enable</i>	Enable destination address negate.									
<i>disable</i>	Disable destination address negate.									
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79							
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
fssso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511							
groups <name>	Names of user groups that can authenticate with this policy. User group name.	string	Maximum length: 79							
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35							
learning-mode	Enable to allow everything, but log all of the meaningful data for security information gathering. A learning report will be generated.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable learning mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable learning mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable learning mode.	<i>disable</i>	Disable learning mode.			
Option	Description									
<i>enable</i>	Enable learning mode.									
<i>disable</i>	Disable learning mode.									

Parameter	Description	Type	Size	Default								
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>all</i></td> <td>Log all sessions accepted or denied by this policy.</td> </tr> <tr> <td><i>utm</i></td> <td>Log traffic that has a security profile applied to it.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable all logging for this policy.</td> </tr> </tbody> </table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.			
Option	Description											
<i>all</i>	Log all sessions accepted or denied by this policy.											
<i>utm</i>	Log traffic that has a security profile applied to it.											
<i>disable</i>	Disable all logging for this policy.											
name	Policy name.	string	Maximum length: 35									
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967294	0								
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								
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>single</i></td> <td>Do not allow security profile groups.</td> </tr> <tr> <td><i>group</i></td> <td>Allow security profile groups.</td> </tr> </tbody> </table>	Option	Description	<i>single</i>	Do not allow security profile groups.	<i>group</i>	Allow security profile groups.					
Option	Description											
<i>single</i>	Do not allow security profile groups.											
<i>group</i>	Allow security profile groups.											
schedule	Schedule name.	string	Maximum length: 35									
send-deny-packet	Enable to send a reply when a session is denied or blocked by a firewall policy.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable deny-packet sending.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable deny-packet sending.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable deny-packet sending.	<i>enable</i>	Enable deny-packet sending.					
Option	Description											
<i>disable</i>	Disable deny-packet sending.											
<i>enable</i>	Enable deny-packet sending.											
service <name>	Service and service group names. Service name.	string	Maximum length: 79									
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable negated service match.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable negated service match.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable negated service match.	<i>disable</i>	Disable negated service match.			
Option	Description									
<i>enable</i>	Enable negated service match.									
<i>disable</i>	Disable negated service match.									
srcaddr <name>	Source IPv4 address name and address group names. Address name.	string	Maximum length: 79							
srcaddr-negate	When enabled srcaddr/srcaddr6 specifies what the source address must NOT be.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable source address negate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable source address negate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable source address negate.	<i>disable</i>	Disable source address negate.			
Option	Description									
<i>enable</i>	Enable source address negate.									
<i>disable</i>	Disable source address negate.									
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79							
status	Enable or disable this policy.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
url-category <id>	URL category ID list. URL category ID.	integer	Minimum value: 0 Maximum value: 255							
users <name>	Names of individual users that can authenticate with this policy. User name.	string	Maximum length: 79							
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35							

config firewall service category

Configure service categories.

Syntax

```
config firewall service category
  edit <name>
    set comment {var-string}
  next
end
```

Parameters

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	Service category name.	string	Maximum length: 63	

config firewall service custom

Configure custom services.

Syntax

```
config firewall service custom
  edit <name>
    set category {string}
    set check-reset-range [disable|strict|...]
    set comment {var-string}
    set fqdn {string}
    set icmpcode {integer}
    set icmptype {integer}
    set iprange {user}
    set protocol [TCP/UDP/SCTP|ICMP|...]
    set protocol-number {integer}
    set sctp-portrange {user}
    set session-ttl {user}
    set tcp-halfclose-timer {integer}
    set tcp-halfopen-timer {integer}
    set tcp-portrange {user}
    set tcp-rst-timer {integer}
    set tcp-timewait-timer {integer}
    set udp-idle-timer {integer}
    set udp-portrange {user}
  next
end
```

Parameters

Parameter	Description	Type	Size	Default										
category	Service category.	string	Maximum length: 63											
check-reset-range	Configure the type of ICMP error message verification.	option	-	default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable RST range check.</td> </tr> <tr> <td><i>strict</i></td> <td>Check RST range strictly.</td> </tr> <tr> <td><i>default</i></td> <td>Using system default setting.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable RST range check.	<i>strict</i>	Check RST range strictly.	<i>default</i>	Using system default setting.					
Option	Description													
<i>disable</i>	Disable RST range check.													
<i>strict</i>	Check RST range strictly.													
<i>default</i>	Using system default setting.													
comment	Comment.	var-string	Maximum length: 255											
fqdn	Fully qualified domain name.	string	Maximum length: 255											
icmpcode	ICMP code.	integer	Minimum value: 0 Maximum value: 255											
icmptype	ICMP type, value from 0 to 255	integer	Minimum value: 0 Maximum value: 255											
iprange	Start and end of the IP range associated with service.	user	Not Specified											
name	Custom service name.	string	Maximum length: 79											
protocol	Protocol type based on IANA numbers.	option	-	TCP/UDP/SCTP										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>TCP/UDP/SCTP</i></td> <td>TCP, UDP and SCTP.</td> </tr> <tr> <td><i>ICMP</i></td> <td>ICMP.</td> </tr> <tr> <td><i>ICMP6</i></td> <td>ICMP6.</td> </tr> <tr> <td><i>IP</i></td> <td>IP.</td> </tr> </tbody> </table>	Option	Description	<i>TCP/UDP/SCTP</i>	TCP, UDP and SCTP.	<i>ICMP</i>	ICMP.	<i>ICMP6</i>	ICMP6.	<i>IP</i>	IP.			
Option	Description													
<i>TCP/UDP/SCTP</i>	TCP, UDP and SCTP.													
<i>ICMP</i>	ICMP.													
<i>ICMP6</i>	ICMP6.													
<i>IP</i>	IP.													
protocol-number	IP protocol number.	integer	Minimum value: 0 Maximum value: 254	0										

Parameter	Description	Type	Size	Default
sctp-portrange	Multiple SCTP port ranges.	user	Not Specified	
session-ttl	Session TTL.	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-portrange	Multiple TCP port ranges.	user	Not Specified	
tcp-rst-timer	Set the length of the TCP CLOSE state in seconds.	integer	Minimum value: 5 Maximum value: 300	0
tcp-timewait-timer	Set the length of the TCP TIME-WAIT state in seconds.	integer	Minimum value: 0 Maximum value: 300	0
udp-idle-timer	UDP half close timeout.	integer	Minimum value: 0 Maximum value: 86400	0
udp-portrange	Multiple UDP port ranges.	user	Not Specified	

config firewall service group

Configure service groups.

Syntax

```
config firewall service group
  edit <name>
    set comment {var-string}
    set member <name1>, <name2>, ...
```

```
next
end
```

Parameters

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

config firewall ssl-ssh-profile

Configure SSL/SSH protocol options.

Syntax

```
config firewall ssl-ssh-profile
  edit <name>
    set block-blocklisted-certificates [disable|enable]
    set caname {string}
    set comment {var-string}
    config dot
      Description: Configure DNS over TLS options.
      set cert-validation-failure [allow|block|...]
      set cert-validation-timeout [allow|block|...]
      set client-certificate [bypass|inspect|...]
      set expired-server-cert [allow|block|...]
      set proxy-after-tcp-handshake [enable|disable]
      set revoked-server-cert [allow|block|...]
      set sni-server-cert-check [enable|strict|...]
      set status [disable|deep-inspection]
      set unsupported-ssl-cipher [allow|block]
      set unsupported-ssl-negotiation [allow|block]
      set untrusted-server-cert [allow|block|...]
    end
    config ftps
      Description: Configure FTPS options.
      set cert-validation-failure [allow|block|...]
      set cert-validation-timeout [allow|block|...]
      set client-certificate [bypass|inspect|...]
      set expired-server-cert [allow|block|...]
      set revoked-server-cert [allow|block|...]
      set sni-server-cert-check [enable|strict|...]
      set status [disable|deep-inspection]
```

```

    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set untrusted-server-cert [allow|block|...]
end
config https
    Description: Configure HTTPS options.
    set cert-probe-failure [allow|block]
    set cert-validation-failure [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set client-certificate [bypass|inspect|...]
    set expired-server-cert [allow|block|...]
    set proxy-after-tcp-handshake [enable|disable]
    set revoked-server-cert [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
    set status [disable|certificate-inspection|...]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set untrusted-server-cert [allow|block|...]
end
config imaps
    Description: Configure IMAPS options.
    set cert-validation-failure [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set client-certificate [bypass|inspect|...]
    set expired-server-cert [allow|block|...]
    set proxy-after-tcp-handshake [enable|disable]
    set revoked-server-cert [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
    set status [disable|deep-inspection]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set untrusted-server-cert [allow|block|...]
end
set mapi-over-https [enable|disable]
config pop3s
    Description: Configure POP3S options.
    set cert-validation-failure [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set client-certificate [bypass|inspect|...]
    set expired-server-cert [allow|block|...]
    set proxy-after-tcp-handshake [enable|disable]
    set revoked-server-cert [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
    set status [disable|deep-inspection]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set untrusted-server-cert [allow|block|...]
end
set rpc-over-https [enable|disable]
set server-cert <name1>, <name2>, ...
set server-cert-mode [re-sign|replace]
config smtps

```

```

Description: Configure SMTPS options.
set cert-validation-failure [allow|block|...]
set cert-validation-timeout [allow|block|...]
set client-certificate [bypass|inspect|...]
set expired-server-cert [allow|block|...]
set proxy-after-tcp-handshake [enable|disable]
set revoked-server-cert [allow|block|...]
set sni-server-cert-check [enable|strict|...]
set status [disable|deep-inspection]
set unsupported-ssl-cipher [allow|block]
set unsupported-ssl-negotiation [allow|block]
set untrusted-server-cert [allow|block|...]
end
config ssh
Description: Configure SSH options.
set inspect-all [disable|deep-inspection]
set proxy-after-tcp-handshake [enable|disable]
set ssh-algorithm [compatible|high-encryption]
set ssh-tun-policy-check [disable|enable]
set status [disable|deep-inspection]
set unsupported-version [bypass|block]
end
config ssl
Description: Configure SSL options.
set cert-validation-failure [allow|block|...]
set cert-validation-timeout [allow|block|...]
set client-certificate [bypass|inspect|...]
set expired-server-cert [allow|block|...]
set inspect-all [disable|certificate-inspection|...]
set revoked-server-cert [allow|block|...]
set sni-server-cert-check [enable|strict|...]
set unsupported-ssl-cipher [allow|block]
set unsupported-ssl-negotiation [allow|block]
set untrusted-server-cert [allow|block|...]
end
set ssl-anomalies-log [disable|enable]
config ssl-exempt
Description: Servers to exempt from SSL inspection.
edit <id>
    set address {string}
    set fortiguard-category {integer}
    set regex {string}
    set type [fortiguard-category|address|...]
    set wildcard-fqdn {string}
next
end
set ssl-exemptions-log [disable|enable]
set ssl-negotiation-log [disable|enable]
config ssl-server
Description: SSL server settings used for client certificate request.
edit <id>
    set ftps-client-certificate [bypass|inspect|...]

```

```

    set https-client-certificate [bypass|inspect|...]
    set imaps-client-certificate [bypass|inspect|...]
    set ip {ipv4-address-any}
    set pop3s-client-certificate [bypass|inspect|...]
    set smtps-client-certificate [bypass|inspect|...]
    set ssl-other-client-certificate [bypass|inspect|...]
  next
end
set supported-alpn [http1-1|http2|...]
set untrusted-caname {string}
set use-ssl-server [disable|enable]
next
end

```

config firewall ssl-ssh-profile

Parameter	Description	Type	Size	Default
block-blocklisted-certificates	Enable/disable blocking SSL-based botnet communication by FortiGuard certificate blacklist.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable FortiGuard certificate blacklist.		
	<i>enable</i>	Enable FortiGuard certificate blacklist.		
caname	CA certificate used by SSL Inspection.	string	Maximum length: 35	Fortinet_CA_SSL
comment	Optional comments.	var-string	Maximum length: 255	
mapi-over-https	Enable/disable inspection of MAPI over HTTPS.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable inspection of MAPI over HTTPS.		
	<i>disable</i>	Disable inspection of MAPI over HTTPS.		
name	Name.	string	Maximum length: 35	
rpc-over-https	Enable/disable inspection of RPC over HTTPS.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable inspection of RPC over HTTPS.		
	<i>disable</i>	Disable inspection of RPC over HTTPS.		

Parameter	Description	Type	Size	Default										
server-cert <name>	Certificate used by SSL Inspection to replace server certificate. Certificate list.	string	Maximum length: 35											
server-cert-mode	Re-sign or replace the server's certificate.	option	-	re-sign										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>re-sign</i></td> <td>Multiple clients connecting to multiple servers.</td> </tr> <tr> <td><i>replace</i></td> <td>Protect an SSL server.</td> </tr> </tbody> </table>	Option	Description	<i>re-sign</i>	Multiple clients connecting to multiple servers.	<i>replace</i>	Protect an SSL server.							
Option	Description													
<i>re-sign</i>	Multiple clients connecting to multiple servers.													
<i>replace</i>	Protect an SSL server.													
ssl-anomalies-log	Enable/disable logging SSL anomalies.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging SSL anomalies.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging SSL anomalies.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging SSL anomalies.	<i>enable</i>	Enable logging SSL anomalies.							
Option	Description													
<i>disable</i>	Disable logging SSL anomalies.													
<i>enable</i>	Enable logging SSL anomalies.													
ssl-exemptions-log	Enable/disable logging SSL exemptions.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging SSL exemptions.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging SSL exemptions.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging SSL exemptions.	<i>enable</i>	Enable logging SSL exemptions.							
Option	Description													
<i>disable</i>	Disable logging SSL exemptions.													
<i>enable</i>	Enable logging SSL exemptions.													
ssl-negotiation-log	Enable/disable logging SSL negotiation.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging SSL negotiation.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging SSL negotiation.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging SSL negotiation.	<i>enable</i>	Enable logging SSL negotiation.							
Option	Description													
<i>disable</i>	Disable logging SSL negotiation.													
<i>enable</i>	Enable logging SSL negotiation.													
supported-alpn	Configure ALPN option.	option	-	all										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>http1-1</i></td> <td>Enable ALPN of HTTP1.1.</td> </tr> <tr> <td><i>http2</i></td> <td>Enable ALPN of HTTP2.</td> </tr> <tr> <td><i>all</i></td> <td>Enable ALPN of HTTP1.1 and HTTP2.</td> </tr> <tr> <td><i>none</i></td> <td>Do not use ALPN.</td> </tr> </tbody> </table>	Option	Description	<i>http1-1</i>	Enable ALPN of HTTP1.1.	<i>http2</i>	Enable ALPN of HTTP2.	<i>all</i>	Enable ALPN of HTTP1.1 and HTTP2.	<i>none</i>	Do not use ALPN.			
Option	Description													
<i>http1-1</i>	Enable ALPN of HTTP1.1.													
<i>http2</i>	Enable ALPN of HTTP2.													
<i>all</i>	Enable ALPN of HTTP1.1 and HTTP2.													
<i>none</i>	Do not use ALPN.													

Parameter	Description	Type	Size	Default
untrusted-caname	Untrusted CA certificate used by SSL Inspection.	string	Maximum length: 35	Fortinet_CA_Untrusted
use-ssl-server	Enable/disable the use of SSL server table for SSL offloading.	option	-	disable
	Option	Description		
	<i>disable</i>	Don't use SSL server configuration.		
	<i>enable</i>	Use SSL server configuration.		

config dot

Parameter	Description	Type	Size	Default
cert-validation-failure	Action based on certificate validation failure.	option	-	block
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
client-certificate	Action based on received client certificate.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
expired-server-cert	Action based on server certificate is expired.	option	-	block

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td> </tr> <tr> <td><i>strict</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											
status	Configure protocol inspection status.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.					
Option	Description											
<i>disable</i>	Disable.											
<i>deep-inspection</i>	Full SSL inspection.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the cipher is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the cipher is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the negotiation is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the negotiation is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											

config ftps

Parameter	Description	Type	Size	Default								
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
client-certificate	Action based on received client certificate.	option	-	bypass								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td> </tr> <tr> <td><i>strict</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.					
Option	Description											
<i>disable</i>	Disable.											
<i>deep-inspection</i>	Full SSL inspection.											

Parameter	Description	Type	Size	Default								
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the cipher is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the cipher is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the negotiation is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the negotiation is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											

config https

Parameter	Description	Type	Size	Default								
cert-probe-failure	Action based on certificate probe failure.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when unable to retrieve server's certificate for inspection.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when unable to retrieve server's certificate for inspection.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when unable to retrieve server's certificate for inspection.	<i>block</i>	Block the session when unable to retrieve server's certificate for inspection.					
Option	Description											
<i>allow</i>	Bypass the session when unable to retrieve server's certificate for inspection.											
<i>block</i>	Block the session when unable to retrieve server's certificate for inspection.											
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											

Parameter	Description	Type	Size	Default								
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
client-certificate	Action based on received client certificate.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td> </tr> <tr> <td><i>strict</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>certificate-inspection</i></td> <td>Inspect SSL handshake only.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>certificate-inspection</i>	Inspect SSL handshake only.	<i>deep-inspection</i>	Full SSL inspection.			
Option	Description											
<i>disable</i>	Disable.											
<i>certificate-inspection</i>	Inspect SSL handshake only.											
<i>deep-inspection</i>	Full SSL inspection.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the cipher is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the cipher is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the negotiation is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the negotiation is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											

config imaps

Parameter	Description	Type	Size	Default								
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
client-certificate	Action based on received client certificate.	option	-	inspect								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											

Parameter	Description	Type	Size	Default								
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td> </tr> <tr> <td><i>strict</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.					
Option	Description											
<i>disable</i>	Disable.											
<i>deep-inspection</i>	Full SSL inspection.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the cipher is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the cipher is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the negotiation is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the negotiation is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											

Parameter	Description	Type	Size	Default
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		

config pop3s

Parameter	Description	Type	Size	Default
cert-validation-failure	Action based on certificate validation failure.	option	-	block
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
client-certificate	Action based on received client certificate.	option	-	inspect
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
expired-server-cert	Action based on server certificate is expired.	option	-	block
	Option	Description		
	<i>allow</i>	Allow the server certificate.		

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.					
Option	Description											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td> </tr> <tr> <td><i>strict</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.					
Option	Description											
<i>disable</i>	Disable.											
<i>deep-inspection</i>	Full SSL inspection.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the cipher is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the cipher is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the negotiation is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the negotiation is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											

config smtps

Parameter	Description	Type	Size	Default								
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
client-certificate	Action based on received client certificate.	option	-	inspect								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td> </tr> <tr> <td><i>strict</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											

Parameter	Description	Type	Size	Default								
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.					
Option	Description											
<i>disable</i>	Disable.											
<i>deep-inspection</i>	Full SSL inspection.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the cipher is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the cipher is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the negotiation is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the negotiation is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											

config ssh

Parameter	Description	Type	Size	Default						
inspect-all	Level of SSL inspection.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.			
Option	Description									
<i>disable</i>	Disable.									
<i>deep-inspection</i>	Full SSL inspection.									
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ssh-algorithm	Relative strength of encryption algorithms accepted during negotiation.	option	-	compatible						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>compatible</i></td> <td>Allow a broader set of encryption algorithms for best compatibility.</td> </tr> <tr> <td><i>high-encryption</i></td> <td>Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.</td> </tr> </tbody> </table>	Option	Description	<i>compatible</i>	Allow a broader set of encryption algorithms for best compatibility.	<i>high-encryption</i>	Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.			
Option	Description									
<i>compatible</i>	Allow a broader set of encryption algorithms for best compatibility.									
<i>high-encryption</i>	Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.									
ssh-tun-policy-check	Enable/disable SSH tunnel policy check.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SSH tunnel policy check.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SSH tunnel policy check.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SSH tunnel policy check.	<i>enable</i>	Enable SSH tunnel policy check.			
Option	Description									
<i>disable</i>	Disable SSH tunnel policy check.									
<i>enable</i>	Enable SSH tunnel policy check.									
status	Configure protocol inspection status.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.			
Option	Description									
<i>disable</i>	Disable.									
<i>deep-inspection</i>	Full SSL inspection.									
unsupported-version	Action based on SSH version being unsupported.	option	-	bypass						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>block</i>	Block the session.			
Option	Description									
<i>bypass</i>	Bypass the session.									
<i>block</i>	Block the session.									

config ssl

Parameter	Description	Type	Size	Default				
cert-validation-failure	Action based on certificate validation failure.	option	-	block				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.			
Option	Description							
<i>allow</i>	Allow the server certificate.							

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.					
Option	Description											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
client-certificate	Action based on received client certificate.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
inspect-all	Level of SSL inspection.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>certificate-inspection</i></td> <td>Inspect SSL handshake only.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>certificate-inspection</i>	Inspect SSL handshake only.	<i>deep-inspection</i>	Full SSL inspection.			
Option	Description											
<i>disable</i>	Disable.											
<i>certificate-inspection</i>	Inspect SSL handshake only.											
<i>deep-inspection</i>	Full SSL inspection.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td> </tr> <tr> <td><i>strict</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the cipher is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the cipher is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the negotiation is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the negotiation is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											

config ssl-exempt

Parameter	Description	Type	Size	Default										
address	IPv4 address object.	string	Maximum length: 79											
fortiguard-category	FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 255	0										
id	ID number.	integer	Minimum value: 0 Maximum value: 512	0										
regex	Exempt servers by regular expression.	string	Maximum length: 255											
type	Type of address object or FortiGuard category.	option	-	fortiguard-category										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortiguard-category</i></td> <td>FortiGuard category.</td> </tr> <tr> <td><i>address</i></td> <td>Firewall IPv4 address.</td> </tr> <tr> <td><i>wildcard-fqdn</i></td> <td>Fully Qualified Domain Name with wildcard characters.</td> </tr> <tr> <td><i>regex</i></td> <td>Regular expression FQDN.</td> </tr> </tbody> </table>	Option	Description	<i>fortiguard-category</i>	FortiGuard category.	<i>address</i>	Firewall IPv4 address.	<i>wildcard-fqdn</i>	Fully Qualified Domain Name with wildcard characters.	<i>regex</i>	Regular expression FQDN.			
Option	Description													
<i>fortiguard-category</i>	FortiGuard category.													
<i>address</i>	Firewall IPv4 address.													
<i>wildcard-fqdn</i>	Fully Qualified Domain Name with wildcard characters.													
<i>regex</i>	Regular expression FQDN.													
wildcard-fqdn	Exempt servers by wildcard FQDN.	string	Maximum length: 79											

config ssl-server

Parameter	Description	Type	Size	Default								
ftps-client-certificate	Action based on received client certificate during the FTPS handshake.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
https-client-certificate	Action based on received client certificate during the HTTPS handshake.	option	-	bypass								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
id	SSL server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
imaps-client-certificate	Action based on received client certificate during the IMAPS handshake.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified	0.0.0.0								
pop3s-client-certificate	Action based on received client certificate during the POP3S handshake.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
smtps-client-certificate	Action based on received client certificate during the SMTPS handshake.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											

Parameter	Description	Type	Size	Default								
ssl-other-client-certificate	Action based on received client certificate during an SSL protocol handshake.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											

config firewall vip

Configure virtual IP for IPv4.

Syntax

```
config firewall vip
  edit <name>
    set comment {var-string}
    set extintf {string}
    set extip {user}
    set extport {user}
    set id {integer}
    set mappedip <range1>, <range2>, ...
    set mappedport {user}
    set portforward [disable|enable]
    set portmapping-type [1-to-1|m-to-n]
    set protocol [tcp|udp|...]
    set service <name1>, <name2>, ...
    set type [static-nat|access-proxy]
  next
end
```

Parameters

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
extintf	Interface connected to the source network that receives the packets that will be forwarded to the destination network.	string	Maximum length: 35	
extip	IP address or address range on the external interface that you want to map to an address or address range on the destination network.	user	Not Specified	

Parameter	Description	Type	Size	Default										
extport	Incoming port number range that you want to map to a port number range on the destination network.	user	Not Specified											
id	Custom defined ID.	integer	Minimum value: 0 Maximum value: 65535	0										
mappedip <range>	IP address or address range on the destination network to which the external IP address is mapped. Mapped IP range.	string	Maximum length: 79											
mappedport	Port number range on the destination network to which the external port number range is mapped.	user	Not Specified											
name	Virtual IP name.	string	Maximum length: 79											
portforward	Enable/disable port forwarding.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable port forward.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable port forward.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable port forward.	<i>enable</i>	Enable port forward.							
Option	Description													
<i>disable</i>	Disable port forward.													
<i>enable</i>	Enable port forward.													
portmapping-type	Port mapping type.	option	-	1-to-1										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>1-to-1</i></td> <td>One to one.</td> </tr> <tr> <td><i>m-to-n</i></td> <td>Many to many.</td> </tr> </tbody> </table>	Option	Description	<i>1-to-1</i>	One to one.	<i>m-to-n</i>	Many to many.							
Option	Description													
<i>1-to-1</i>	One to one.													
<i>m-to-n</i>	Many to many.													
protocol	Protocol to use when forwarding packets.	option	-	tcp										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tcp</i></td> <td>TCP.</td> </tr> <tr> <td><i>udp</i></td> <td>UDP.</td> </tr> <tr> <td><i>sctp</i></td> <td>SCTP.</td> </tr> <tr> <td><i>icmp</i></td> <td>ICMP.</td> </tr> </tbody> </table>	Option	Description	<i>tcp</i>	TCP.	<i>udp</i>	UDP.	<i>sctp</i>	SCTP.	<i>icmp</i>	ICMP.			
Option	Description													
<i>tcp</i>	TCP.													
<i>udp</i>	UDP.													
<i>sctp</i>	SCTP.													
<i>icmp</i>	ICMP.													
service <name>	Service name. Service name.	string	Maximum length: 79											
type	Configure a static NAT or access proxy.	option	-	static-nat										

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static-nat</i></td> <td>Static NAT.</td> </tr> <tr> <td><i>access-proxy</i></td> <td>Access proxy.</td> </tr> </tbody> </table>	Option	Description	<i>static-nat</i>	Static NAT.	<i>access-proxy</i>	Access proxy.			
Option	Description									
<i>static-nat</i>	Static NAT.									
<i>access-proxy</i>	Access proxy.									

config firewall wildcard-fqdn custom

Config Wildcard FQDN address.

Syntax

```
config firewall wildcard-fqdn custom
  edit <name>
    set comment {var-string}
    set wildcard-fqdn {string}
  next
end
```

config firewall wildcard-fqdn custom

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	Address name.	string	Maximum length: 79	
wildcard-fqdn	Wildcard FQDN.	string	Maximum length: 255	

ips

This section includes syntax for the following commands:

- [config ips global on page 112](#)
- [config ips rule on page 115](#)
- [config ips sensor on page 117](#)
- [config ips settings on page 122](#)

config ips global

Configure IPS global parameter.

Syntax

```
config ips global
  set anomaly-mode [periodical|continuous]
  set database [regular|extended]
  set deep-app-insp-db-limit {integer}
  set deep-app-insp-timeout {integer}
  set engine-count {integer}
  set exclude-signatures [none|industrial]
  set fail-open [enable|disable]
  set ngfw-max-scan-range {integer}
  set packet-log-queue-depth {integer}
  set session-limit-mode [accurate|heuristic]
  set socket-size {integer}
  set sync-session-ttl [enable|disable]
  config tls-active-probe
    Description: TLS active probe configuration.
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set source-ip {ipv4-address}
  end
  set traffic-submit [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default
anomaly-mode	Global blocking mode for rate-based anomalies.	option	-	continuous

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>periodical</i></td> <td>After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.</td> </tr> <tr> <td><i>continuous</i></td> <td>Block packets once an anomaly is detected. Overrides individual anomaly settings.</td> </tr> </tbody> </table>	Option	Description	<i>periodical</i>	After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.	<i>continuous</i>	Block packets once an anomaly is detected. Overrides individual anomaly settings.			
Option	Description									
<i>periodical</i>	After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.									
<i>continuous</i>	Block packets once an anomaly is detected. Overrides individual anomaly settings.									
database	Regular or extended IPS database. Regular protects against the latest common and in-the-wild attacks. Extended includes protection from legacy attacks.	option	-	regular						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>regular</i></td> <td>IPS regular database package.</td> </tr> <tr> <td><i>extended</i></td> <td>IPS extended database package.</td> </tr> </tbody> </table>	Option	Description	<i>regular</i>	IPS regular database package.	<i>extended</i>	IPS extended database package.			
Option	Description									
<i>regular</i>	IPS regular database package.									
<i>extended</i>	IPS extended database package.									
deep-app-insp-db-limit	Limit on number of entries in deep application inspection database	integer	Minimum value: 0 Maximum value: 2147483647	0						
deep-app-insp-timeout	Timeout for Deep application inspection.	integer	Minimum value: 0 Maximum value: 2147483647	0						
engine-count	Number of IPS engines running. If set to the default value of 0, FortiOS sets the number to optimize performance depending on the number of CPU cores.	integer	Minimum value: 0 Maximum value: 255	0						
exclude-signatures	Excluded signatures.	option	-	industrial						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No signatures excluded.</td> </tr> <tr> <td><i>industrial</i></td> <td>Exclude industrial signatures.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No signatures excluded.	<i>industrial</i>	Exclude industrial signatures.			
Option	Description									
<i>none</i>	No signatures excluded.									
<i>industrial</i>	Exclude industrial signatures.									
fail-open	Enable to allow traffic if the IPS process crashes. Default is disable and IPS traffic is blocked when the IPS process crashes.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPS fail open.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPS fail open.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPS fail open.	<i>disable</i>	Disable IPS fail open.			
Option	Description									
<i>enable</i>	Enable IPS fail open.									
<i>disable</i>	Disable IPS fail open.									
ngfw-max-scan-range	NGFW policy-mode app detection threshold.	integer	Minimum value: 0 Maximum value: 4294967295	4096						
packet-log-queue-depth	Packet/pcap log queue depth per IPS engine.	integer	Minimum value: 128 Maximum value: 4096	128						
session-limit-mode	Method of counting concurrent sessions used by session limit anomalies. Choose between greater accuracy (accurate) or improved performance (heuristics).	option	-	heuristic						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accurate</i></td> <td>Accurately count concurrent sessions, demands more resources.</td> </tr> <tr> <td><i>heuristic</i></td> <td>Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.</td> </tr> </tbody> </table>	Option	Description	<i>accurate</i>	Accurately count concurrent sessions, demands more resources.	<i>heuristic</i>	Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.			
Option	Description									
<i>accurate</i>	Accurately count concurrent sessions, demands more resources.									
<i>heuristic</i>	Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.									
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: 512	256						
sync-session-ttl	Enable/disable use of kernel session TTL for IPS sessions.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of kernel session TTL for IPS sessions.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of kernel session TTL for IPS sessions.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of kernel session TTL for IPS sessions.	<i>disable</i>	Disable use of kernel session TTL for IPS sessions.			
Option	Description									
<i>enable</i>	Enable use of kernel session TTL for IPS sessions.									
<i>disable</i>	Disable use of kernel session TTL for IPS sessions.									
traffic-submit	Enable/disable submitting attack data found by this Container FortiOS to FortiGuard.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable traffic submit.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable traffic submit.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable traffic submit.	<i>disable</i>	Disable traffic submit.			
Option	Description									
<i>enable</i>	Enable traffic submit.									
<i>disable</i>	Disable traffic submit.									

config tls-active-probe

Parameter	Description	Type	Size	Default								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></tbody></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
source-ip	Source IP address used for TLS active probe.	ipv4-address	Not Specified	0.0.0.0								

config ips rule

Configure IPS rules. Read-only.

This table cannot be edited.

Syntax

```
config ips rule
  edit <name>
    get
  next
end
```

Parameters

Parameter	Description	Type	Size	Default						
action	Action.	option	-	pass						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>pass</i></td><td>Pass or allow matching traffic.</td></tr><tr><td><i>block</i></td><td>Block or drop matching traffic.</td></tr></tbody></table>	Option	Description	<i>pass</i>	Pass or allow matching traffic.	<i>block</i>	Block or drop matching traffic.			
Option	Description									
<i>pass</i>	Pass or allow matching traffic.									
<i>block</i>	Block or drop matching traffic.									
application	Vulnerable applications.	user	Not Specified							

Parameter	Description	Type	Size	Default
date	Date.	integer	Minimum value: 0 Maximum value: 4294967295	0
group	Group.	string	Maximum length: 63	
location	Vulnerable location.	user	Not Specified	
log	Enable/disable logging.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable logging.		
	<i>enable</i>	Enable logging.		
log-packet	Enable/disable packet logging.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable packet logging.		
	<i>enable</i>	Enable packet logging.		
name	Rule name.	string	Maximum length: 63	
os	Vulnerable operation systems.	user	Not Specified	
rev	Revision.	integer	Minimum value: 0 Maximum value: 4294967295	0
rule-id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
service	Vulnerable service.	user	Not Specified	
severity	Severity.	user	Not Specified	
status	Enable/disable status.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		

config ips sensor

Configure IPS sensor.

Syntax

```
config ips sensor
  edit <name>
    set block-malicious-url [disable|enable]
    set comment {var-string}
    config entries
      Description: IPS sensor filter.
      edit <id>
        set action [pass|block|...]
        set application {user}
        set cve <cve-entry1>, <cve-entry2>, ...
        config exempt-ip
          Description: Traffic from selected source or destination IP addresses is
          exempt from this signature.
          edit <id>
            set dst-ip {ipv4-classnet}
            set src-ip {ipv4-classnet}
          next
        end
        set location {user}
        set log [disable|enable]
        set log-attack-context [disable|enable]
        set log-packet [disable|enable]
        set os {user}
        set protocol {user}
        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]
        set rate-count {integer}
        set rate-duration {integer}
        set rate-mode [periodical|continuous]
        set rate-track [none|src-ip|...]
        set rule <id1>, <id2>, ...
        set severity {user}
        set status [disable|enable|...]
      next
    end
    set extended-log [enable|disable]
    set replacemsg-group {string}
    set scan-botnet-connections [disable|block|...]
  next
end
```

Parameters

Parameter	Description	Type	Size	Default								
block-malicious-url	Enable/disable malicious URL blocking.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable malicious URL blocking.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable malicious URL blocking.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable malicious URL blocking.	<i>enable</i>	Enable malicious URL blocking.					
Option	Description											
<i>disable</i>	Disable malicious URL blocking.											
<i>enable</i>	Enable malicious URL blocking.											
comment	Comment.	var-string	Maximum length: 255									
extended-log	Enable/disable extended logging.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
name	Sensor name.	string	Maximum length: 35									
replacemsg-group	Replacement message group.	string	Maximum length: 35									
scan-botnet-connections	Block or monitor connections to Botnet servers, or disable Botnet scanning.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not scan connections to botnet servers.</td> </tr> <tr> <td><i>block</i></td> <td>Block connections to botnet servers.</td> </tr> <tr> <td><i>monitor</i></td> <td>Log connections to botnet servers.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not scan connections to botnet servers.	<i>block</i>	Block connections to botnet servers.	<i>monitor</i>	Log connections to botnet servers.			
Option	Description											
<i>disable</i>	Do not scan connections to botnet servers.											
<i>block</i>	Block connections to botnet servers.											
<i>monitor</i>	Log connections to botnet servers.											

config entries

Parameter	Description	Type	Size	Default						
action	Action taken with traffic in which signatures are detected.	option	-	default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Pass or allow matching traffic.</td> </tr> <tr> <td><i>block</i></td> <td>Block or drop matching traffic.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Pass or allow matching traffic.	<i>block</i>	Block or drop matching traffic.			
Option	Description									
<i>pass</i>	Pass or allow matching traffic.									
<i>block</i>	Block or drop matching traffic.									

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>reset</i></td> <td>Reset sessions for matching traffic.</td> </tr> <tr> <td><i>default</i></td> <td>Pass or drop matching traffic, depending on the default action of the signature.</td> </tr> </tbody> </table>	Option	Description	<i>reset</i>	Reset sessions for matching traffic.	<i>default</i>	Pass or drop matching traffic, depending on the default action of the signature.			
Option	Description									
<i>reset</i>	Reset sessions for matching traffic.									
<i>default</i>	Pass or drop matching traffic, depending on the default action of the signature.									
application	Applications to be protected. set application ? lists available applications. all includes all applications. other includes all unlisted applications.	user	Not Specified	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							
id	Rule ID in IPS database.	integer	Minimum value: 0 Maximum value: 4294967295	0						
location	Protect client or server traffic.	user	Not Specified	all						
log	Enable/disable logging of signatures included in filter.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging of selected rules.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging of selected rules.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging of selected rules.	<i>enable</i>	Enable logging of selected rules.			
Option	Description									
<i>disable</i>	Disable logging of selected rules.									
<i>enable</i>	Enable logging of selected rules.									
log-attack-context	Enable/disable logging of attack context: URL buffer, header buffer, body buffer, packet buffer.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging of detailed attack context.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging of detailed attack context.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging of detailed attack context.	<i>enable</i>	Enable logging of detailed attack context.			
Option	Description									
<i>disable</i>	Disable logging of detailed attack context.									
<i>enable</i>	Enable logging of detailed attack context.									
log-packet	Enable/disable packet logging. Enable to save the packet that triggers the filter. You can download the packets in pcap format for diagnostic use.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable packet logging of selected rules.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable packet logging of selected rules.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable packet logging of selected rules.	<i>enable</i>	Enable packet logging of selected rules.			
Option	Description									
<i>disable</i>	Disable packet logging of selected rules.									
<i>enable</i>	Enable packet logging of selected rules.									

Parameter	Description	Type	Size	Default						
os	Operating systems to be protected. all includes all operating systems. other includes all unlisted operating systems.	user	Not Specified	all						
protocol	Protocols to be examined. set protocol ? lists available protocols. all includes all protocols. other includes all unlisted protocols.	user	Not Specified	all						
quarantine	Quarantine method.	option	-	none						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Quarantine is disabled.</td> </tr> <tr> <td><i>attacker</i></td> <td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.			
Option	Description									
<i>none</i>	Quarantine is disabled.									
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
quarantine-expiry	Duration of quarantine. Requires quarantine set to attacker.	user	Not Specified	5m						
quarantine-log	Enable/disable quarantine logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable quarantine logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable quarantine logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable quarantine logging.	<i>enable</i>	Enable quarantine logging.			
Option	Description									
<i>disable</i>	Disable quarantine logging.									
<i>enable</i>	Enable quarantine logging.									
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						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>periodical</i></td> <td>Allow configured number of packets every rate-duration.</td> </tr> <tr> <td><i>continuous</i></td> <td>Block packets once the rate is reached.</td> </tr> </tbody> </table>	Option	Description	<i>periodical</i>	Allow configured number of packets every rate-duration.	<i>continuous</i>	Block packets once the rate is reached.			
Option	Description									
<i>periodical</i>	Allow configured number of packets every rate-duration.									
<i>continuous</i>	Block packets once the rate is reached.									
rate-track	Track the packet protocol field.	option	-	none						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>none</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	none					
Option	Description									
<i>none</i>	none									

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>src-ip</i></td> <td>Source IP.</td> </tr> <tr> <td><i>dest-ip</i></td> <td>Destination IP.</td> </tr> <tr> <td><i>dhcp-client-mac</i></td> <td>DHCP client.</td> </tr> <tr> <td><i>dns-domain</i></td> <td>DNS domain.</td> </tr> </tbody> </table>	Option	Description	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.	<i>dhcp-client-mac</i>	DHCP client.	<i>dns-domain</i>	DNS domain.			
Option	Description													
<i>src-ip</i>	Source IP.													
<i>dest-ip</i>	Destination IP.													
<i>dhcp-client-mac</i>	DHCP client.													
<i>dns-domain</i>	DNS domain.													
rule <id>	Identifies the predefined or custom IPS signatures to add to the sensor. Rule IPS.	integer	Minimum value: 0 Maximum value: 4294967295											
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified	all										
status	Status of the signatures included in filter. default enables the filter and only use filters with default status of enable. Filters with default status of disable will not be used.	option	-	default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status of selected rules.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status of selected rules.</td> </tr> <tr> <td><i>default</i></td> <td>Default.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status of selected rules.	<i>enable</i>	Enable status of selected rules.	<i>default</i>	Default.					
Option	Description													
<i>disable</i>	Disable status of selected rules.													
<i>enable</i>	Enable status of selected rules.													
<i>default</i>	Default.													

config exempt-ip

Parameter	Description	Type	Size	Default
dst-ip	Destination IP address and netmask.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
id	Exempt IP ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
src-ip	Source IP address and netmask.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config ips settings

Configure IPS parameter.

Syntax

```
config ips settings
  set ips-packet-quota {integer}
  set packet-log-history {integer}
  set packet-log-memory {integer}
  set packet-log-post-attack {integer}
end
```

Parameters

Parameter	Description	Type	Size	Default
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
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-memory	Maximum memory can be used by packet log.	integer	Minimum value: 64 Maximum value: 8192	256
packet-log-post-attack	Number of packets to log after the IPS signature is detected.	integer	Minimum value: 0 Maximum value: 255	0

log

This section includes syntax for the following commands:

- [config log custom-field on page 123](#)
- [config log disk setting on page 124](#)
- [config log memory global-setting on page 129](#)
- [config log memory setting on page 130](#)
- [config log setting on page 130](#)
- [config log syslogd2 filter on page 132](#)
- [config log syslogd2 setting on page 134](#)
- [config log syslogd3 filter on page 138](#)
- [config log syslogd3 setting on page 140](#)
- [config log syslogd4 filter on page 144](#)
- [config log syslogd4 setting on page 146](#)
- [config log syslogd filter on page 150](#)
- [config log syslogd setting on page 152](#)

config log custom-field

Configure custom log fields.

Syntax

```
config log custom-field
  edit <id>
    set name {string}
    set value {string}
  next
end
```

config log custom-field

Parameter	Description	Type	Size	Default
id	field ID <string>.	string	Maximum length: 35	
name	Field name (max: 15 characters).	string	Maximum length: 15	
value	Field value (max: 63 characters).	string	Maximum length: 63	

config log disk setting

Settings for local disk logging.

Syntax

```
config log disk setting
  set diskfull [overwrite|nolog]
  set dlp-archive-quota {integer}
  set full-final-warning-threshold {integer}
  set full-first-warning-threshold {integer}
  set full-second-warning-threshold {integer}
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set ips-archive [enable|disable]
  set log-quota {integer}
  set max-log-file-size {integer}
  set max-policy-packet-capture-size {integer}
  set maximum-log-age {integer}
  set report-quota {integer}
  set roll-day {option1}, {option2}, ...
  set roll-schedule [daily|weekly]
  set roll-time {user}
  set source-ip {ipv4-address}
  set status [enable|disable]
  set upload [enable|disable]
  set upload-delete-files [enable|disable]
  set upload-destination {option}
  set upload-ssl-conn [default|high|...]
  set uploaddir {string}
  set uploadip {ipv4-address}
  set uploadpass {password}
  set uploadport {integer}
  set uploadsched [disable|enable]
  set uploadtime {user}
  set uploadtype {option1}, {option2}, ...
  set uploaduser {string}
end
```

Parameters

Parameter	Description	Type	Size	Default
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

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>overwrite</i></td> <td>Overwrite the oldest logs when the log disk is full.</td> </tr> <tr> <td><i>nolog</i></td> <td>Stop logging when the log disk is full.</td> </tr> </tbody> </table>	Option	Description	<i>overwrite</i>	Overwrite the oldest logs when the log disk is full.	<i>nolog</i>	Stop logging when the log disk is full.					
Option	Description											
<i>overwrite</i>	Overwrite the oldest logs when the log disk is full.											
<i>nolog</i>	Stop logging when the log disk is full.											
dlp-archive-quota	DLP archive quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0								
full-final-warning-threshold	Log full final warning threshold as a percent.	integer	Minimum value: 3 Maximum value: 100	95								
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								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
ips-archive	Enable/disable IPS packet archiving to the local disk.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPS packet archiving.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPS packet archiving.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPS packet archiving.	<i>disable</i>	Disable IPS packet archiving.					
Option	Description											
<i>enable</i>	Enable IPS packet archiving.											
<i>disable</i>	Disable IPS packet archiving.											

Parameter	Description	Type	Size	Default																
log-quota	Disk log quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0																
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																
maximum-log-age	Delete log files older than (days).	integer	Minimum value: 0 Maximum value: 3650	7																
report-quota	Report quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0																
roll-day	Day of week on which to roll log file.	option	-	sunday																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sunday</i></td> <td>Sunday</td> </tr> <tr> <td><i>monday</i></td> <td>Monday</td> </tr> <tr> <td><i>tuesday</i></td> <td>Tuesday</td> </tr> <tr> <td><i>wednesday</i></td> <td>Wednesday</td> </tr> <tr> <td><i>thursday</i></td> <td>Thursday</td> </tr> <tr> <td><i>friday</i></td> <td>Friday</td> </tr> <tr> <td><i>saturday</i></td> <td>Saturday</td> </tr> </tbody> </table>	Option	Description	<i>sunday</i>	Sunday	<i>monday</i>	Monday	<i>tuesday</i>	Tuesday	<i>wednesday</i>	Wednesday	<i>thursday</i>	Thursday	<i>friday</i>	Friday	<i>saturday</i>	Saturday			
Option	Description																			
<i>sunday</i>	Sunday																			
<i>monday</i>	Monday																			
<i>tuesday</i>	Tuesday																			
<i>wednesday</i>	Wednesday																			
<i>thursday</i>	Thursday																			
<i>friday</i>	Friday																			
<i>saturday</i>	Saturday																			
roll-schedule	Frequency to check log file for rolling.	option	-	daily																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>daily</i></td> <td>Check the log file once a day.</td> </tr> <tr> <td><i>weekly</i></td> <td>Check the log file once a week.</td> </tr> </tbody> </table>	Option	Description	<i>daily</i>	Check the log file once a day.	<i>weekly</i>	Check the log file once a week.													
Option	Description																			
<i>daily</i>	Check the log file once a day.																			
<i>weekly</i>	Check the log file once a week.																			

Parameter	Description	Type	Size	Default
roll-time	Time of day to roll the log file (hh:mm).	user	Not Specified	
source-ip	Source IP address to use for uploading disk log files.	ipv4-address	Not Specified	0.0.0.0
status	Enable/disable local disk logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Log to local disk.		
	<i>disable</i>	Do not log to local disk.		
upload	Enable/disable uploading log files when they are rolled.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable uploading log files when they are rolled.		
	<i>disable</i>	Disable uploading log files when they are rolled.		
upload-delete-files	Delete log files after uploading.	option	-	enable
	Option	Description		
	<i>enable</i>	Delete log files after uploading.		
	<i>disable</i>	Do not delete log files after uploading.		
upload-destination	The type of server to upload log files to. Only FTP is currently supported.	option	-	ftp-server
	Option	Description		
	<i>ftp-server</i>	Upload rolled log files to an FTP server.		
upload-ssl-conn	Enable/disable encrypted FTPS communication to upload log files.	option	-	default
	Option	Description		
	<i>default</i>	FTPS with high and medium encryption algorithms.		
	<i>high</i>	FTPS with high encryption algorithms.		
	<i>low</i>	FTPS with low encryption algorithms.		
	<i>disable</i>	Disable FTPS communication.		
uploaddir	The remote directory on the FTP server to upload log files to.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default																				
uploadip	IP address of the FTP server to upload log files to.	ipv4-address	Not Specified	0.0.0.0																				
uploadpass	Password required to log into the FTP server to upload disk log files.	password	Not Specified																					
uploadport	TCP port to use for communicating with the FTP server.	integer	Minimum value: 0 Maximum value: 65535	21																				
uploadsched	Set the schedule for uploading log files to the FTP server.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Upload when rolling.</td> </tr> <tr> <td><i>enable</i></td> <td>Scheduled upload.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Upload when rolling.	<i>enable</i>	Scheduled upload.																	
Option	Description																							
<i>disable</i>	Upload when rolling.																							
<i>enable</i>	Scheduled upload.																							
uploadtime	Time of day at which log files are uploaded if uploadsched is enabled (hh:mm or hh).	user	Not Specified																					
uploadtype	Types of log files to upload. Separate multiple entries with a space.	option	-	traffic event virus webfilter IPS emailfilter dlp-archive anomaly voip dlp app-ctrl waf dns ssh ssl																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>traffic</i></td> <td>Upload traffic log.</td> </tr> <tr> <td><i>event</i></td> <td>Upload event log.</td> </tr> <tr> <td><i>virus</i></td> <td>Upload anti-virus log.</td> </tr> <tr> <td><i>webfilter</i></td> <td>Upload web filter log.</td> </tr> <tr> <td><i>IPS</i></td> <td>Upload IPS log.</td> </tr> <tr> <td><i>emailfilter</i></td> <td>Upload spam filter log.</td> </tr> <tr> <td><i>dlp-archive</i></td> <td>Upload DLP archive.</td> </tr> <tr> <td><i>anomaly</i></td> <td>Upload anomaly log.</td> </tr> <tr> <td><i>voip</i></td> <td>Upload VoIP log.</td> </tr> </tbody> </table>	Option	Description	<i>traffic</i>	Upload traffic log.	<i>event</i>	Upload event log.	<i>virus</i>	Upload anti-virus log.	<i>webfilter</i>	Upload web filter log.	<i>IPS</i>	Upload IPS log.	<i>emailfilter</i>	Upload spam filter log.	<i>dlp-archive</i>	Upload DLP archive.	<i>anomaly</i>	Upload anomaly log.	<i>voip</i>	Upload VoIP log.			
Option	Description																							
<i>traffic</i>	Upload traffic log.																							
<i>event</i>	Upload event log.																							
<i>virus</i>	Upload anti-virus log.																							
<i>webfilter</i>	Upload web filter log.																							
<i>IPS</i>	Upload IPS log.																							
<i>emailfilter</i>	Upload spam filter log.																							
<i>dlp-archive</i>	Upload DLP archive.																							
<i>anomaly</i>	Upload anomaly log.																							
<i>voip</i>	Upload VoIP log.																							

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>dlp</i></td> <td>Upload DLP log.</td> </tr> <tr> <td><i>app-ctrl</i></td> <td>Upload application control log.</td> </tr> <tr> <td><i>waf</i></td> <td>Upload web application firewall log.</td> </tr> <tr> <td><i>dns</i></td> <td>Upload DNS log.</td> </tr> <tr> <td><i>ssh</i></td> <td>Upload SSH log.</td> </tr> <tr> <td><i>ssl</i></td> <td>Upload SSL log.</td> </tr> <tr> <td><i>file-filter</i></td> <td>Upload file-filter log.</td> </tr> <tr> <td><i>icap</i></td> <td>Upload ICAP log.</td> </tr> <tr> <td><i>ztna</i></td> <td>Upload ZTNA log.</td> </tr> </tbody> </table>	Option	Description	<i>dlp</i>	Upload DLP log.	<i>app-ctrl</i>	Upload application control log.	<i>waf</i>	Upload web application firewall log.	<i>dns</i>	Upload DNS log.	<i>ssh</i>	Upload SSH log.	<i>ssl</i>	Upload SSL log.	<i>file-filter</i>	Upload file-filter log.	<i>icap</i>	Upload ICAP log.	<i>ztna</i>	Upload ZTNA log.			
Option	Description																							
<i>dlp</i>	Upload DLP log.																							
<i>app-ctrl</i>	Upload application control log.																							
<i>waf</i>	Upload web application firewall log.																							
<i>dns</i>	Upload DNS log.																							
<i>ssh</i>	Upload SSH log.																							
<i>ssl</i>	Upload SSL log.																							
<i>file-filter</i>	Upload file-filter log.																							
<i>icap</i>	Upload ICAP log.																							
<i>ztna</i>	Upload ZTNA log.																							
uploaduser	Username required to log into the FTP server to upload disk log files.	string	Maximum length: 35																					

config log memory global-setting

Global settings for memory logging.

Syntax

```
config log memory global-setting
  set full-final-warning-threshold {integer}
  set full-first-warning-threshold {integer}
  set full-second-warning-threshold {integer}
  set max-size {integer}
end
```

config log memory global-setting

Parameter	Description	Type	Size	Default
full-final-warning-threshold	Log full final warning threshold as a percent.	integer	Minimum value: 3 Maximum value: 100	95
full-first-warning-threshold	Log full first warning threshold as a percent.	integer	Minimum value: 1 Maximum value: 98	75

Parameter	Description	Type	Size	Default
full-second-warning-threshold	Log full second warning threshold as a percent.	integer	Minimum value: 2 Maximum value: 99	90
max-size	Maximum amount of memory that can be used for memory logging in bytes.	integer	Minimum value: 0 Maximum value: 268435456	67108864

config log memory setting

Settings for memory buffer.

Syntax

```
config log memory setting
    set status [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default
status	Enable/disable logging to Container FortiOS memory.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to memory.		
	<i>disable</i>	Disable logging to memory.		

config log setting

Configure general log settings.

Syntax

```
config log setting
    set custom-log-fields <field-id1>, <field-id2>, ...
    set expolicy-implicit-log [enable|disable]
    set fwpolicy-implicit-log [enable|disable]
    set fwpolicy6-implicit-log [enable|disable]
    set log-policy-comment [enable|disable]
    set resolve-ip [enable|disable]
```

```

set resolve-port [enable|disable]
set syslog-override [enable|disable]
end

```

Parameters

Parameter	Description	Type	Size	Default						
custom-log-fields <field-id>	Custom fields to append to all log messages. Custom log field.	string	Maximum length: 35							
expolicy-implicit-log	Enable/disable explicit proxy firewall implicit policy logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable explicit proxy firewall implicit policy logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable explicit proxy firewall implicit policy logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable explicit proxy firewall implicit policy logging.	<i>disable</i>	Disable explicit proxy firewall implicit policy logging.			
Option	Description									
<i>enable</i>	Enable explicit proxy firewall implicit policy logging.									
<i>disable</i>	Disable explicit proxy firewall implicit policy logging.									
fwpolicy-implicit-log	Enable/disable implicit firewall policy logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable implicit firewall policy logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable implicit firewall policy logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable implicit firewall policy logging.	<i>disable</i>	Disable implicit firewall policy logging.			
Option	Description									
<i>enable</i>	Enable implicit firewall policy logging.									
<i>disable</i>	Disable implicit firewall policy logging.									
fwpolicy6-implicit-log	Enable/disable implicit firewall policy6 logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable implicit firewall policy6 logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable implicit firewall policy6 logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable implicit firewall policy6 logging.	<i>disable</i>	Disable implicit firewall policy6 logging.			
Option	Description									
<i>enable</i>	Enable implicit firewall policy6 logging.									
<i>disable</i>	Disable implicit firewall policy6 logging.									
log-policy-comment	Enable/disable inserting policy comments into traffic logs.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable inserting policy comments into traffic logs.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable inserting policy comments into traffic logs.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable inserting policy comments into traffic logs.	<i>disable</i>	Disable inserting policy comments into traffic logs.			
Option	Description									
<i>enable</i>	Enable inserting policy comments into traffic logs.									
<i>disable</i>	Disable inserting policy comments into traffic logs.									
resolve-ip	Enable/disable adding resolved domain names to traffic logs if possible.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable adding resolved domain names to traffic logs.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable adding resolved domain names to traffic logs.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable adding resolved domain names to traffic logs.	<i>disable</i>	Disable adding resolved domain names to traffic logs.			
Option	Description									
<i>enable</i>	Enable adding resolved domain names to traffic logs.									
<i>disable</i>	Disable adding resolved domain names to traffic logs.									
resolve-port	Enable/disable adding resolved service names to traffic logs.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable adding resolved service names to traffic logs.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable adding resolved service names to traffic logs.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable adding resolved service names to traffic logs.	<i>disable</i>	Disable adding resolved service names to traffic logs.			
Option	Description									
<i>enable</i>	Enable adding resolved service names to traffic logs.									
<i>disable</i>	Disable adding resolved service names to traffic logs.									
syslog-override	Enable/disable override Syslog settings.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable override Syslog settings.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable override Syslog settings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable override Syslog settings.	<i>disable</i>	Disable override Syslog settings.			
Option	Description									
<i>enable</i>	Enable override Syslog settings.									
<i>disable</i>	Disable override Syslog settings.									

config log syslogd2 filter

Filters for remote system server.

Syntax

```

config log syslogd2 filter
  set forward-traffic [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
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
end

```

Parameters

Parameter	Description	Type	Size	Default																		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
severity	Lowest severity level to log.	option	-	information																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Parameter	Description	Type	Size	Default																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>traffic</i></td> <td>Traffic log.</td> </tr> <tr> <td><i>event</i></td> <td>Event log.</td> </tr> <tr> <td><i>virus</i></td> <td>Antivirus log.</td> </tr> <tr> <td><i>webfilter</i></td> <td>Web filter log.</td> </tr> <tr> <td><i>attack</i></td> <td>Attack log.</td> </tr> <tr> <td><i>app-ctrl</i></td> <td>Application control log.</td> </tr> <tr> <td><i>ssl</i></td> <td>SSL log.</td> </tr> </tbody> </table>	Option	Description	<i>traffic</i>	Traffic log.	<i>event</i>	Event log.	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>app-ctrl</i>	Application control log.	<i>ssl</i>	SSL log.			
Option	Description																			
<i>traffic</i>	Traffic log.																			
<i>event</i>	Event log.																			
<i>virus</i>	Antivirus log.																			
<i>webfilter</i>	Web filter log.																			
<i>attack</i>	Attack log.																			
<i>app-ctrl</i>	Application control log.																			
<i>ssl</i>	SSL log.																			
filter	Free style filter string.	string	Maximum length: 1023																	
filter-type	Include/exclude logs that match the filter.	option	-	include																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.													
Option	Description																			
<i>include</i>	Include logs that match the filter.																			
<i>exclude</i>	Exclude logs that match the filter.																			
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0																

config log syslogd2 setting

Global settings for remote syslog server.

Syntax

```

config log syslogd2 setting
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set custom {string}
      set name {string}
    next
  end
  set enc-algorithm [high-medium|high|...]
  set facility [kernel|user|...]
  set format [default|csv|...]

```

```

set interface {string}
set interface-select-method [auto|sdwan|...]
set max-log-rate {integer}
set mode [udp|reliable]
set port {integer}
set priority [default|low]
set server {string}
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
end

```

Parameters

Parameter	Description	Type	Size	Default																								
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35																									
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>SSL communication with high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>SSL communication with high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>SSL communication with low encryption algorithms.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL communication.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.																	
Option	Description																											
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.																											
<i>high</i>	SSL communication with high encryption algorithms.																											
<i>low</i>	SSL communication with low encryption algorithms.																											
<i>disable</i>	Disable SSL communication.																											
facility	Remote syslog facility.	option	-	local7																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>kernel</i></td> <td>Kernel messages.</td> </tr> <tr> <td><i>user</i></td> <td>Random user-level messages.</td> </tr> <tr> <td><i>mail</i></td> <td>Mail system.</td> </tr> <tr> <td><i>daemon</i></td> <td>System daemons.</td> </tr> <tr> <td><i>auth</i></td> <td>Security/authorization messages.</td> </tr> <tr> <td><i>syslog</i></td> <td>Messages generated internally by syslog.</td> </tr> <tr> <td><i>lpr</i></td> <td>Line printer subsystem.</td> </tr> <tr> <td><i>news</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>uucp</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>cron</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>authpriv</i></td> <td>Security/authorization messages (private).</td> </tr> </tbody> </table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).			
Option	Description																											
<i>kernel</i>	Kernel messages.																											
<i>user</i>	Random user-level messages.																											
<i>mail</i>	Mail system.																											
<i>daemon</i>	System daemons.																											
<i>auth</i>	Security/authorization messages.																											
<i>syslog</i>	Messages generated internally by syslog.																											
<i>lpr</i>	Line printer subsystem.																											
<i>news</i>	Network news subsystem.																											
<i>uucp</i>	Network news subsystem.																											
<i>cron</i>	Clock daemon.																											
<i>authpriv</i>	Security/authorization messages (private).																											

Parameter	Description	Type	Size	Default																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ftp</i></td> <td>FTP daemon.</td> </tr> <tr> <td><i>ntp</i></td> <td>NTP daemon.</td> </tr> <tr> <td><i>audit</i></td> <td>Log audit.</td> </tr> <tr> <td><i>alert</i></td> <td>Log alert.</td> </tr> <tr> <td><i>clock</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>local0</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local1</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local2</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local3</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local4</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local5</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local6</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local7</i></td> <td>Reserved for local use.</td> </tr> </tbody> </table>	Option	Description	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
Option	Description																															
<i>ftp</i>	FTP daemon.																															
<i>ntp</i>	NTP daemon.																															
<i>audit</i>	Log audit.																															
<i>alert</i>	Log alert.																															
<i>clock</i>	Clock daemon.																															
<i>local0</i>	Reserved for local use.																															
<i>local1</i>	Reserved for local use.																															
<i>local2</i>	Reserved for local use.																															
<i>local3</i>	Reserved for local use.																															
<i>local4</i>	Reserved for local use.																															
<i>local5</i>	Reserved for local use.																															
<i>local6</i>	Reserved for local use.																															
<i>local7</i>	Reserved for local use.																															
format	Log format.	option	-	default																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Syslog format.</td> </tr> <tr> <td><i>csv</i></td> <td>CSV (Comma Separated Values) format.</td> </tr> <tr> <td><i>cef</i></td> <td>CEF (Common Event Format) format.</td> </tr> <tr> <td><i>rfc5424</i></td> <td>Syslog RFC5424 format.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.																					
Option	Description																															
<i>default</i>	Syslog format.																															
<i>csv</i>	CSV (Comma Separated Values) format.																															
<i>cef</i>	CEF (Common Event Format) format.																															
<i>rfc5424</i>	Syslog RFC5424 format.																															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15																													
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.																							
Option	Description																															
<i>auto</i>	Set outgoing interface automatically.																															
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.																															
<i>specify</i>	Set outgoing interface manually.																															

Parameter	Description	Type	Size	Default												
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0												
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>udp</i></td> <td>Enable syslogging over UDP.</td> </tr> <tr> <td><i>reliable</i></td> <td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td> </tr> </tbody> </table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).									
Option	Description															
<i>udp</i>	Enable syslogging over UDP.															
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).															
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514												
priority	Set log transmission priority.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set Syslog transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set Syslog transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.									
Option	Description															
<i>default</i>	Set Syslog transmission priority to default.															
<i>low</i>	Set Syslog transmission priority to low.															
server	Address of remote syslog server.	string	Maximum length: 127													
source-ip	Source IP address of syslog.	string	Maximum length: 63													
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
status	Enable/disable remote syslog logging.	option	-	disable												

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Log to remote syslog server.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not log to remote syslog server.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.			
Option	Description									
<i>enable</i>	Log to remote syslog server.									
<i>disable</i>	Do not log to remote syslog server.									

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name.	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	

config log syslogd3 filter

Filters for remote system server.

Syntax

```

config log syslogd3 filter
  set forward-traffic [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
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
end

```

Parameters

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

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
severity	Lowest severity level to log.	option	-	information																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					

config free-style

Parameter	Description	Type	Size	Default				
category	Log category.	option	-	traffic				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>traffic</i></td> <td>Traffic log.</td> </tr> </tbody> </table>	Option	Description	<i>traffic</i>	Traffic log.			
Option	Description							
<i>traffic</i>	Traffic log.							

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>event</i></td> <td>Event log.</td> </tr> <tr> <td><i>virus</i></td> <td>Antivirus log.</td> </tr> <tr> <td><i>webfilter</i></td> <td>Web filter log.</td> </tr> <tr> <td><i>attack</i></td> <td>Attack log.</td> </tr> <tr> <td><i>app-ctrl</i></td> <td>Application control log.</td> </tr> <tr> <td><i>ssl</i></td> <td>SSL log.</td> </tr> </tbody> </table>	Option	Description	<i>event</i>	Event log.	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>app-ctrl</i>	Application control log.	<i>ssl</i>	SSL log.			
Option	Description																	
<i>event</i>	Event log.																	
<i>virus</i>	Antivirus log.																	
<i>webfilter</i>	Web filter log.																	
<i>attack</i>	Attack log.																	
<i>app-ctrl</i>	Application control log.																	
<i>ssl</i>	SSL log.																	
filter	Free style filter string.	string	Maximum length: 1023															
filter-type	Include/exclude logs that match the filter.	option	-	include														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.											
Option	Description																	
<i>include</i>	Include logs that match the filter.																	
<i>exclude</i>	Exclude logs that match the filter.																	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0														

config log syslogd3 setting

Global settings for remote syslog server.

Syntax

```

config log syslogd3 setting
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set custom {string}
      set name {string}
    next
  end
  set enc-algorithm [high-medium|high|...]
  set facility [kernel|user|...]
  set format [default|csv|...]
  set interface {string}
  set interface-select-method [auto|sdwan|...]

```

```

set max-log-rate {integer}
set mode [udp|reliable]
set port {integer}
set priority [default|low]
set server {string}
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
end

```

Parameters

Parameter	Description	Type	Size	Default																										
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35																											
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>SSL communication with high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>SSL communication with high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>SSL communication with low encryption algorithms.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL communication.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.																			
Option	Description																													
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.																													
<i>high</i>	SSL communication with high encryption algorithms.																													
<i>low</i>	SSL communication with low encryption algorithms.																													
<i>disable</i>	Disable SSL communication.																													
facility	Remote syslog facility.	option	-	local7																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>kernel</i></td> <td>Kernel messages.</td> </tr> <tr> <td><i>user</i></td> <td>Random user-level messages.</td> </tr> <tr> <td><i>mail</i></td> <td>Mail system.</td> </tr> <tr> <td><i>daemon</i></td> <td>System daemons.</td> </tr> <tr> <td><i>auth</i></td> <td>Security/authorization messages.</td> </tr> <tr> <td><i>syslog</i></td> <td>Messages generated internally by syslog.</td> </tr> <tr> <td><i>lpr</i></td> <td>Line printer subsystem.</td> </tr> <tr> <td><i>news</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>uucp</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>cron</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>authpriv</i></td> <td>Security/authorization messages (private).</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP daemon.</td> </tr> </tbody> </table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.			
Option	Description																													
<i>kernel</i>	Kernel messages.																													
<i>user</i>	Random user-level messages.																													
<i>mail</i>	Mail system.																													
<i>daemon</i>	System daemons.																													
<i>auth</i>	Security/authorization messages.																													
<i>syslog</i>	Messages generated internally by syslog.																													
<i>lpr</i>	Line printer subsystem.																													
<i>news</i>	Network news subsystem.																													
<i>uucp</i>	Network news subsystem.																													
<i>cron</i>	Clock daemon.																													
<i>authpriv</i>	Security/authorization messages (private).																													
<i>ftp</i>	FTP daemon.																													

Parameter	Description	Type	Size	Default																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ntp</i></td> <td>NTP daemon.</td> </tr> <tr> <td><i>audit</i></td> <td>Log audit.</td> </tr> <tr> <td><i>alert</i></td> <td>Log alert.</td> </tr> <tr> <td><i>clock</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>local0</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local1</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local2</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local3</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local4</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local5</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local6</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local7</i></td> <td>Reserved for local use.</td> </tr> </tbody> </table>	Option	Description	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
Option	Description																													
<i>ntp</i>	NTP daemon.																													
<i>audit</i>	Log audit.																													
<i>alert</i>	Log alert.																													
<i>clock</i>	Clock daemon.																													
<i>local0</i>	Reserved for local use.																													
<i>local1</i>	Reserved for local use.																													
<i>local2</i>	Reserved for local use.																													
<i>local3</i>	Reserved for local use.																													
<i>local4</i>	Reserved for local use.																													
<i>local5</i>	Reserved for local use.																													
<i>local6</i>	Reserved for local use.																													
<i>local7</i>	Reserved for local use.																													
format	Log format.	option	-	default																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Syslog format.</td> </tr> <tr> <td><i>csv</i></td> <td>CSV (Comma Separated Values) format.</td> </tr> <tr> <td><i>cef</i></td> <td>CEF (Common Event Format) format.</td> </tr> <tr> <td><i>rfc5424</i></td> <td>Syslog RFC5424 format.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.																			
Option	Description																													
<i>default</i>	Syslog format.																													
<i>csv</i>	CSV (Comma Separated Values) format.																													
<i>cef</i>	CEF (Common Event Format) format.																													
<i>rfc5424</i>	Syslog RFC5424 format.																													
interface	Specify outgoing interface to reach server.	string	Maximum length: 15																											
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.																					
Option	Description																													
<i>auto</i>	Set outgoing interface automatically.																													
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.																													
<i>specify</i>	Set outgoing interface manually.																													

Parameter	Description	Type	Size	Default												
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0												
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>udp</i></td> <td>Enable syslogging over UDP.</td> </tr> <tr> <td><i>reliable</i></td> <td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td> </tr> </tbody> </table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).									
Option	Description															
<i>udp</i>	Enable syslogging over UDP.															
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).															
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514												
priority	Set log transmission priority.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set Syslog transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set Syslog transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.									
Option	Description															
<i>default</i>	Set Syslog transmission priority to default.															
<i>low</i>	Set Syslog transmission priority to low.															
server	Address of remote syslog server.	string	Maximum length: 127													
source-ip	Source IP address of syslog.	string	Maximum length: 63													
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
status	Enable/disable remote syslog logging.	option	-	disable												

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Log to remote syslog server.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not log to remote syslog server.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.			
Option	Description									
<i>enable</i>	Log to remote syslog server.									
<i>disable</i>	Do not log to remote syslog server.									

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name.	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	

config log syslogd4 filter

Filters for remote system server.

Syntax

```

config log syslogd4 filter
  set forward-traffic [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
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
end

```

Parameters

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

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
severity	Lowest severity level to log.	option	-	information																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					

config free-style

Parameter	Description	Type	Size	Default				
category	Log category.	option	-	traffic				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>traffic</i></td> <td>Traffic log.</td> </tr> </tbody> </table>	Option	Description	<i>traffic</i>	Traffic log.			
Option	Description							
<i>traffic</i>	Traffic log.							

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>event</i></td> <td>Event log.</td> </tr> <tr> <td><i>virus</i></td> <td>Antivirus log.</td> </tr> <tr> <td><i>webfilter</i></td> <td>Web filter log.</td> </tr> <tr> <td><i>attack</i></td> <td>Attack log.</td> </tr> <tr> <td><i>app-ctrl</i></td> <td>Application control log.</td> </tr> <tr> <td><i>ssl</i></td> <td>SSL log.</td> </tr> </tbody> </table>	Option	Description	<i>event</i>	Event log.	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>app-ctrl</i>	Application control log.	<i>ssl</i>	SSL log.			
Option	Description																	
<i>event</i>	Event log.																	
<i>virus</i>	Antivirus log.																	
<i>webfilter</i>	Web filter log.																	
<i>attack</i>	Attack log.																	
<i>app-ctrl</i>	Application control log.																	
<i>ssl</i>	SSL log.																	
filter	Free style filter string.	string	Maximum length: 1023															
filter-type	Include/exclude logs that match the filter.	option	-	include														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.											
Option	Description																	
<i>include</i>	Include logs that match the filter.																	
<i>exclude</i>	Exclude logs that match the filter.																	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0														

config log syslogd4 setting

Global settings for remote syslog server.

Syntax

```

config log syslogd4 setting
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set custom {string}
      set name {string}
    next
  end
  set enc-algorithm [high-medium|high|...]
  set facility [kernel|user|...]
  set format [default|csv|...]
  set interface {string}
  set interface-select-method [auto|sdwan|...]

```

```

set max-log-rate {integer}
set mode [udp|reliable]
set port {integer}
set priority [default|low]
set server {string}
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
end

```

Parameters

Parameter	Description	Type	Size	Default																										
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35																											
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>SSL communication with high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>SSL communication with high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>SSL communication with low encryption algorithms.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL communication.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.																			
Option	Description																													
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.																													
<i>high</i>	SSL communication with high encryption algorithms.																													
<i>low</i>	SSL communication with low encryption algorithms.																													
<i>disable</i>	Disable SSL communication.																													
facility	Remote syslog facility.	option	-	local7																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>kernel</i></td> <td>Kernel messages.</td> </tr> <tr> <td><i>user</i></td> <td>Random user-level messages.</td> </tr> <tr> <td><i>mail</i></td> <td>Mail system.</td> </tr> <tr> <td><i>daemon</i></td> <td>System daemons.</td> </tr> <tr> <td><i>auth</i></td> <td>Security/authorization messages.</td> </tr> <tr> <td><i>syslog</i></td> <td>Messages generated internally by syslog.</td> </tr> <tr> <td><i>lpr</i></td> <td>Line printer subsystem.</td> </tr> <tr> <td><i>news</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>uucp</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>cron</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>authpriv</i></td> <td>Security/authorization messages (private).</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP daemon.</td> </tr> </tbody> </table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.			
Option	Description																													
<i>kernel</i>	Kernel messages.																													
<i>user</i>	Random user-level messages.																													
<i>mail</i>	Mail system.																													
<i>daemon</i>	System daemons.																													
<i>auth</i>	Security/authorization messages.																													
<i>syslog</i>	Messages generated internally by syslog.																													
<i>lpr</i>	Line printer subsystem.																													
<i>news</i>	Network news subsystem.																													
<i>uucp</i>	Network news subsystem.																													
<i>cron</i>	Clock daemon.																													
<i>authpriv</i>	Security/authorization messages (private).																													
<i>ftp</i>	FTP daemon.																													

Parameter	Description	Type	Size	Default																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ntp</i></td> <td>NTP daemon.</td> </tr> <tr> <td><i>audit</i></td> <td>Log audit.</td> </tr> <tr> <td><i>alert</i></td> <td>Log alert.</td> </tr> <tr> <td><i>clock</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>local0</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local1</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local2</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local3</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local4</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local5</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local6</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local7</i></td> <td>Reserved for local use.</td> </tr> </tbody> </table>	Option	Description	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
Option	Description																													
<i>ntp</i>	NTP daemon.																													
<i>audit</i>	Log audit.																													
<i>alert</i>	Log alert.																													
<i>clock</i>	Clock daemon.																													
<i>local0</i>	Reserved for local use.																													
<i>local1</i>	Reserved for local use.																													
<i>local2</i>	Reserved for local use.																													
<i>local3</i>	Reserved for local use.																													
<i>local4</i>	Reserved for local use.																													
<i>local5</i>	Reserved for local use.																													
<i>local6</i>	Reserved for local use.																													
<i>local7</i>	Reserved for local use.																													
format	Log format.	option	-	default																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Syslog format.</td> </tr> <tr> <td><i>csv</i></td> <td>CSV (Comma Separated Values) format.</td> </tr> <tr> <td><i>cef</i></td> <td>CEF (Common Event Format) format.</td> </tr> <tr> <td><i>rfc5424</i></td> <td>Syslog RFC5424 format.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.																			
Option	Description																													
<i>default</i>	Syslog format.																													
<i>csv</i>	CSV (Comma Separated Values) format.																													
<i>cef</i>	CEF (Common Event Format) format.																													
<i>rfc5424</i>	Syslog RFC5424 format.																													
interface	Specify outgoing interface to reach server.	string	Maximum length: 15																											
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.																					
Option	Description																													
<i>auto</i>	Set outgoing interface automatically.																													
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.																													
<i>specify</i>	Set outgoing interface manually.																													

Parameter	Description	Type	Size	Default												
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0												
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>udp</i></td> <td>Enable syslogging over UDP.</td> </tr> <tr> <td><i>reliable</i></td> <td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td> </tr> </tbody> </table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).									
Option	Description															
<i>udp</i>	Enable syslogging over UDP.															
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).															
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514												
priority	Set log transmission priority.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set Syslog transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set Syslog transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.									
Option	Description															
<i>default</i>	Set Syslog transmission priority to default.															
<i>low</i>	Set Syslog transmission priority to low.															
server	Address of remote syslog server.	string	Maximum length: 127													
source-ip	Source IP address of syslog.	string	Maximum length: 63													
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
status	Enable/disable remote syslog logging.	option	-	disable												

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Log to remote syslog server.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not log to remote syslog server.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.			
Option	Description									
<i>enable</i>	Log to remote syslog server.									
<i>disable</i>	Do not log to remote syslog server.									

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name.	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	

config log syslogd filter

Filters for remote system server.

Syntax

```

config log syslogd filter
  set forward-traffic [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
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
end

```

Parameters

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

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
severity	Lowest severity level to log.	option	-	information																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					

config free-style

Parameter	Description	Type	Size	Default				
category	Log category.	option	-	traffic				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>traffic</i></td> <td>Traffic log.</td> </tr> </tbody> </table>	Option	Description	<i>traffic</i>	Traffic log.			
Option	Description							
<i>traffic</i>	Traffic log.							

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>event</i></td> <td>Event log.</td> </tr> <tr> <td><i>virus</i></td> <td>Antivirus log.</td> </tr> <tr> <td><i>webfilter</i></td> <td>Web filter log.</td> </tr> <tr> <td><i>attack</i></td> <td>Attack log.</td> </tr> <tr> <td><i>app-ctrl</i></td> <td>Application control log.</td> </tr> <tr> <td><i>ssl</i></td> <td>SSL log.</td> </tr> </tbody> </table>	Option	Description	<i>event</i>	Event log.	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>app-ctrl</i>	Application control log.	<i>ssl</i>	SSL log.			
Option	Description																	
<i>event</i>	Event log.																	
<i>virus</i>	Antivirus log.																	
<i>webfilter</i>	Web filter log.																	
<i>attack</i>	Attack log.																	
<i>app-ctrl</i>	Application control log.																	
<i>ssl</i>	SSL log.																	
filter	Free style filter string.	string	Maximum length: 1023															
filter-type	Include/exclude logs that match the filter.	option	-	include														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.											
Option	Description																	
<i>include</i>	Include logs that match the filter.																	
<i>exclude</i>	Exclude logs that match the filter.																	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0														

config log syslogd setting

Global settings for remote syslog server.

Syntax

```

config log syslogd setting
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set custom {string}
      set name {string}
    next
  end
  set enc-algorithm [high-medium|high|...]
  set facility [kernel|user|...]
  set format [default|csv|...]
  set interface {string}
  set interface-select-method [auto|sdwan|...]

```

```

set max-log-rate {integer}
set mode [udp|reliable]
set port {integer}
set priority [default|low]
set server {string}
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
end

```

Parameters

Parameter	Description	Type	Size	Default																										
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35																											
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>SSL communication with high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>SSL communication with high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>SSL communication with low encryption algorithms.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL communication.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.																			
Option	Description																													
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.																													
<i>high</i>	SSL communication with high encryption algorithms.																													
<i>low</i>	SSL communication with low encryption algorithms.																													
<i>disable</i>	Disable SSL communication.																													
facility	Remote syslog facility.	option	-	local7																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>kernel</i></td> <td>Kernel messages.</td> </tr> <tr> <td><i>user</i></td> <td>Random user-level messages.</td> </tr> <tr> <td><i>mail</i></td> <td>Mail system.</td> </tr> <tr> <td><i>daemon</i></td> <td>System daemons.</td> </tr> <tr> <td><i>auth</i></td> <td>Security/authorization messages.</td> </tr> <tr> <td><i>syslog</i></td> <td>Messages generated internally by syslog.</td> </tr> <tr> <td><i>lpr</i></td> <td>Line printer subsystem.</td> </tr> <tr> <td><i>news</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>uucp</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>cron</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>authpriv</i></td> <td>Security/authorization messages (private).</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP daemon.</td> </tr> </tbody> </table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.			
Option	Description																													
<i>kernel</i>	Kernel messages.																													
<i>user</i>	Random user-level messages.																													
<i>mail</i>	Mail system.																													
<i>daemon</i>	System daemons.																													
<i>auth</i>	Security/authorization messages.																													
<i>syslog</i>	Messages generated internally by syslog.																													
<i>lpr</i>	Line printer subsystem.																													
<i>news</i>	Network news subsystem.																													
<i>uucp</i>	Network news subsystem.																													
<i>cron</i>	Clock daemon.																													
<i>authpriv</i>	Security/authorization messages (private).																													
<i>ftp</i>	FTP daemon.																													

Parameter	Description	Type	Size	Default																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ntp</i></td> <td>NTP daemon.</td> </tr> <tr> <td><i>audit</i></td> <td>Log audit.</td> </tr> <tr> <td><i>alert</i></td> <td>Log alert.</td> </tr> <tr> <td><i>clock</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>local0</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local1</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local2</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local3</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local4</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local5</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local6</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local7</i></td> <td>Reserved for local use.</td> </tr> </tbody> </table>	Option	Description	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
Option	Description																													
<i>ntp</i>	NTP daemon.																													
<i>audit</i>	Log audit.																													
<i>alert</i>	Log alert.																													
<i>clock</i>	Clock daemon.																													
<i>local0</i>	Reserved for local use.																													
<i>local1</i>	Reserved for local use.																													
<i>local2</i>	Reserved for local use.																													
<i>local3</i>	Reserved for local use.																													
<i>local4</i>	Reserved for local use.																													
<i>local5</i>	Reserved for local use.																													
<i>local6</i>	Reserved for local use.																													
<i>local7</i>	Reserved for local use.																													
format	Log format.	option	-	default																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Syslog format.</td> </tr> <tr> <td><i>csv</i></td> <td>CSV (Comma Separated Values) format.</td> </tr> <tr> <td><i>cef</i></td> <td>CEF (Common Event Format) format.</td> </tr> <tr> <td><i>rfc5424</i></td> <td>Syslog RFC5424 format.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.																			
Option	Description																													
<i>default</i>	Syslog format.																													
<i>csv</i>	CSV (Comma Separated Values) format.																													
<i>cef</i>	CEF (Common Event Format) format.																													
<i>rfc5424</i>	Syslog RFC5424 format.																													
interface	Specify outgoing interface to reach server.	string	Maximum length: 15																											
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.																					
Option	Description																													
<i>auto</i>	Set outgoing interface automatically.																													
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.																													
<i>specify</i>	Set outgoing interface manually.																													

Parameter	Description	Type	Size	Default												
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0												
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>udp</i></td> <td>Enable syslogging over UDP.</td> </tr> <tr> <td><i>reliable</i></td> <td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td> </tr> </tbody> </table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).									
Option	Description															
<i>udp</i>	Enable syslogging over UDP.															
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).															
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514												
priority	Set log transmission priority.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set Syslog transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set Syslog transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.									
Option	Description															
<i>default</i>	Set Syslog transmission priority to default.															
<i>low</i>	Set Syslog transmission priority to low.															
server	Address of remote syslog server.	string	Maximum length: 127													
source-ip	Source IP address of syslog.	string	Maximum length: 63													
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
status	Enable/disable remote syslog logging.	option	-	disable												

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Log to remote syslog server.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not log to remote syslog server.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.			
Option	Description									
<i>enable</i>	Log to remote syslog server.									
<i>disable</i>	Do not log to remote syslog server.									

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name.	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	

report

This section includes syntax for the following commands:

- [config report setting on page 157](#)

config report setting

Report setting configuration.

Syntax

```
config report setting
  set report-source {option1}, {option2}, ...
end
```

Parameters

Parameter	Description	Type	Size	Default								
report-source	Report log source.	option	-	forward-traffic								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>forward-traffic</i></td><td>Report includes forward traffic logs.</td></tr><tr><td><i>sniffer-traffic</i></td><td>Report includes sniffer traffic logs.</td></tr><tr><td><i>local-deny-traffic</i></td><td>Report includes local deny traffic logs.</td></tr></tbody></table>	Option	Description	<i>forward-traffic</i>	Report includes forward traffic logs.	<i>sniffer-traffic</i>	Report includes sniffer traffic logs.	<i>local-deny-traffic</i>	Report includes local deny traffic logs.			
Option	Description											
<i>forward-traffic</i>	Report includes forward traffic logs.											
<i>sniffer-traffic</i>	Report includes sniffer traffic logs.											
<i>local-deny-traffic</i>	Report includes local deny traffic logs.											

router

This section includes syntax for the following commands:

- [config router static on page 158](#)

config router static

Configure IPv4 static routing tables.

Syntax

```
config router static
  edit <seq-num>
    set comment {var-string}
    set device {string}
    set distance {integer}
    set dst {ipv4-classnet}
    set dstaddr {string}
    set gateway {ipv4-address}
    set priority {integer}
    set src {ipv4-address}
    set status [enable|disable]
    set weight {integer}
  next
end
```

Parameters

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
device	Gateway out interface or tunnel.	string	Maximum length: 35	
distance	Administrative distance.	integer	Minimum value: 1 Maximum value: 255	10
dst	Destination IP and mask for this route.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
dstaddr	Name of firewall address or address group.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
gateway	Gateway IP for this route.	ipv4-address	Not Specified	0.0.0.0						
priority	Administrative priority.	integer	Minimum value: 1 Maximum value: 65535	1						
seq-num	Sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	0						
src	Source address for this route.	ipv4-address	Not Specified	0.0.0.0						
status	Enable/disable this static route.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable static route.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable static route.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable static route.	<i>disable</i>	Disable static route.			
Option	Description									
<i>enable</i>	Enable static route.									
<i>disable</i>	Disable static route.									
weight	Administrative weight.	integer	Minimum value: 0 Maximum value: 255	0						

system

This section includes syntax for the following commands:

- [config system admin on page 160](#)
- [config system api-user on page 161](#)
- [config system autoupdate schedule on page 161](#)
- [config system dns on page 162](#)
- [config system external-resource on page 163](#)
- [config system fortiguard on page 165](#)
- [config system global on page 167](#)
- [config system interface on page 168](#)
- [config system ips on page 168](#)
- [config system replacemsg-group on page 169](#)
- [config system replacemsg-image on page 172](#)
- [config system replacemsg fortiguard-wf on page 173](#)
- [config system replacemsg http on page 174](#)
- [config system replacemsg utm on page 175](#)
- [config system settings on page 176](#)

config system admin

Configure admin users.

Syntax

```
config system admin
  edit <name>
    set passwd {password}
  next
end
```

Parameters

Parameter	Description	Type	Size	Default
name	Admin user name.	string	Maximum length: 15	
passwd	Admin user password.	password	Not Specified	

config system api-user

Configure API users.

Syntax

```
config system api-user
  edit <name>
  next
end
```

config system api-user

Parameter	Description	Type	Size	Default
name	API user name.	string	Maximum length: 15	

config system autoupdate schedule

Configure update schedule.

Syntax

```
config system autoupdate schedule
  set day [Sunday|Monday|...]
  set frequency [every|daily|...]
  set status [enable|disable]
  set time {user}
end
```

Parameters

Parameter	Description	Type	Size	Default												
day	Update day.	option	-	Monday												
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>Sunday</i></td><td>Update every Sunday.</td></tr><tr><td><i>Monday</i></td><td>Update every Monday.</td></tr><tr><td><i>Tuesday</i></td><td>Update every Tuesday.</td></tr><tr><td><i>Wednesday</i></td><td>Update every Wednesday.</td></tr><tr><td><i>Thursday</i></td><td>Update every Thursday.</td></tr></tbody></table>	Option	Description	<i>Sunday</i>	Update every Sunday.	<i>Monday</i>	Update every Monday.	<i>Tuesday</i>	Update every Tuesday.	<i>Wednesday</i>	Update every Wednesday.	<i>Thursday</i>	Update every Thursday.			
Option	Description															
<i>Sunday</i>	Update every Sunday.															
<i>Monday</i>	Update every Monday.															
<i>Tuesday</i>	Update every Tuesday.															
<i>Wednesday</i>	Update every Wednesday.															
<i>Thursday</i>	Update every Thursday.															

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>Friday</i></td> <td>Update every Friday.</td> </tr> <tr> <td><i>Saturday</i></td> <td>Update every Saturday.</td> </tr> </tbody> </table>	Option	Description	<i>Friday</i>	Update every Friday.	<i>Saturday</i>	Update every Saturday.							
Option	Description													
<i>Friday</i>	Update every Friday.													
<i>Saturday</i>	Update every Saturday.													
frequency	Update frequency.	option	-	automatic										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>every</i></td> <td>Time interval.</td> </tr> <tr> <td><i>daily</i></td> <td>Every day.</td> </tr> <tr> <td><i>weekly</i></td> <td>Every week.</td> </tr> <tr> <td><i>automatic</i></td> <td>Update automatically within every one hour period.</td> </tr> </tbody> </table>	Option	Description	<i>every</i>	Time interval.	<i>daily</i>	Every day.	<i>weekly</i>	Every week.	<i>automatic</i>	Update automatically within every one hour period.			
Option	Description													
<i>every</i>	Time interval.													
<i>daily</i>	Every day.													
<i>weekly</i>	Every week.													
<i>automatic</i>	Update automatically within every one hour period.													
status	Enable/disable scheduled updates.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
time	Update time.	user	Not Specified											

config system dns

Configure DNS.

Syntax

```
config system dns
  set dns-cache-ttl {integer}
  set fqdn-cache-ttl {integer}
end
```

Parameters

Parameter	Description	Type	Size	Default
dns-cache-ttl	Duration in seconds that the DNS cache retains information.	integer	Minimum value: 60 Maximum value: 86400	1800

Parameter	Description	Type	Size	Default
fqdn-cache-ttl	FQDN cache time to live in seconds.	integer	Minimum value: 0 Maximum value: 86400	0

config system external-resource

Configure external resource.

Syntax

```

config system external-resource
  edit <name>
    set category {integer}
    set comments {var-string}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set password {password}
    set refresh-rate {integer}
    set resource {string}
    set source-ip {ipv4-address}
    set status [enable|disable]
    set type [category|address|...]
    set user-agent {string}
    set username {string}
    set uuid {uuid}
  next
end

```

config system external-resource

Parameter	Description	Type	Size	Default
category	User resource category 192 - 221.	integer	Minimum value: 192 Maximum value: 221	0
comments	Comment.	var-string	Maximum length: 255	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default										
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.					
Option	Description													
<i>auto</i>	Set outgoing interface automatically.													
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.													
<i>specify</i>	Set outgoing interface manually.													
name	External resource name.	string	Maximum length: 35											
password	HTTP basic authentication password.	password	Not Specified											
refresh-rate	Time interval to refresh external resource.	integer	Minimum value: 1 Maximum value: 43200	5										
resource	URI of external resource.	string	Maximum length: 511											
source-ip	Source IPv4 address used to communicate with server.	ipv4-address	Not Specified	0.0.0.0										
status	Enable/disable user resource.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable user resource.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable user resource.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable user resource.	<i>disable</i>	Disable user resource.							
Option	Description													
<i>enable</i>	Enable user resource.													
<i>disable</i>	Disable user resource.													
type	User resource type.	option	-	category										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>category</i></td> <td>FortiGuard category.</td> </tr> <tr> <td><i>address</i></td> <td>Firewall IP address.</td> </tr> <tr> <td><i>domain</i></td> <td>Domain Name.</td> </tr> <tr> <td><i>malware</i></td> <td>Malware hash.</td> </tr> </tbody> </table>	Option	Description	<i>category</i>	FortiGuard category.	<i>address</i>	Firewall IP address.	<i>domain</i>	Domain Name.	<i>malware</i>	Malware hash.			
Option	Description													
<i>category</i>	FortiGuard category.													
<i>address</i>	Firewall IP address.													
<i>domain</i>	Domain Name.													
<i>malware</i>	Malware hash.													
user-agent	HTTP User-Agent header.	string	Maximum length: 127	curl/7.58.0										
username	HTTP basic authentication user name.	string	Maximum length: 64											

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 system fortiguard

Configure FortiGuard services.

Syntax

```

config system fortiguard
  set fortiguard-anycast [enable|disable]
  set fortiguard-anycast-source [fortinet|aws|...]
  set interface {string}
  set update-extdb [enable|disable]
  set update-ffdb [enable|disable]
  set webfilter-cache [enable|disable]
  set webfilter-cache-ttl {integer}
  set webfilter-expiration {string}
  set webfilter-force-off [enable|disable]
  set webfilter-license {string}
  set webfilter-timeout {integer}
end

```

Parameters

Parameter	Description	Type	Size	Default						
fortiguard-anycast	Enable/disable use of FortiGuard's Anycast network.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of FortiGuard's Anycast network.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of FortiGuard's Anycast network.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of FortiGuard's Anycast network.	<i>disable</i>	Disable use of FortiGuard's Anycast network.			
Option	Description									
<i>enable</i>	Enable use of FortiGuard's Anycast network.									
<i>disable</i>	Disable use of FortiGuard's Anycast network.									
fortiguard-anycast-source	Configure which of Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network. Default is Fortinet.	option	-	fortinet						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortinet</i></td> <td>Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network.</td> </tr> </tbody> </table>	Option	Description	<i>fortinet</i>	Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network.					
Option	Description									
<i>fortinet</i>	Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network.									

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>aws</i></td> <td>Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network.</td> </tr> <tr> <td><i>debug</i></td> <td>Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.</td> </tr> </tbody> </table>	Option	Description	<i>aws</i>	Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network.	<i>debug</i>	Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.			
Option	Description									
<i>aws</i>	Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network.									
<i>debug</i>	Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	any						
update-extdb	Enable/disable external resource update.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable external resource update.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable external resource update.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable external resource update.	<i>disable</i>	Disable external resource update.			
Option	Description									
<i>enable</i>	Enable external resource update.									
<i>disable</i>	Disable external resource update.									
update-ffdb	Enable/disable Internet Service Database update.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Internet Service Database update.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Internet Service Database update.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Internet Service Database update.	<i>disable</i>	Disable Internet Service Database update.			
Option	Description									
<i>enable</i>	Enable Internet Service Database update.									
<i>disable</i>	Disable Internet Service Database update.									
webfilter-cache	Enable/disable FortiGuard web filter caching.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiGuard web filter caching.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiGuard web filter caching.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiGuard web filter caching.	<i>disable</i>	Disable FortiGuard web filter caching.			
Option	Description									
<i>enable</i>	Enable FortiGuard web filter caching.									
<i>disable</i>	Disable FortiGuard web filter caching.									
webfilter-cache-ttl	Time-to-live for web filter cache entries in seconds.	integer	Minimum value: 300 Maximum value: 86400	3600						
webfilter-expiration	Expiration date of the FortiGuard web filter contract. Read-only.	string	Maximum length: -							
webfilter-force-off	Enable/disable turning off the FortiGuard web filtering service.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Turn off the FortiGuard web filtering service.</td> </tr> <tr> <td><i>disable</i></td> <td>Allow the FortiGuard web filtering service to operate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Turn off the FortiGuard web filtering service.	<i>disable</i>	Allow the FortiGuard web filtering service to operate.			
Option	Description									
<i>enable</i>	Turn off the FortiGuard web filtering service.									
<i>disable</i>	Allow the FortiGuard web filtering service to operate.									

Parameter	Description	Type	Size	Default
webfilter-license	Web filter license status. Read-only.	string	Maximum length: -	
webfilter-timeout	Web filter query time out.	integer	Minimum value: 1 Maximum value: 30	15

config system global

Configure global attributes.

Syntax

```
config system global
  set admin-port {integer}
  set admin-server-cert {string}
  set admin-sport {integer}
  set cert-chain-max {integer}
  set remoteauthtimeout {integer}
end
```

Parameters

Parameter	Description	Type	Size	Default
admin-port	REST API access port for HTTP. 0 disables HTTP.	integer	Minimum value: 0 Maximum value: 65535	0
admin-server-cert	Server certificate that Container FortiOS uses for HTTPS administrative connections.	string	Maximum length: -	Fortinet_GUI_Server
admin-sport	REST API access port for HTTPS. 0 disables HTTPS.	integer	Minimum value: 0 Maximum value: 65535	443
cert-chain-max	Maximum number of certificates that can be traversed in a certificate chain.	integer	Minimum value: 1 Maximum value: 2147483647	8
remoteauthtimeout	Number of seconds that Container FortiOS waits for responses from remote authentication servers.	integer	Minimum value: 1 Maximum value: 300	5

config system interface

Configure interfaces.

Syntax

```
config system interface
  edit <name>
    set ip {ipv4-classnet-host}
  next
end
```

Parameters

Parameter	Description	Type	Size	Default
ip	Interface IPv4 address and subnet mask, syntax: X.X.X.X/24.	ipv4-classnet-host	Not Specified	0.0.0.0
name	Name.	string	Maximum length: 15	

config system ips

Configure IPS system settings.

Syntax

```
config system ips
  set override-signature-hold-by-id [enable|disable]
  set signature-hold-time {user}
end
```

Parameters

Parameter	Description	Type	Size	Default						
override-signature-hold-by-id	Enable/disable override of hold of triggering signatures that are specified by IDs regardless of hold.	option	-	enable						
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Allow the signatures specified by IDs to be triggered even if they are on hold.</td></tr><tr><td><i>disable</i></td><td>Do not trigger the signatures that are on hold.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Allow the signatures specified by IDs to be triggered even if they are on hold.	<i>disable</i>	Do not trigger the signatures that are on hold.			
Option	Description									
<i>enable</i>	Allow the signatures specified by IDs to be triggered even if they are on hold.									
<i>disable</i>	Do not trigger the signatures that are on hold.									

Parameter	Description	Type	Size	Default
signature-hold-time	Time to hold and monitor IPS signatures. Format <#d##h>.	user	Not Specified	0h

config system replacemsg-group

Configure replacement message groups.

Syntax

```

config system replacemsg-group
  edit <name>
    set comment {var-string}
    config custom-message
      Description: Replacement message table entries.
      edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
      next
    end
    config fortiguard-wf
      Description: Replacement message table entries.
      edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
      next
    end
    set group-type {option}
    config http
      Description: Replacement message table entries.
      edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
      next
    end
    config utm
      Description: Replacement message table entries.
      edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
      next
    end
  next
end

```

config system replacemsg-group

Parameter	Description	Type	Size	Default				
comment	Comment.	var-string	Maximum length: 255					
group-type	Group type.	option	-	utm				
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>utm</i></td><td>For use with UTM settings in firewall policies.</td></tr></tbody></table>	Option	Description	<i>utm</i>	For use with UTM settings in firewall policies.			
Option	Description							
<i>utm</i>	For use with UTM settings in firewall policies.							
name	Group name.	string	Maximum length: 35					

config custom-message

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
format	Format flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											
header	Header flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
msg-type	Message type.	string	Maximum length: 28									

config fortiguard-wf

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
format	Format flag.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											
header	Header flag.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
msg-type	Message type.	string	Maximum length: 28									

config http

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
format	Format flag.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											
header	Header flag.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP					
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											

Parameter	Description	Type	Size	Default				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>8bit</i>	8 bit.			
Option	Description							
<i>8bit</i>	8 bit.							
msg-type	Message type.	string	Maximum length: 28					

config utm

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
format	Format flag.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											
header	Header flag.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
msg-type	Message type.	string	Maximum length: 28									

config system replacemsg-image

Configure replacement message images.

Syntax

```

config system replacemsg-image
  edit <name>
    set image-base64 {var-string}
    set image-type [gif|jpg|...]
  next
end

```

config system replacemsg-image

Parameter	Description	Type	Size	Default										
image-base64	Image data.	var-string	Maximum length: 32768											
image-type	Image type.	option	-	png										
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>gif</i></td><td>GIF image.</td></tr><tr><td><i>jpg</i></td><td>JPEG image.</td></tr><tr><td><i>tiff</i></td><td>TIFF image.</td></tr><tr><td><i>png</i></td><td>PNG image.</td></tr></tbody></table>	Option	Description	<i>gif</i>	GIF image.	<i>jpg</i>	JPEG image.	<i>tiff</i>	TIFF image.	<i>png</i>	PNG image.			
Option	Description													
<i>gif</i>	GIF image.													
<i>jpg</i>	JPEG image.													
<i>tiff</i>	TIFF image.													
<i>png</i>	PNG image.													
name	Image name.	string	Maximum length: 23											

config system replacemsg fortiguard-wf

Replacement messages.

Syntax

```
config system replacemsg fortiguard-wf
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg fortiguard-wf

Parameter	Description	Type	Size	Default				
buffer	Message string.	var-string	Maximum length: 32768					
format	Format flag.	option	-					
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.			
Option	Description							
<i>none</i>	No format type.							

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>text</i>	Text format.	<i>html</i>	HTML format.					
Option	Description											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											
header	Header flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
msg-type	Message type.	string	Maximum length: 28									

config system replacemsg http

Replacement messages.

Syntax

```
config system replacemsg http
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

Parameters

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
format	Format flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

Parameter	Description	Type	Size	Default								
header	Header flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
msg-type	Message type.	string	Maximum length: 28									

config system replacemsg utm

Replacement messages.

Syntax

```
config system replacemsg utm
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

Parameters

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
format	Format flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											
header	Header flag.	option	-									

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
msg-type	Message type.	string	Maximum length: 28									

config system settings

Configure settings.

Syntax

```
config system settings
  set central-nat [enable|disable]
  set ngfw-mode [profile-based|policy-based]
  set tcp-session-without-syn [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default						
central-nat	Enable/disable central NAT.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable central NAT.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable central NAT.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable central NAT.	<i>disable</i>	Disable central NAT.			
Option	Description									
<i>enable</i>	Enable central NAT.									
<i>disable</i>	Disable central NAT.									
ngfw-mode	Next Generation Firewall (NGFW) mode.	option	-	profile-based						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>profile-based</i></td> <td>Application and web-filtering are configured using profiles applied to policy entries.</td> </tr> <tr> <td><i>policy-based</i></td> <td>Application and web-filtering are configured as policy match conditions.</td> </tr> </tbody> </table>	Option	Description	<i>profile-based</i>	Application and web-filtering are configured using profiles applied to policy entries.	<i>policy-based</i>	Application and web-filtering are configured as policy match conditions.			
Option	Description									
<i>profile-based</i>	Application and web-filtering are configured using profiles applied to policy entries.									
<i>policy-based</i>	Application and web-filtering are configured as policy match conditions.									
tcp-session-without-syn	Enable/disable allowing TCP session without SYN flags.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Allow TCP session without SYN flags.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not allow TCP session without SYN flags.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Allow TCP session without SYN flags.	<i>disable</i>	Do not allow TCP session without SYN flags.			
Option	Description									
<i>enable</i>	Allow TCP session without SYN flags.									
<i>disable</i>	Do not allow TCP session without SYN flags.									

user

This section includes syntax for the following commands:

- [config user peer on page 178](#)
- [config user peergrp on page 179](#)

config user peer

Configure peer users.

Syntax

```
config user peer
  edit <name>
    set ca {string}
    set cn {string}
    set email {string}
    set fqdn {string}
    set ip {string}
    set mandatory-ca-verify [enable|disable]
    set subject {string}
  next
end
```

Parameters

Parameter	Description	Type	Size	Default
ca	Name of the CA certificate.	string	Maximum length: 127	
cn	Peer certificate common name.	string	Maximum length: 255	
email	Peer certificate email address.	string	Maximum length: 255	
fqdn	Peer certificate FQDN.	string	Maximum length: 255	
ip	Peer certificate ip address.	string	Maximum length: 255	
mandatory-ca-verify	Determine what happens to the peer if the CA certificate is not installed. Disable to automatically consider the peer certificate as valid.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
name	Peer name.	string	Maximum length: 35							
subject	Peer certificate name constraints.	string	Maximum length: 255							

config user peergrp

Configure peer groups.

Syntax

```
config user peergrp
  edit <name>
    set member <name1>, <name2>, ...
  next
end
```

Parameters

Parameter	Description	Type	Size	Default
member <name>	Peer group members. Peer name.	string	Maximum length: 79	
name	Peer group name.	string	Maximum length: 79	

vpn

This section includes syntax for the following commands:

- [config vpn certificate ca on page 180](#)
- [config vpn certificate local on page 181](#)
- [config vpn certificate setting on page 181](#)
- [config vpn ipsec phase1-interface on page 182](#)
- [config vpn ipsec phase2-interface on page 187](#)

config vpn certificate ca

CA certificate.

Syntax

```
config vpn certificate ca
  edit <name>
    set ca {user}
    set source [factory|user|...]
    set ssl-inspection-trusted [enable|disable]
  next
end
```

Parameters

Parameter	Description	Type	Size	Default								
ca	CA certificate as a PEM file.	user	Not Specified									
name	Name.	string	Maximum length: 64									
source	CA certificate source type.	option	-	user								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></tbody></table>	Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.			
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-	enable								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Trusted CA for SSL inspection.</td> </tr> <tr> <td><i>disable</i></td> <td>Untrusted CA for SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Trusted CA for SSL inspection.	<i>disable</i>	Untrusted CA for SSL inspection.			
Option	Description									
<i>enable</i>	Trusted CA for SSL inspection.									
<i>disable</i>	Untrusted CA for SSL inspection.									

config vpn certificate local

Local keys and certificates.

Syntax

```

config vpn certificate local
  edit <name>
    set certificate {user}
    set comments {string}
    set password {password}
    set private-key {user}
  next
end

```

Parameters

Parameter	Description	Type	Size	Default
certificate	PEM format certificate.	user	Not Specified	
comments	Comment.	string	Maximum length: 511	
name	Name.	string	Maximum length: 35	
password	Password as a PEM file.	password	Not Specified	
private-key	PEM format key, encrypted with a password.	user	Not Specified	

config vpn certificate setting

VPN certificate setting.

Syntax

```
config vpn certificate setting
  set ocs-status [enable|disable]
  set strict-ocsp-check [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default						
ocsp-status	Enable/disable receiving certificates using the OCSP.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
strict-ocsp-check	Enable/disable strict mode OCSP checking.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

config vpn ipsec phase1-interface

Configure VPN remote gateway.

Syntax

```
config vpn ipsec phase1-interface
  edit <name>
    set add-route [disable|enable]
    set authmethod [psk|signature]
    set auto-negotiate [enable|disable]
    set certificate <name1>, <name2>, ...
    set dhgrp {option1}, {option2}, ...
    set dpd [disable|on-idle|...]
    set dpd-retrycount {integer}
    set dpd-retryinterval {integer}
    set fragmentation [enable|disable]
    set fragmentation-mtu {integer}
    set interface {string}
    set keepalive {integer}
    set keylife {integer}
    set localid {string}
```

```

set localid-type [auto|fqdn|...]
set mode-cfg [disable|enable]
set peer {string}
set peergrp {string}
set peertype [any|one|...]
set proposal {option1}, {option2}, ...
set psksecret {password-3}
set reauth [disable|enable]
set rekey [enable|disable]
set remote-gw {ipv4-address}
set type [static|dynamic|...]
next
end

```

config vpn ipsec phase1-interface

Parameter	Description	Type	Size	Default						
add-route	Enable/disable control addition of a route to peer destination selector.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not add a route to destination of peer selector.</td> </tr> <tr> <td><i>enable</i></td> <td>Add route to destination of peer selector.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not add a route to destination of peer selector.	<i>enable</i>	Add route to destination of peer selector.			
Option	Description									
<i>disable</i>	Do not add a route to destination of peer selector.									
<i>enable</i>	Add route to destination of peer selector.									
authmethod	Authentication method.	option	-	psk						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>psk</i></td> <td>PSK authentication method.</td> </tr> <tr> <td><i>signature</i></td> <td>Signature authentication method.</td> </tr> </tbody> </table>	Option	Description	<i>psk</i>	PSK authentication method.	<i>signature</i>	Signature authentication method.			
Option	Description									
<i>psk</i>	PSK authentication method.									
<i>signature</i>	Signature authentication method.									
auto-negotiate	Enable/disable automatic initiation of IKE SA negotiation.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic initiation of IKE SA negotiation.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic initiation of IKE SA negotiation.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic initiation of IKE SA negotiation.	<i>disable</i>	Disable automatic initiation of IKE SA negotiation.			
Option	Description									
<i>enable</i>	Enable automatic initiation of IKE SA negotiation.									
<i>disable</i>	Disable automatic initiation of IKE SA negotiation.									
certificate <name>	The names of up to 4 signed personal certificates. Certificate name.	string	Maximum length: 79							
dhgrp	DH group.	option	-	14						

Parameter	Description	Type	Size	Default																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>2</td> <td>DH Group 2.</td> </tr> <tr> <td>5</td> <td>DH Group 5.</td> </tr> <tr> <td>14</td> <td>DH Group 14.</td> </tr> <tr> <td>15</td> <td>DH Group 15.</td> </tr> <tr> <td>16</td> <td>DH Group 16.</td> </tr> <tr> <td>17</td> <td>DH Group 17.</td> </tr> <tr> <td>18</td> <td>DH Group 18.</td> </tr> <tr> <td>19</td> <td>DH Group 19.</td> </tr> <tr> <td>20</td> <td>DH Group 20.</td> </tr> <tr> <td>21</td> <td>DH Group 21.</td> </tr> </tbody> </table>	Option	Description	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.			
Option	Description																									
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.																									
dpd	Dead Peer Detection mode.	option	-	on-demand																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Dead Peer Detection.</td> </tr> <tr> <td><i>on-idle</i></td> <td>Trigger Dead Peer Detection when IPsec is idle.</td> </tr> <tr> <td><i>on-demand</i></td> <td>Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Dead Peer Detection.	<i>on-idle</i>	Trigger Dead Peer Detection when IPsec is idle.	<i>on-demand</i>	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.																	
Option	Description																									
<i>disable</i>	Disable Dead Peer Detection.																									
<i>on-idle</i>	Trigger Dead Peer Detection when IPsec is idle.																									
<i>on-demand</i>	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.																									
dpd-retrycount	Number of DPD retry attempts.	integer	Minimum value: 0 Maximum value: 10	3																						
dpd-retryinterval	DPD retry interval.	integer	Minimum value: 0 Maximum value: 3600	20																						
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-	enable																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable intra-IKE fragmentation support on re-transmission.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable intra-IKE fragmentation support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.	<i>disable</i>	Disable intra-IKE fragmentation support.																			
Option	Description																									
<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.																									
<i>disable</i>	Disable intra-IKE fragmentation support.																									

Parameter	Description	Type	Size	Default														
fragmentation-mtu	IKE fragmentation MTU.	integer	Minimum value: 500 Maximum value: 16000	1200														
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35															
keepalive	NAT-T keep alive interval.	integer	Minimum value: 10 Maximum value: 900	10														
keylife	Time to wait in seconds before phase 1 encryption key expires.	integer	Minimum value: 120 Maximum value: 172800	86400														
localid	Local ID.	string	Maximum length: 63															
localid-type	Local ID type.	option	-	auto														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Select ID type automatically.</td> </tr> <tr> <td><i>fqdn</i></td> <td>Use fully qualified domain name.</td> </tr> <tr> <td><i>user-fqdn</i></td> <td>Use user fully qualified domain name.</td> </tr> <tr> <td><i>keyid</i></td> <td>Use key-id string.</td> </tr> <tr> <td><i>address</i></td> <td>Use local IP address.</td> </tr> <tr> <td><i>asn1dn</i></td> <td>Use ASN.1 distinguished name.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Select ID type automatically.	<i>fqdn</i>	Use fully qualified domain name.	<i>user-fqdn</i>	Use user fully qualified domain name.	<i>keyid</i>	Use key-id string.	<i>address</i>	Use local IP address.	<i>asn1dn</i>	Use ASN.1 distinguished name.			
Option	Description																	
<i>auto</i>	Select ID type automatically.																	
<i>fqdn</i>	Use fully qualified domain name.																	
<i>user-fqdn</i>	Use user fully qualified domain name.																	
<i>keyid</i>	Use key-id string.																	
<i>address</i>	Use local IP address.																	
<i>asn1dn</i>	Use ASN.1 distinguished name.																	
mode-cfg	Enable/disable configuration method.	option	-	disable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Configuration Method.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable Configuration Method.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Configuration Method.	<i>enable</i>	Enable Configuration Method.											
Option	Description																	
<i>disable</i>	Disable Configuration Method.																	
<i>enable</i>	Enable Configuration Method.																	
peer	Accept this peer certificate.	string	Maximum length: 35															
peergrp	Accept this peer certificate group.	string	Maximum length: 35															
peertype	Accept this peer type.	option	-	any														

Parameter	Description	Type	Size	Default																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>any</i></td> <td>Accept any peer ID.</td> </tr> <tr> <td><i>one</i></td> <td>Accept this peer ID.</td> </tr> <tr> <td><i>dialup</i></td> <td>Accept peer ID in dialup group.</td> </tr> <tr> <td><i>peer</i></td> <td>Accept this peer certificate.</td> </tr> <tr> <td><i>peergrp</i></td> <td>Accept this peer certificate group.</td> </tr> </tbody> </table>	Option	Description	<i>any</i>	Accept any peer ID.	<i>one</i>	Accept this peer ID.	<i>dialup</i>	Accept peer ID in dialup group.	<i>peer</i>	Accept this peer certificate.	<i>peergrp</i>	Accept this peer certificate group.																											
Option	Description																																							
<i>any</i>	Accept any peer ID.																																							
<i>one</i>	Accept this peer ID.																																							
<i>dialup</i>	Accept peer ID in dialup group.																																							
<i>peer</i>	Accept this peer certificate.																																							
<i>peergrp</i>	Accept this peer certificate group.																																							
proposal	Phase1 proposal.	option	-	aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384 chacha20poly1305-prfsha256																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>aes128-sha1</i></td> <td>aes128-sha1</td> </tr> <tr> <td><i>aes128-sha256</i></td> <td>aes128-sha256</td> </tr> <tr> <td><i>aes128-sha384</i></td> <td>aes128-sha384</td> </tr> <tr> <td><i>aes128-sha512</i></td> <td>aes128-sha512</td> </tr> <tr> <td><i>aes128gcm-prfsha1</i></td> <td>aes128gcm-prfsha1</td> </tr> <tr> <td><i>aes128gcm-prfsha256</i></td> <td>aes128gcm-prfsha256</td> </tr> <tr> <td><i>aes128gcm-prfsha384</i></td> <td>aes128gcm-prfsha384</td> </tr> <tr> <td><i>aes128gcm-prfsha512</i></td> <td>aes128gcm-prfsha512</td> </tr> <tr> <td><i>aes192-sha1</i></td> <td>aes192-sha1</td> </tr> <tr> <td><i>aes192-sha256</i></td> <td>aes192-sha256</td> </tr> <tr> <td><i>aes192-sha384</i></td> <td>aes192-sha384</td> </tr> <tr> <td><i>aes192-sha512</i></td> <td>aes192-sha512</td> </tr> <tr> <td><i>aes256-sha1</i></td> <td>aes256-sha1</td> </tr> <tr> <td><i>aes256-sha256</i></td> <td>aes256-sha256</td> </tr> <tr> <td><i>aes256-sha384</i></td> <td>aes256-sha384</td> </tr> <tr> <td><i>aes256-sha512</i></td> <td>aes256-sha512</td> </tr> <tr> <td><i>aes256gcm-prfsha1</i></td> <td>aes256gcm-prfsha1</td> </tr> </tbody> </table>	Option	Description	<i>aes128-sha1</i>	aes128-sha1	<i>aes128-sha256</i>	aes128-sha256	<i>aes128-sha384</i>	aes128-sha384	<i>aes128-sha512</i>	aes128-sha512	<i>aes128gcm-prfsha1</i>	aes128gcm-prfsha1	<i>aes128gcm-prfsha256</i>	aes128gcm-prfsha256	<i>aes128gcm-prfsha384</i>	aes128gcm-prfsha384	<i>aes128gcm-prfsha512</i>	aes128gcm-prfsha512	<i>aes192-sha1</i>	aes192-sha1	<i>aes192-sha256</i>	aes192-sha256	<i>aes192-sha384</i>	aes192-sha384	<i>aes192-sha512</i>	aes192-sha512	<i>aes256-sha1</i>	aes256-sha1	<i>aes256-sha256</i>	aes256-sha256	<i>aes256-sha384</i>	aes256-sha384	<i>aes256-sha512</i>	aes256-sha512	<i>aes256gcm-prfsha1</i>	aes256gcm-prfsha1			
Option	Description																																							
<i>aes128-sha1</i>	aes128-sha1																																							
<i>aes128-sha256</i>	aes128-sha256																																							
<i>aes128-sha384</i>	aes128-sha384																																							
<i>aes128-sha512</i>	aes128-sha512																																							
<i>aes128gcm-prfsha1</i>	aes128gcm-prfsha1																																							
<i>aes128gcm-prfsha256</i>	aes128gcm-prfsha256																																							
<i>aes128gcm-prfsha384</i>	aes128gcm-prfsha384																																							
<i>aes128gcm-prfsha512</i>	aes128gcm-prfsha512																																							
<i>aes192-sha1</i>	aes192-sha1																																							
<i>aes192-sha256</i>	aes192-sha256																																							
<i>aes192-sha384</i>	aes192-sha384																																							
<i>aes192-sha512</i>	aes192-sha512																																							
<i>aes256-sha1</i>	aes256-sha1																																							
<i>aes256-sha256</i>	aes256-sha256																																							
<i>aes256-sha384</i>	aes256-sha384																																							
<i>aes256-sha512</i>	aes256-sha512																																							
<i>aes256gcm-prfsha1</i>	aes256gcm-prfsha1																																							

Parameter	Description	Type	Size	Default																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>aes256gcm-prfsha256</i></td> <td>aes256gcm-prfsha256</td> </tr> <tr> <td><i>aes256gcm-prfsha384</i></td> <td>aes256gcm-prfsha384</td> </tr> <tr> <td><i>aes256gcm-prfsha512</i></td> <td>aes256gcm-prfsha512</td> </tr> <tr> <td><i>chacha20poly1305-prfsha1</i></td> <td>chacha20poly1305-prfsha1</td> </tr> <tr> <td><i>chacha20poly1305-prfsha256</i></td> <td>chacha20poly1305-prfsha256</td> </tr> <tr> <td><i>chacha20poly1305-prfsha384</i></td> <td>chacha20poly1305-prfsha384</td> </tr> <tr> <td><i>chacha20poly1305-prfsha512</i></td> <td>chacha20poly1305-prfsha512</td> </tr> </tbody> </table>	Option	Description	<i>aes256gcm-prfsha256</i>	aes256gcm-prfsha256	<i>aes256gcm-prfsha384</i>	aes256gcm-prfsha384	<i>aes256gcm-prfsha512</i>	aes256gcm-prfsha512	<i>chacha20poly1305-prfsha1</i>	chacha20poly1305-prfsha1	<i>chacha20poly1305-prfsha256</i>	chacha20poly1305-prfsha256	<i>chacha20poly1305-prfsha384</i>	chacha20poly1305-prfsha384	<i>chacha20poly1305-prfsha512</i>	chacha20poly1305-prfsha512			
Option	Description																			
<i>aes256gcm-prfsha256</i>	aes256gcm-prfsha256																			
<i>aes256gcm-prfsha384</i>	aes256gcm-prfsha384																			
<i>aes256gcm-prfsha512</i>	aes256gcm-prfsha512																			
<i>chacha20poly1305-prfsha1</i>	chacha20poly1305-prfsha1																			
<i>chacha20poly1305-prfsha256</i>	chacha20poly1305-prfsha256																			
<i>chacha20poly1305-prfsha384</i>	chacha20poly1305-prfsha384																			
<i>chacha20poly1305-prfsha512</i>	chacha20poly1305-prfsha512																			
psksecret	Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified																	
reauth	Enable/disable re-authentication upon IKE SA lifetime expiration.	option	-	disable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable IKE SA re-authentication.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable IKE SA re-authentication.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable IKE SA re-authentication.	<i>enable</i>	Enable IKE SA re-authentication.													
Option	Description																			
<i>disable</i>	Disable IKE SA re-authentication.																			
<i>enable</i>	Enable IKE SA re-authentication.																			
rekey	Enable/disable phase1 rekey.	option	-	enable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable phase1 rekey.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable phase1 rekey.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable phase1 rekey.	<i>disable</i>	Disable phase1 rekey.													
Option	Description																			
<i>enable</i>	Enable phase1 rekey.																			
<i>disable</i>	Disable phase1 rekey.																			
remote-gw	IPv4 address of the remote gateway's external interface.	ipv4-address	Not Specified	0.0.0.0																
type	Remote gateway type.	option	-	static																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static</i></td> <td>Remote VPN gateway has fixed IP address.</td> </tr> <tr> <td><i>dynamic</i></td> <td>Remote VPN gateway has dynamic IP address.</td> </tr> <tr> <td><i>ddns</i></td> <td>Remote VPN gateway has dynamic IP address and is a dynamic DNS client.</td> </tr> </tbody> </table>	Option	Description	<i>static</i>	Remote VPN gateway has fixed IP address.	<i>dynamic</i>	Remote VPN gateway has dynamic IP address.	<i>ddns</i>	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.											
Option	Description																			
<i>static</i>	Remote VPN gateway has fixed IP address.																			
<i>dynamic</i>	Remote VPN gateway has dynamic IP address.																			
<i>ddns</i>	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.																			

config vpn ipsec phase2-interface

Configure VPN autokey tunnel.

Syntax

```
config vpn ipsec phase2-interface
  edit <name>
    set dst-end-ip {ipv4-address-any}
    set dst-name {string}
    set dst-start-ip {ipv4-address-any}
    set dst-subnet {ipv4-classnet-any}
    set keylifeseconds {integer}
    set phase1name {string}
    set proposal {option1}, {option2}, ...
    set src-addr-type [subnet|range|...]
    set src-end-ip {ipv4-address-any}
    set src-name {string}
    set src-start-ip {ipv4-address-any}
    set src-subnet {ipv4-classnet-any}
  next
end
```

config vpn ipsec phase2-interface

Parameter	Description	Type	Size	Default
dst-end-ip	Remote proxy ID IPv4 end.	ipv4-address-any	Not Specified	0.0.0.0
dst-name	Remote proxy ID name.	string	Maximum length: 79	
dst-start-ip	Remote proxy ID IPv4 start.	ipv4-address-any	Not Specified	0.0.0.0
dst-subnet	Remote proxy ID IPv4 subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
keylifeseconds	Phase2 key life in time in seconds.	integer	Minimum value: 120 Maximum value: 172800	43200
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 15	
proposal	Phase2 proposal.	option	-	aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305

Parameter	Description	Type	Size	Default																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>aes128-sha1</i></td> <td>aes128-sha1</td> </tr> <tr> <td><i>aes128-sha256</i></td> <td>aes128-sha256</td> </tr> <tr> <td><i>aes128-sha384</i></td> <td>aes128-sha384</td> </tr> <tr> <td><i>aes128-sha512</i></td> <td>aes128-sha512</td> </tr> <tr> <td><i>aes192-sha1</i></td> <td>aes192-sha1</td> </tr> <tr> <td><i>aes192-sha256</i></td> <td>aes192-sha256</td> </tr> <tr> <td><i>aes192-sha384</i></td> <td>aes192-sha384</td> </tr> <tr> <td><i>aes192-sha512</i></td> <td>aes192-sha512</td> </tr> <tr> <td><i>aes256-sha1</i></td> <td>aes256-sha1</td> </tr> <tr> <td><i>aes256-sha256</i></td> <td>aes256-sha256</td> </tr> <tr> <td><i>aes256-sha384</i></td> <td>aes256-sha384</td> </tr> <tr> <td><i>aes256-sha512</i></td> <td>aes256-sha512</td> </tr> <tr> <td><i>aes128gcm</i></td> <td>aes128gcm</td> </tr> <tr> <td><i>aes256gcm</i></td> <td>aes256gcm</td> </tr> <tr> <td><i>chacha20poly1305</i></td> <td>chacha20poly1305</td> </tr> </tbody> </table>	Option	Description	<i>aes128-sha1</i>	aes128-sha1	<i>aes128-sha256</i>	aes128-sha256	<i>aes128-sha384</i>	aes128-sha384	<i>aes128-sha512</i>	aes128-sha512	<i>aes192-sha1</i>	aes192-sha1	<i>aes192-sha256</i>	aes192-sha256	<i>aes192-sha384</i>	aes192-sha384	<i>aes192-sha512</i>	aes192-sha512	<i>aes256-sha1</i>	aes256-sha1	<i>aes256-sha256</i>	aes256-sha256	<i>aes256-sha384</i>	aes256-sha384	<i>aes256-sha512</i>	aes256-sha512	<i>aes128gcm</i>	aes128gcm	<i>aes256gcm</i>	aes256gcm	<i>chacha20poly1305</i>	chacha20poly1305			
Option	Description																																			
<i>aes128-sha1</i>	aes128-sha1																																			
<i>aes128-sha256</i>	aes128-sha256																																			
<i>aes128-sha384</i>	aes128-sha384																																			
<i>aes128-sha512</i>	aes128-sha512																																			
<i>aes192-sha1</i>	aes192-sha1																																			
<i>aes192-sha256</i>	aes192-sha256																																			
<i>aes192-sha384</i>	aes192-sha384																																			
<i>aes192-sha512</i>	aes192-sha512																																			
<i>aes256-sha1</i>	aes256-sha1																																			
<i>aes256-sha256</i>	aes256-sha256																																			
<i>aes256-sha384</i>	aes256-sha384																																			
<i>aes256-sha512</i>	aes256-sha512																																			
<i>aes128gcm</i>	aes128gcm																																			
<i>aes256gcm</i>	aes256gcm																																			
<i>chacha20poly1305</i>	chacha20poly1305																																			
src-addr-type	Local proxy ID type.	option	-	subnet																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>subnet</i></td> <td>IPv4 subnet.</td> </tr> <tr> <td><i>range</i></td> <td>IPv4 range.</td> </tr> <tr> <td><i>ip</i></td> <td>IPv4 IP.</td> </tr> <tr> <td><i>name</i></td> <td>IPv4 firewall address or group name.</td> </tr> </tbody> </table>	Option	Description	<i>subnet</i>	IPv4 subnet.	<i>range</i>	IPv4 range.	<i>ip</i>	IPv4 IP.	<i>name</i>	IPv4 firewall address or group name.																									
Option	Description																																			
<i>subnet</i>	IPv4 subnet.																																			
<i>range</i>	IPv4 range.																																			
<i>ip</i>	IPv4 IP.																																			
<i>name</i>	IPv4 firewall address or group name.																																			
src-end-ip	Local proxy ID end.	ipv4-address-any	Not Specified	0.0.0.0																																
src-name	Local proxy ID name.	string	Maximum length: 79																																	
src-start-ip	Local proxy ID start.	ipv4-address-any	Not Specified	0.0.0.0																																
src-subnet	Local proxy ID subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0																																

webfilter

This section includes syntax for the following commands:

- [config webfilter content-header on page 190](#)
- [config webfilter content on page 191](#)
- [config webfilter fortiguard on page 193](#)
- [config webfilter ftgd-local-cat on page 195](#)
- [config webfilter ftgd-local-rating on page 196](#)
- [config webfilter ips-urlfilter-cache-setting on page 197](#)
- [config webfilter ips-urlfilter-setting on page 197](#)
- [config webfilter profile on page 198](#)
- [config webfilter search-engine on page 208](#)
- [config webfilter urlfilter on page 209](#)

config webfilter content-header

Configure content types used by Web filter.

Syntax

```
config webfilter content-header
  edit <id>
    set comment {var-string}
    config entries
      Description: Configure content types used by web filter.
      edit <pattern>
        set action [block|allow|...]
        set category {user}
      next
    end
  set name {string}
next
end
```

config webfilter content-header

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

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

config entries

Parameter	Description	Type	Size	Default								
action	Action to take for this content type.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Block content type.</td> </tr> <tr> <td><i>allow</i></td> <td>Allow content type.</td> </tr> <tr> <td><i>exempt</i></td> <td>Exempt content type.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Block content type.	<i>allow</i>	Allow content type.	<i>exempt</i>	Exempt content type.			
Option	Description											
<i>block</i>	Block content type.											
<i>allow</i>	Allow content type.											
<i>exempt</i>	Exempt content type.											
category	Categories that this content type applies to.	user	Not Specified	all								
pattern	Content type (regular expression).	string	Maximum length: 31									

config webfilter content

Configure Web filter banned word table.

Syntax

```

config webfilter content
  edit <id>
    set comment {var-string}
    config entries
      Description: Configure banned word entries.
      edit <name>
        set action [block|exempt]
        set lang [western|simch|...]
        set pattern-type [wildcard|regexp]
        set score {integer}
        set status [enable|disable]
      next
    end
  set name {string}

```

```
next
end
```

Parameters

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

config entries

Parameter	Description	Type	Size	Default																				
action	Block or exempt word when a match is found.	option	-	block																				
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>block</i></td><td>Block matches.</td></tr><tr><td><i>exempt</i></td><td>Exempt matches.</td></tr></tbody></table>	Option	Description	<i>block</i>	Block matches.	<i>exempt</i>	Exempt matches.																	
Option	Description																							
<i>block</i>	Block matches.																							
<i>exempt</i>	Exempt matches.																							
lang	Language of banned word.	option	-	western																				
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>western</i></td><td>Western.</td></tr><tr><td><i>simch</i></td><td>Simplified Chinese.</td></tr><tr><td><i>trach</i></td><td>Traditional Chinese.</td></tr><tr><td><i>japanese</i></td><td>Japanese.</td></tr><tr><td><i>korean</i></td><td>Korean.</td></tr><tr><td><i>french</i></td><td>French.</td></tr><tr><td><i>thai</i></td><td>Thai.</td></tr><tr><td><i>spanish</i></td><td>Spanish.</td></tr><tr><td><i>cyrillic</i></td><td>Cyrillic.</td></tr></tbody></table>	Option	Description	<i>western</i>	Western.	<i>simch</i>	Simplified Chinese.	<i>trach</i>	Traditional Chinese.	<i>japanese</i>	Japanese.	<i>korean</i>	Korean.	<i>french</i>	French.	<i>thai</i>	Thai.	<i>spanish</i>	Spanish.	<i>cyrillic</i>	Cyrillic.			
Option	Description																							
<i>western</i>	Western.																							
<i>simch</i>	Simplified Chinese.																							
<i>trach</i>	Traditional Chinese.																							
<i>japanese</i>	Japanese.																							
<i>korean</i>	Korean.																							
<i>french</i>	French.																							
<i>thai</i>	Thai.																							
<i>spanish</i>	Spanish.																							
<i>cyrillic</i>	Cyrillic.																							
name	Banned word.	string	Maximum length: 127																					

Parameter	Description	Type	Size	Default						
pattern-type	Banned word pattern type: wildcard pattern or Perl regular expression.	option	-	wildcard						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>wildcard</i></td> <td>Wildcard pattern.</td> </tr> <tr> <td><i>regex</i></td> <td>Perl regular expression.</td> </tr> </tbody> </table>	Option	Description	<i>wildcard</i>	Wildcard pattern.	<i>regex</i>	Perl regular expression.			
Option	Description									
<i>wildcard</i>	Wildcard pattern.									
<i>regex</i>	Perl regular expression.									
score	Score, to be applied every time the word appears on a web page.	integer	Minimum value: 0 Maximum value: 4294967295	10						
status	Enable/disable banned word.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

config webfilter fortiguard

Configure FortiGuard Web Filter service.

Syntax

```
config webfilter fortiguard
  set cache-mem-percent {integer}
  set cache-mode [ttl|db-ver]
  set cache-prefix-match [enable|disable]
  set close-ports [enable|disable]
  set ovr-auth-https [enable|disable]
  set ovr-auth-port-http {integer}
  set ovr-auth-port-https {integer}
  set ovr-auth-port-https-flow {integer}
  set ovr-auth-port-warning {integer}
  set request-packet-size-limit {integer}
  set warn-auth-https [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default						
cache-mem-percent	Maximum percentage of available memory allocated to caching.	integer	Minimum value: 1 Maximum value: 15	2						
cache-mode	Cache entry expiration mode.	option	-	ttd						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ttd</i></td> <td>Expire cache items by time-to-live.</td> </tr> <tr> <td><i>db-ver</i></td> <td>Expire cache items when the server DB version changes.</td> </tr> </tbody> </table>	Option	Description	<i>ttd</i>	Expire cache items by time-to-live.	<i>db-ver</i>	Expire cache items when the server DB version changes.			
Option	Description									
<i>ttd</i>	Expire cache items by time-to-live.									
<i>db-ver</i>	Expire cache items when the server DB version changes.									
cache-prefix-match	Enable/disable prefix matching in the cache.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
close-ports	Close ports used for HTTP/HTTPS override authentication and disable user overrides.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ovrd-auth-https	Enable/disable use of HTTPS for override authentication.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
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						

Parameter	Description	Type	Size	Default						
id	Local category ID.	integer	Minimum value: 140 Maximum value: 191	0						
status	Enable/disable the local category.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the local category.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the local category.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the local category.	<i>disable</i>	Disable the local category.			
Option	Description									
<i>enable</i>	Enable the local category.									
<i>disable</i>	Disable the local category.									

config webfilter ftgd-local-rating

Configure local FortiGuard Web Filter local ratings.

Syntax

```
config webfilter ftgd-local-rating
  edit <url>
    set comment {var-string}
    set rating {user}
    set status [enable|disable]
  next
end
```

config webfilter ftgd-local-rating

Parameter	Description	Type	Size	Default						
comment	Comment.	var-string	Maximum length: 255							
rating	Local rating.	user	Not Specified							
status	Enable/disable local rating.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local rating.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local rating.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local rating.	<i>disable</i>	Disable local rating.			
Option	Description									
<i>enable</i>	Enable local rating.									
<i>disable</i>	Disable local rating.									
url	URL to rate locally.	string	Maximum length: 511							

config webfilter ips-urlfilter-cache-setting

Configure IPS URL filter cache settings.

Syntax

```
config webfilter ips-urlfilter-cache-setting
  set dns-retry-interval {integer}
  set extended-ttl {integer}
end
```

config webfilter ips-urlfilter-cache-setting

Parameter	Description	Type	Size	Default
dns-retry-interval	Retry interval. Refresh DNS faster than TTL to capture multiple IPs for hosts. 0 means use DNS server's TTL only.	integer	Minimum value: 0 Maximum value: 2147483	0
extended-ttl	Extend time to live beyond reported by DNS. 0 means use DNS server's TTL	integer	Minimum value: 0 Maximum value: 2147483	0

config webfilter ips-urlfilter-setting

Configure IPS URL filter settings.

Syntax

```
config webfilter ips-urlfilter-setting
  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	

Parameter	Description	Type	Size	Default
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 profile

Configure Web filter profiles.

Syntax

```

config webfilter profile
  edit <name>
    set comment {var-string}
    set extended-log [enable|disable]
    config ftgd-wf
      Description: FortiGuard Web Filter settings.
      set exempt-quota {user}
      config filters
        Description: FortiGuard filters.
        edit <id>
          set action [block|authenticate|...]
          set auth-usr-grp <name1>, <name2>, ...
          set category {integer}
          set log [enable|disable]
          set override-replacemsg {string}
          set warn-duration {user}
          set warning-duration-type [session|timeout]
          set warning-prompt [per-domain|per-category]
        next
      end
      set max-quota-timeout {integer}
      set options {option1}, {option2}, ...
      set ovrd {user}
      config quota
        Description: FortiGuard traffic quota settings.
        edit <id>
          set category {user}
          set duration {user}
          set override-replacemsg {string}
          set type [time|traffic]
          set unit [B|KB|...]

```

```

        set value {integer}
    next
end
set rate-crl-urls [disable|enable]
set rate-css-urls [disable|enable]
set rate-javascript-urls [disable|enable]
end
set https-replacemsg [enable|disable]
set log-all-url [enable|disable]
set options {option1}, {option2}, ...
config override
    Description: Web Filter override settings.
    set ovr-d-cookie [allow|deny]
    set ovr-d-dur {user}
    set ovr-d-dur-mode [constant|ask]
    set ovr-d-scope [user|user-group|...]
    set ovr-d-user-group <name1>, <name2>, ...
    set profile <name1>, <name2>, ...
    set profile-attribute [User-Name|NAS-IP-Address|...]
    set profile-type [list|radius]
end
set post-action [normal|block]
set replacemsg-group {string}
config web
    Description: Web content filtering settings.
    set bword-table {integer}
    set bword-threshold {integer}
    set content-header-list {integer}
    set urlfilter-table {integer}
end
set web-content-log [enable|disable]
set web-filter-command-block-log [enable|disable]
set web-filter-cookie-log [enable|disable]
set web-ftgd-err-log [enable|disable]
set web-ftgd-quota-usage [enable|disable]
set web-invalid-domain-log [enable|disable]
set web-url-log [enable|disable]
next
end

```

Parameters

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
extended-log	Enable/disable extended logging for web filtering.	option	-	disable

Parameter	Description	Type	Size	Default																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																					
Option	Description																											
<i>enable</i>	Enable setting.																											
<i>disable</i>	Disable setting.																											
https-replacemsg	Enable replacement messages for HTTPS.	option	-	enable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																					
Option	Description																											
<i>enable</i>	Enable setting.																											
<i>disable</i>	Disable setting.																											
log-all-url	Enable/disable logging all URLs visited.	option	-	disable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																					
Option	Description																											
<i>enable</i>	Enable setting.																											
<i>disable</i>	Disable setting.																											
name	Profile name.	string	Maximum length: 35																									
options	Options.	option	-																									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>activexfilter</i></td> <td>ActiveX filter.</td> </tr> <tr> <td><i>cookiefilter</i></td> <td>Cookie filter.</td> </tr> <tr> <td><i>javafilter</i></td> <td>Java applet filter.</td> </tr> <tr> <td><i>block-invalid-url</i></td> <td>Block sessions contained an invalid domain name.</td> </tr> <tr> <td><i>jscript</i></td> <td>Javascript block.</td> </tr> <tr> <td><i>js</i></td> <td>JS block.</td> </tr> <tr> <td><i>vbs</i></td> <td>VB script block.</td> </tr> <tr> <td><i>unknown</i></td> <td>Unknown script block.</td> </tr> <tr> <td><i>intrinsic</i></td> <td>Intrinsic script block.</td> </tr> <tr> <td><i>wf-referer</i></td> <td>Referring block.</td> </tr> <tr> <td><i>wf-cookie</i></td> <td>Cookie block.</td> </tr> </tbody> </table>	Option	Description	<i>activexfilter</i>	ActiveX filter.	<i>cookiefilter</i>	Cookie filter.	<i>javafilter</i>	Java applet filter.	<i>block-invalid-url</i>	Block sessions contained an invalid domain name.	<i>jscript</i>	Javascript block.	<i>js</i>	JS block.	<i>vbs</i>	VB script block.	<i>unknown</i>	Unknown script block.	<i>intrinsic</i>	Intrinsic script block.	<i>wf-referer</i>	Referring block.	<i>wf-cookie</i>	Cookie block.			
Option	Description																											
<i>activexfilter</i>	ActiveX filter.																											
<i>cookiefilter</i>	Cookie filter.																											
<i>javafilter</i>	Java applet filter.																											
<i>block-invalid-url</i>	Block sessions contained an invalid domain name.																											
<i>jscript</i>	Javascript block.																											
<i>js</i>	JS block.																											
<i>vbs</i>	VB script block.																											
<i>unknown</i>	Unknown script block.																											
<i>intrinsic</i>	Intrinsic script block.																											
<i>wf-referer</i>	Referring block.																											
<i>wf-cookie</i>	Cookie block.																											
post-action	Action taken for HTTP POST traffic.	option	-	normal																								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>normal</i></td> <td>Normal, POST requests are allowed.</td> </tr> <tr> <td><i>block</i></td> <td>POST requests are blocked.</td> </tr> </tbody> </table>	Option	Description	<i>normal</i>	Normal, POST requests are allowed.	<i>block</i>	POST requests are blocked.			
Option	Description									
<i>normal</i>	Normal, POST requests are allowed.									
<i>block</i>	POST requests are blocked.									
replacemsg-group	Replacement message group.	string	Maximum length: 35							
web-content-log	Enable/disable logging logging blocked web content.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-command-block-log	Enable/disable logging logging blocked commands.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-cookie-log	Enable/disable logging cookie filtering.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-ftgd-err-log	Enable/disable logging rating errors.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-ftgd-quota-usage	Enable/disable logging daily quota usage.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.					
Option	Description									
<i>enable</i>	Enable setting.									

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable setting.					
Option	Description									
<i>disable</i>	Disable setting.									
web-invalid-domain-log	Enable/disable logging invalid domain names.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-url-log	Enable/disable logging URL filtering.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

config ftgd-wf

Parameter	Description	Type	Size	Default										
exempt-quota	Do not stop quota for these categories.	user	Not Specified	17										
max-quota-timeout	Maximum FortiGuard quota used by single page view in seconds (excludes streams).	integer	Minimum value: 1 Maximum value: 86400	300										
options	Options for FortiGuard Web Filter.	option	-											
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>error-allow</i></td> <td>Allow web pages with a rating error to pass through.</td> </tr> <tr> <td><i>rate-server-ip</i></td> <td>Rate the server IP in addition to the domain name.</td> </tr> <tr> <td><i>connect-request-bypass</i></td> <td>Bypass connection which has CONNECT request.</td> </tr> <tr> <td><i>ftgd-disable</i></td> <td>Disable FortiGuard scanning.</td> </tr> </tbody> </table>	Option	Description	<i>error-allow</i>	Allow web pages with a rating error to pass through.	<i>rate-server-ip</i>	Rate the server IP in addition to the domain name.	<i>connect-request-bypass</i>	Bypass connection which has CONNECT request.	<i>ftgd-disable</i>	Disable FortiGuard scanning.			
Option	Description													
<i>error-allow</i>	Allow web pages with a rating error to pass through.													
<i>rate-server-ip</i>	Rate the server IP in addition to the domain name.													
<i>connect-request-bypass</i>	Bypass connection which has CONNECT request.													
<i>ftgd-disable</i>	Disable FortiGuard scanning.													
ovrd	Allow web filter profile overrides.	user	Not Specified											
rate-crl-urls	Enable/disable rating CRL by URL.	option	-	enable										

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable rating CRL by URL.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable rating CRL by URL.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable rating CRL by URL.	<i>enable</i>	Enable rating CRL by URL.			
Option	Description									
<i>disable</i>	Disable rating CRL by URL.									
<i>enable</i>	Enable rating CRL by URL.									
rate-css-urls	Enable/disable rating CSS by URL.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable rating CSS by URL.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable rating CSS by URL.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable rating CSS by URL.	<i>enable</i>	Enable rating CSS by URL.			
Option	Description									
<i>disable</i>	Disable rating CSS by URL.									
<i>enable</i>	Enable rating CSS by URL.									
rate-javascript-urls	Enable/disable rating JavaScript by URL.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable rating JavaScript by URL.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable rating JavaScript by URL.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable rating JavaScript by URL.	<i>enable</i>	Enable rating JavaScript by URL.			
Option	Description									
<i>disable</i>	Disable rating JavaScript by URL.									
<i>enable</i>	Enable rating JavaScript by URL.									

config filters

Parameter	Description	Type	Size	Default										
action	Action to take for matches.	option	-	monitor										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Block access.</td> </tr> <tr> <td><i>authenticate</i></td> <td>Authenticate user before allowing access.</td> </tr> <tr> <td><i>monitor</i></td> <td>Allow access while logging the action.</td> </tr> <tr> <td><i>warning</i></td> <td>Allow access after warning the user.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Block access.	<i>authenticate</i>	Authenticate user before allowing access.	<i>monitor</i>	Allow access while logging the action.	<i>warning</i>	Allow access after warning the user.			
Option	Description													
<i>block</i>	Block access.													
<i>authenticate</i>	Authenticate user before allowing access.													
<i>monitor</i>	Allow access while logging the action.													
<i>warning</i>	Allow access after warning the user.													
auth-usr-grp <name>	Groups with permission to authenticate. User group name.	string	Maximum length: 79											
category	Categories and groups the filter examines.	integer	Minimum value: 0 Maximum value: 255	0										
id	ID number.	integer	Minimum value: 0 Maximum value: 255	0										

Parameter	Description	Type	Size	Default						
log	Enable/disable logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
override-replacemsg	Override replacement message.	string	Maximum length: 28							
warn-duration	Duration of warnings.	user	Not Specified	5m						
warning-duration-type	Re-display warning after closing browser or after a timeout.	option	-	timeout						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>session</i></td> <td>After session ends.</td> </tr> <tr> <td><i>timeout</i></td> <td>After timeout occurs.</td> </tr> </tbody> </table>	Option	Description	<i>session</i>	After session ends.	<i>timeout</i>	After timeout occurs.			
Option	Description									
<i>session</i>	After session ends.									
<i>timeout</i>	After timeout occurs.									
warning-prompt	Warning prompts in each category or each domain.	option	-	per-category						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>per-domain</i></td> <td>Per-domain warnings.</td> </tr> <tr> <td><i>per-category</i></td> <td>Per-category warnings.</td> </tr> </tbody> </table>	Option	Description	<i>per-domain</i>	Per-domain warnings.	<i>per-category</i>	Per-category warnings.			
Option	Description									
<i>per-domain</i>	Per-domain warnings.									
<i>per-category</i>	Per-category warnings.									

config quota

Parameter	Description	Type	Size	Default
category	FortiGuard categories to apply quota to (category action must be set to monitor).	user	Not Specified	
duration	Duration of quota.	user	Not Specified	5m
id	ID number.	integer	Minimum value: 0 Maximum value: 4294967295	0
override-replacemsg	Override replacement message.	string	Maximum length: 28	
type	Quota type.	option	-	time

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>time</i></td> <td>Use a time-based quota.</td> </tr> <tr> <td><i>traffic</i></td> <td>Use a traffic-based quota.</td> </tr> </tbody> </table>	Option	Description	<i>time</i>	Use a time-based quota.	<i>traffic</i>	Use a traffic-based quota.							
Option	Description													
<i>time</i>	Use a time-based quota.													
<i>traffic</i>	Use a traffic-based quota.													
unit	Traffic quota unit of measurement.	option	-	MB										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>B</i></td> <td>Quota in bytes.</td> </tr> <tr> <td><i>KB</i></td> <td>Quota in kilobytes.</td> </tr> <tr> <td><i>MB</i></td> <td>Quota in megabytes.</td> </tr> <tr> <td><i>GB</i></td> <td>Quota in gigabytes.</td> </tr> </tbody> </table>	Option	Description	<i>B</i>	Quota in bytes.	<i>KB</i>	Quota in kilobytes.	<i>MB</i>	Quota in megabytes.	<i>GB</i>	Quota in gigabytes.			
Option	Description													
<i>B</i>	Quota in bytes.													
<i>KB</i>	Quota in kilobytes.													
<i>MB</i>	Quota in megabytes.													
<i>GB</i>	Quota in gigabytes.													
value	Traffic quota value.	integer	Minimum value: 1 Maximum value: 4294967295	1024										

config override

Parameter	Description	Type	Size	Default						
ovrd-cookie	Allow/deny browser-based (cookie) overrides.	option	-	deny						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow browser-based (cookie) override.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny browser-based (cookie) override.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow browser-based (cookie) override.	<i>deny</i>	Deny browser-based (cookie) override.			
Option	Description									
<i>allow</i>	Allow browser-based (cookie) override.									
<i>deny</i>	Deny browser-based (cookie) override.									
ovrd-dur	Override duration.	user	Not Specified	15m						
ovrd-dur-mode	Override duration mode.	option	-	constant						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>constant</i></td> <td>Constant mode.</td> </tr> <tr> <td><i>ask</i></td> <td>Prompt for duration when initiating an override.</td> </tr> </tbody> </table>	Option	Description	<i>constant</i>	Constant mode.	<i>ask</i>	Prompt for duration when initiating an override.			
Option	Description									
<i>constant</i>	Constant mode.									
<i>ask</i>	Prompt for duration when initiating an override.									
ovrd-scope	Override scope.	option	-	user						

Parameter	Description	Type	Size	Default																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>user</i></td> <td>Override for the user.</td> </tr> <tr> <td><i>user-group</i></td> <td>Override for the user's group.</td> </tr> <tr> <td><i>ip</i></td> <td>Override for the initiating IP.</td> </tr> <tr> <td><i>browser</i></td> <td>Create browser-based (cookie) override.</td> </tr> <tr> <td><i>ask</i></td> <td>Prompt for scope when initiating an override.</td> </tr> </tbody> </table>	Option	Description	<i>user</i>	Override for the user.	<i>user-group</i>	Override for the user's group.	<i>ip</i>	Override for the initiating IP.	<i>browser</i>	Create browser-based (cookie) override.	<i>ask</i>	Prompt for scope when initiating an override.																					
Option	Description																																	
<i>user</i>	Override for the user.																																	
<i>user-group</i>	Override for the user's group.																																	
<i>ip</i>	Override for the initiating IP.																																	
<i>browser</i>	Create browser-based (cookie) override.																																	
<i>ask</i>	Prompt for scope when initiating an override.																																	
ovrd-user-group <name>	User groups with permission to use the override. User group name.	string	Maximum length: 79																															
profile <name>	Web filter profile with permission to create overrides. Web profile.	string	Maximum length: 79																															
profile-attribute	Profile attribute to retrieve from the RADIUS server.	option	-	Login-LAT-Service																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>User-Name</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>NAS-IP-Address</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-IP-Address</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-IP-Netmask</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Filter-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-IP-Host</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Reply-Message</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Callback-Number</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Callback-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-Route</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-IPX-Network</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Class</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Called-Station-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Calling-Station-Id</i></td> <td>Use this attribute.</td> </tr> </tbody> </table>	Option	Description	<i>User-Name</i>	Use this attribute.	<i>NAS-IP-Address</i>	Use this attribute.	<i>Framed-IP-Address</i>	Use this attribute.	<i>Framed-IP-Netmask</i>	Use this attribute.	<i>Filter-Id</i>	Use this attribute.	<i>Login-IP-Host</i>	Use this attribute.	<i>Reply-Message</i>	Use this attribute.	<i>Callback-Number</i>	Use this attribute.	<i>Callback-Id</i>	Use this attribute.	<i>Framed-Route</i>	Use this attribute.	<i>Framed-IPX-Network</i>	Use this attribute.	<i>Class</i>	Use this attribute.	<i>Called-Station-Id</i>	Use this attribute.	<i>Calling-Station-Id</i>	Use this attribute.			
Option	Description																																	
<i>User-Name</i>	Use this attribute.																																	
<i>NAS-IP-Address</i>	Use this attribute.																																	
<i>Framed-IP-Address</i>	Use this attribute.																																	
<i>Framed-IP-Netmask</i>	Use this attribute.																																	
<i>Filter-Id</i>	Use this attribute.																																	
<i>Login-IP-Host</i>	Use this attribute.																																	
<i>Reply-Message</i>	Use this attribute.																																	
<i>Callback-Number</i>	Use this attribute.																																	
<i>Callback-Id</i>	Use this attribute.																																	
<i>Framed-Route</i>	Use this attribute.																																	
<i>Framed-IPX-Network</i>	Use this attribute.																																	
<i>Class</i>	Use this attribute.																																	
<i>Called-Station-Id</i>	Use this attribute.																																	
<i>Calling-Station-Id</i>	Use this attribute.																																	

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>NAS-Identifier</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Proxy-State</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-LAT-Service</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-LAT-Node</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-LAT-Group</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-AppleTalk-Zone</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Acct-Session-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Acct-Multi-Session-Id</i></td> <td>Use this attribute.</td> </tr> </tbody> </table>	Option	Description	<i>NAS-Identifier</i>	Use this attribute.	<i>Proxy-State</i>	Use this attribute.	<i>Login-LAT-Service</i>	Use this attribute.	<i>Login-LAT-Node</i>	Use this attribute.	<i>Login-LAT-Group</i>	Use this attribute.	<i>Framed-AppleTalk-Zone</i>	Use this attribute.	<i>Acct-Session-Id</i>	Use this attribute.	<i>Acct-Multi-Session-Id</i>	Use this attribute.			
Option	Description																					
<i>NAS-Identifier</i>	Use this attribute.																					
<i>Proxy-State</i>	Use this attribute.																					
<i>Login-LAT-Service</i>	Use this attribute.																					
<i>Login-LAT-Node</i>	Use this attribute.																					
<i>Login-LAT-Group</i>	Use this attribute.																					
<i>Framed-AppleTalk-Zone</i>	Use this attribute.																					
<i>Acct-Session-Id</i>	Use this attribute.																					
<i>Acct-Multi-Session-Id</i>	Use this attribute.																					
profile-type	Override profile type.	option	-	list																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>list</i></td> <td>Profile chosen from list.</td> </tr> <tr> <td><i>radius</i></td> <td>Profile determined by RADIUS server.</td> </tr> </tbody> </table>	Option	Description	<i>list</i>	Profile chosen from list.	<i>radius</i>	Profile determined by RADIUS server.															
Option	Description																					
<i>list</i>	Profile chosen from list.																					
<i>radius</i>	Profile determined by RADIUS server.																					

config web

Parameter	Description	Type	Size	Default
bword-table	Banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
bword-threshold	Banned word score threshold.	integer	Minimum value: 0 Maximum value: 2147483647	10
content-header-list	Content header list.	integer	Minimum value: 0 Maximum value: 4294967295	0

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

config webfilter search-engine

Configure web filter search engines.

Syntax

```

config webfilter search-engine
  edit <name>
    set charset [utf-8|gb2312]
    set hostname {string}
    set query {string}
    set safesearch [disable|url|...]
    set safesearch-str {string}
    set url {string}
  next
end

```

config webfilter search-engine

Parameter	Description	Type	Size	Default						
charset	Search engine charset.	option	-	utf-8						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>utf-8</i></td> <td>UTF-8 encoding.</td> </tr> <tr> <td><i>gb2312</i></td> <td>GB2312 encoding.</td> </tr> </tbody> </table>	Option	Description	<i>utf-8</i>	UTF-8 encoding.	<i>gb2312</i>	GB2312 encoding.			
Option	Description									
<i>utf-8</i>	UTF-8 encoding.									
<i>gb2312</i>	GB2312 encoding.									
hostname	Hostname (regular expression).	string	Maximum length: 127							
name	Search engine name.	string	Maximum length: 35							
query	Code used to prefix a query (must end with an equals character).	string	Maximum length: 15							
safesearch	Safe search method. You can disable safe search, add the safe search string to URLs, or insert a safe search header.	option	-	disable						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Site does not support safe search.</td> </tr> <tr> <td><i>url</i></td> <td>Safe search selected with a parameter in the URL.</td> </tr> <tr> <td><i>header</i></td> <td>Safe search selected by search header (i.e. youtube.edu).</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Site does not support safe search.	<i>url</i>	Safe search selected with a parameter in the URL.	<i>header</i>	Safe search selected by search header (i.e. youtube.edu).			
Option	Description											
<i>disable</i>	Site does not support safe search.											
<i>url</i>	Safe search selected with a parameter in the URL.											
<i>header</i>	Safe search selected by search header (i.e. youtube.edu).											
safesearch-str	Safe search parameter used in the URL.	string	Maximum length: 79									
url	URL (regular expression).	string	Maximum length: 127									

config webfilter urlfilter

Configure URL filter lists.

Syntax

```

config webfilter urlfilter
  edit <id>
    set comment {var-string}
    config entries
      Description: URL filter entries.
      edit <id>
        set action [exempt|block|...]
        set antiphish-action [block|log]
        set dns-address-family {option}
        set exempt {option1}, {option2}, ...
        set referrer-host {string}
        set status [enable|disable]
        set type [simple|regex|...]
        set url {string}
        set web-proxy-profile {string}
      next
    end
    set ip-addr-block [enable|disable]
    set name {string}
    set one-arm-ips-urlfilter [enable|disable]
  next
end

```

Parameters

Parameter	Description	Type	Size	Default						
comment	Optional comments.	var-string	Maximum length: 255							
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
ip-addr-block	Enable/disable blocking URLs when the hostname appears as an IP address.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable blocking URLs when the hostname appears as an IP address.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable blocking URLs when the hostname appears as an IP address.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable blocking URLs when the hostname appears as an IP address.	<i>disable</i>	Disable blocking URLs when the hostname appears as an IP address.			
Option	Description									
<i>enable</i>	Enable blocking URLs when the hostname appears as an IP address.									
<i>disable</i>	Disable blocking URLs when the hostname appears as an IP address.									
name	Name of URL filter list.	string	Maximum length: 63							
one-arm-ips-urfilter	Enable/disable DNS resolver for one-arm IPS URL filter operation.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DNS resolver for one-arm IPS URL filter operation.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DNS resolver for one-arm IPS URL filter operation.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DNS resolver for one-arm IPS URL filter operation.	<i>disable</i>	Disable DNS resolver for one-arm IPS URL filter operation.			
Option	Description									
<i>enable</i>	Enable DNS resolver for one-arm IPS URL filter operation.									
<i>disable</i>	Disable DNS resolver for one-arm IPS URL filter operation.									

config entries

Parameter	Description	Type	Size	Default										
action	Action to take for URL filter matches.	option	-	exempt										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>exempt</i></td> <td>Exempt matches.</td> </tr> <tr> <td><i>block</i></td> <td>Block matches.</td> </tr> <tr> <td><i>allow</i></td> <td>Allow matches (no log).</td> </tr> <tr> <td><i>monitor</i></td> <td>Allow matches (with log).</td> </tr> </tbody> </table>	Option	Description	<i>exempt</i>	Exempt matches.	<i>block</i>	Block matches.	<i>allow</i>	Allow matches (no log).	<i>monitor</i>	Allow matches (with log).			
Option	Description													
<i>exempt</i>	Exempt matches.													
<i>block</i>	Block matches.													
<i>allow</i>	Allow matches (no log).													
<i>monitor</i>	Allow matches (with log).													
antiphish-action	Action to take for AntiPhishing matches.	option	-	block										

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Block matches.</td> </tr> <tr> <td><i>log</i></td> <td>Allow matches with log.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Block matches.	<i>log</i>	Allow matches with log.																	
Option	Description																							
<i>block</i>	Block matches.																							
<i>log</i>	Allow matches with log.																							
dns-address-family	Resolve IPv4 address from DNS server.	option	-	ipv4																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipv4</i></td> <td>Resolve IPv4 address from DNS server.</td> </tr> </tbody> </table>	Option	Description	<i>ipv4</i>	Resolve IPv4 address from DNS server.																			
Option	Description																							
<i>ipv4</i>	Resolve IPv4 address from DNS server.																							
exempt	If action is set to exempt, select the security profile operations that exempt URLs skip. Separate multiple options with a space.	option	-	av web-content activex-java-cookie dlp fortiguard range-block antiphish all																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>av</i></td> <td>AntiVirus scanning.</td> </tr> <tr> <td><i>web-content</i></td> <td>Web filter content matching.</td> </tr> <tr> <td><i>activex-java-cookie</i></td> <td>ActiveX, Java, and cookie filtering.</td> </tr> <tr> <td><i>dlp</i></td> <td>DLP scanning.</td> </tr> <tr> <td><i>fortiguard</i></td> <td>FortiGuard web filtering.</td> </tr> <tr> <td><i>range-block</i></td> <td>Range block feature.</td> </tr> <tr> <td><i>pass</i></td> <td>Pass single connection from all.</td> </tr> <tr> <td><i>antiphish</i></td> <td>AntiPhish credential checking.</td> </tr> <tr> <td><i>all</i></td> <td>Exempt from all security profiles.</td> </tr> </tbody> </table>	Option	Description	<i>av</i>	AntiVirus scanning.	<i>web-content</i>	Web filter content matching.	<i>activex-java-cookie</i>	ActiveX, Java, and cookie filtering.	<i>dlp</i>	DLP scanning.	<i>fortiguard</i>	FortiGuard web filtering.	<i>range-block</i>	Range block feature.	<i>pass</i>	Pass single connection from all.	<i>antiphish</i>	AntiPhish credential checking.	<i>all</i>	Exempt from all security profiles.			
Option	Description																							
<i>av</i>	AntiVirus scanning.																							
<i>web-content</i>	Web filter content matching.																							
<i>activex-java-cookie</i>	ActiveX, Java, and cookie filtering.																							
<i>dlp</i>	DLP scanning.																							
<i>fortiguard</i>	FortiGuard web filtering.																							
<i>range-block</i>	Range block feature.																							
<i>pass</i>	Pass single connection from all.																							
<i>antiphish</i>	AntiPhish credential checking.																							
<i>all</i>	Exempt from all security profiles.																							
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295	0																				
referrer-host	Referrer host name.	string	Maximum length: 255																					
status	Enable/disable this URL filter.	option	-	enable																				

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this URL filter.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this URL filter.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this URL filter.	<i>disable</i>	Disable this URL filter.					
Option	Description											
<i>enable</i>	Enable this URL filter.											
<i>disable</i>	Disable this URL filter.											
type	Filter type (simple, regex, or wildcard).	option	-	simple								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>simple</i></td> <td>Simple URL string.</td> </tr> <tr> <td><i>regex</i></td> <td>Regular expression URL string.</td> </tr> <tr> <td><i>wildcard</i></td> <td>Wildcard URL string.</td> </tr> </tbody> </table>	Option	Description	<i>simple</i>	Simple URL string.	<i>regex</i>	Regular expression URL string.	<i>wildcard</i>	Wildcard URL string.			
Option	Description											
<i>simple</i>	Simple URL string.											
<i>regex</i>	Regular expression URL string.											
<i>wildcard</i>	Wildcard URL string.											
url	URL to be filtered.	string	Maximum length: 511									
web-proxy-profile	Web proxy profile.	string	Maximum length: 63									

diagnose

Use `diagnose` commands to view and debug system information.

- [diagnose autoupdate versions on page 212](#)
- [diagnose debug on page 212](#)
- [diagnose sniffer packet on page 214](#)
- [diagnose sys on page 215](#)
- [diagnose test application on page 216](#)

diagnose autoupdate versions

Dump database and engine versions.

For each database, this command displays the database version as well as the time and result of the last update attempt, if applicable.

```
diagnose autoupdate versions
```

diagnose debug

Enable or disable debugging and view debugging configuration.

diagnose debug application

Set or view debugging levels for each application.

```
diagnose debug application <application> [debug level]
```

diagnose debug application

Parameter	Description	Type	Size	Default																										
application	Application name	string	-																											
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>certd</i></td><td>Certificate service daemon.</td></tr><tr><td><i>cmdbwatcher</i></td><td>Configuration management watcher.</td></tr><tr><td><i>httpd</i></td><td>HTTPD daemon.</td></tr><tr><td><i>iked</i></td><td>IKE daemon.</td></tr><tr><td><i>ipsengine</i></td><td>IPS engine.</td></tr><tr><td><i>ipsmonitor</i></td><td>IPS monitor.</td></tr><tr><td><i>miglogd</i></td><td>Log daemon.</td></tr><tr><td><i>restapi</i></td><td>REST API daemon.</td></tr><tr><td><i>scanunitd</i></td><td>Scan unit daemon.</td></tr><tr><td><i>syslogd</i></td><td>syslogd daemon.</td></tr><tr><td><i>urlfilter</i></td><td>URL filter daemon.</td></tr><tr><td><i>vipproxy</i></td><td>VIP proxy daemon.</td></tr></tbody></table>	Option	Description	<i>certd</i>	Certificate service daemon.	<i>cmdbwatcher</i>	Configuration management watcher.	<i>httpd</i>	HTTPD daemon.	<i>iked</i>	IKE daemon.	<i>ipsengine</i>	IPS engine.	<i>ipsmonitor</i>	IPS monitor.	<i>miglogd</i>	Log daemon.	<i>restapi</i>	REST API daemon.	<i>scanunitd</i>	Scan unit daemon.	<i>syslogd</i>	syslogd daemon.	<i>urlfilter</i>	URL filter daemon.	<i>vipproxy</i>	VIP proxy daemon.			
Option	Description																													
<i>certd</i>	Certificate service daemon.																													
<i>cmdbwatcher</i>	Configuration management watcher.																													
<i>httpd</i>	HTTPD daemon.																													
<i>iked</i>	IKE daemon.																													
<i>ipsengine</i>	IPS engine.																													
<i>ipsmonitor</i>	IPS monitor.																													
<i>miglogd</i>	Log daemon.																													
<i>restapi</i>	REST API daemon.																													
<i>scanunitd</i>	Scan unit daemon.																													
<i>syslogd</i>	syslogd daemon.																													
<i>urlfilter</i>	URL filter daemon.																													
<i>vipproxy</i>	VIP proxy daemon.																													
debug level	<p>Set the debug level. Each application has different debug levels available. To see the available levels and the current setting, enter the command without the debug level value. For example, <code>diagnose debug application iked</code> displays:</p> <pre>ike debug level is 0 0: none, 1: error, 2: warning, 3: info, 4: debug</pre>	string	-																											

diagnose debug disable

Disable debugging.

```
diagnose debug disable
```

diagnose debug enable

Enable debugging.

```
diagnose debug enable
```

diagnose router info routing-table all

Show all routing table entries.

```
diagnose router info routing-table all
```

diagnose sniffer packet

Run a packet sniffer to view network traffic.

```
diagnose sniffer packet [<interface> <filter> <verbose> <count> <tsformat> <frame size>]
```

diagnose sniffer packet

Parameter	Description	Type	Size	Default
interface	Network interface to sniff (or "any").	string	-	any
filter	Flexible logical filters for sniffer (or "none"). For example: To print UDP 1812 traffic between fort1 and either fort2 or fort3: udp and port 1812 and host fort1 and (fort2 or fort3)	string	-	
verbose	<ul style="list-style-type: none">1: Print header of packets.2: Print header and data from IP of packets.3: Print header and data from ethernet of packets (if available).4: Print header of packets with interface name.5: Print header and data from IP of packets with interface name.6: Print header and data from ethernet of packets (if available) with interface name.	integer	Minimum value: 1 Maximum value: 6	1

Parameter	Description	Type	Size	Default
count	Sniffer count.	integer		
tsformat	Format of timestamp. <ul style="list-style-type: none"> a: absolute UTC time, yyyy-mm-dd hh:mm:ss.ms l: absolute LOCAL time, yyyy-mm-dd hh:mm:ss.ms otherwise: relative to the start of sniffing, ss.ms 	string		
frame size	Set the frame size that is printed before truncation. Defaults to the interface MTU.			

diagnose sys

View system information.

- [diagnose sys botnet-ip list on page 215](#)
- [diagnose sys license on page 215](#)
- [diagnose sys status on page 216](#)
- [diagnose sys top on page 216](#)

diagnose sys botnet-ip list

List known botnets.

```
diagnose sys botnet-ip list
```

diagnose sys license

Show license information.

```
diagnose sys license
```

diagnose sys license

Field	Description
Status	The license status.
SN	The device serial number.
Valid From	The license start date.
Valid To	The license expiration date.

diagnose sys status

Show system status.

```
diagnose sys status
```

diagnose sys status

Field	Description
Version	The Container FortiOS version and build number.
Serial-Number	The device serial number.
System time	The current system time, with timezone.

diagnose sys top

Show top processes information.

```
diagnose sys top
```

This command is similar to the standard Linux `top` command, with a limited set of interactions available. The set of columns displayed is not editable.

By default, the table is sorted by %CPU.

The following interactive commands are available:

Command	Description
S s	Turn on cumulative time mode. Each process is listed with the CPU time it and its children have used.
1 C c	Toggle CPU single or separate display in the summary area.
M m	Sort by %MEM (memory usage) column, which is not displayed.
N n	Sort by PID (process ID) column.
P p	Sort by %CPU (CPU usage) column.
R r	Reverse the order of the current sort.
Up, PgUp, down, PgDn	Scroll up or down through the list.
Home, End	Scroll to the top of bottom of the list.

diagnose test application

Test, view information about, and perform operations on system applications.

```
diagnose test application <application> [option]
```

diagnose test application

Parameter	Description	Type	Size	Default										
application	Application name	string	-											
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>ipsmonitor</i></td><td>Display information about the IPS engine and perform operations.</td></tr><tr><td><i>miglogd</i></td><td>View local log daemon information.</td></tr><tr><td><i>syslogd</i></td><td>View syslogd daemon information.</td></tr><tr><td><i>restapi</i></td><td>Test access to the REST API.</td></tr></tbody></table>	Option	Description	<i>ipsmonitor</i>	Display information about the IPS engine and perform operations.	<i>miglogd</i>	View local log daemon information.	<i>syslogd</i>	View syslogd daemon information.	<i>restapi</i>	Test access to the REST API.			
Option	Description													
<i>ipsmonitor</i>	Display information about the IPS engine and perform operations.													
<i>miglogd</i>	View local log daemon information.													
<i>syslogd</i>	View syslogd daemon information.													
<i>restapi</i>	Test access to the REST API.													

ipsmonitor

Parameter	Description	Type	Size	Default																																
option	The information to display or operation to perform.	integer	-																																	
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>1</td><td>Display IPS engine information.</td></tr><tr><td>2</td><td>Toggle IPS engine enable/disable status.</td></tr><tr><td>3</td><td>Display restart log.</td></tr><tr><td>4</td><td>Clear restart log.</td></tr><tr><td>5</td><td>Toggle bypass status.</td></tr><tr><td>6</td><td>Submit attack characteristics now.</td></tr><tr><td>10</td><td>IPS queue length.</td></tr><tr><td>11</td><td>Clear IPS queue length.</td></tr><tr><td>12</td><td>IPS L7 socket statistics.</td></tr><tr><td>13</td><td>IPS session list.</td></tr><tr><td>14</td><td>IPS NTurbo statistics.</td></tr><tr><td>15</td><td>IPSA statistics.</td></tr><tr><td>18</td><td>Display session info cache.</td></tr><tr><td>19</td><td>Clear session info cache.</td></tr><tr><td>21</td><td>Reload FSA malicious URL database.</td></tr></tbody></table>	Option	Description	1	Display IPS engine information.	2	Toggle IPS engine enable/disable status.	3	Display restart log.	4	Clear restart log.	5	Toggle bypass status.	6	Submit attack characteristics now.	10	IPS queue length.	11	Clear IPS queue length.	12	IPS L7 socket statistics.	13	IPS session list.	14	IPS NTurbo statistics.	15	IPSA statistics.	18	Display session info cache.	19	Clear session info cache.	21	Reload FSA malicious URL database.			
Option	Description																																			
1	Display IPS engine information.																																			
2	Toggle IPS engine enable/disable status.																																			
3	Display restart log.																																			
4	Clear restart log.																																			
5	Toggle bypass status.																																			
6	Submit attack characteristics now.																																			
10	IPS queue length.																																			
11	Clear IPS queue length.																																			
12	IPS L7 socket statistics.																																			
13	IPS session list.																																			
14	IPS NTurbo statistics.																																			
15	IPSA statistics.																																			
18	Display session info cache.																																			
19	Clear session info cache.																																			
21	Reload FSA malicious URL database.																																			

Parameter	Description	Type	Size	Default																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>22</td> <td>Reload allowlist URL database.</td> </tr> <tr> <td>24</td> <td>Display Flow AV statistics.</td> </tr> <tr> <td>25</td> <td>Reset Flow AV statistics.</td> </tr> <tr> <td>32</td> <td>Reload certificate blocklist database.</td> </tr> <tr> <td>40</td> <td>Display packet log statistics.</td> </tr> <tr> <td>41</td> <td>Reset packet log statistics.</td> </tr> <tr> <td>96</td> <td>Toggle IPS engines watchdog timer.</td> </tr> <tr> <td>97</td> <td>Start all IPS engines.</td> </tr> <tr> <td>98</td> <td>Stop all IPS engines.</td> </tr> <tr> <td>99</td> <td>Restart all IPS engines and monitor.</td> </tr> </tbody> </table>	Option	Description	22	Reload allowlist URL database.	24	Display Flow AV statistics.	25	Reset Flow AV statistics.	32	Reload certificate blocklist database.	40	Display packet log statistics.	41	Reset packet log statistics.	96	Toggle IPS engines watchdog timer.	97	Start all IPS engines.	98	Stop all IPS engines.	99	Restart all IPS engines and monitor.			
Option	Description																									
22	Reload allowlist URL database.																									
24	Display Flow AV statistics.																									
25	Reset Flow AV statistics.																									
32	Reload certificate blocklist database.																									
40	Display packet log statistics.																									
41	Reset packet log statistics.																									
96	Toggle IPS engines watchdog timer.																									
97	Start all IPS engines.																									
98	Stop all IPS engines.																									
99	Restart all IPS engines and monitor.																									

miglod

Parameter	Description	Type	Size	Default								
option	The information to display or operation to perform.	integer	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>4</td> <td>Show log statistics.</td> </tr> <tr> <td>16</td> <td>Show log disk usage.</td> </tr> <tr> <td>48</td> <td>Show publish info.</td> </tr> </tbody> </table>	Option	Description	4	Show log statistics.	16	Show log disk usage.	48	Show publish info.			
Option	Description											
4	Show log statistics.											
16	Show log disk usage.											
48	Show publish info.											

syslogd

Parameter	Description	Type	Size	Default														
option	The information to display or operation to perform.	integer	-															
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Show syslog setting.</td> </tr> <tr> <td>3</td> <td>Show syslog statistics</td> </tr> <tr> <td>5</td> <td>Show dropped logs due to log rate limit for all devices.</td> </tr> <tr> <td>6</td> <td>Show subscribe log info</td> </tr> <tr> <td>7</td> <td>Show subscribe log filter</td> </tr> <tr> <td>9</td> <td>Show remote sockets.</td> </tr> </tbody> </table>	Option	Description	1	Show syslog setting.	3	Show syslog statistics	5	Show dropped logs due to log rate limit for all devices.	6	Show subscribe log info	7	Show subscribe log filter	9	Show remote sockets.			
Option	Description																	
1	Show syslog setting.																	
3	Show syslog statistics																	
5	Show dropped logs due to log rate limit for all devices.																	
6	Show subscribe log info																	
7	Show subscribe log filter																	
9	Show remote sockets.																	

restapi

Parameter	Description	Type	Size	Default
host	The REST API host address.	ipv4-address or FQDN	-	
port	The REST API host listening port.	integer	-	

execute

Execute static commands.

Syntax

```
execute {
  api-user generate-key <name>
  config backup <filename> [password] |
  import-vmlicense <license_string> |
  log filter category <category> |
  log filter device <device> |
  log filter dump |
  log display |
  log delete |
  log delete-all |
  ping <host> |
  shutdown |
  telnet <host> [port] |
  update-now |
}
```

Commands

Command	Description
config backup	Back up full configuration to <filename> in the /data directory. If password is specified, the backup config file will be encrypted with it.
import-vmlicense	Import license. Paste the full contents of the license file, enclosed in quotes.
log filter category	Specify the log category to filter on for display or delete. Press Enter without entering a category to see a list of available categories.

Command	Description
log filter device	Specify the log category to filter on for <code>display</code> or <code>delete</code> . Press Enter without entering a device to see a list of available devices.
log filter dump	Display the currently set log filters.
log display	Display the logs matching the currently set log filters.
log delete	Delete the logs matching the currently set log filters.
log delete-all	Delete all logs.
ping	Ping remote hosts. <code>host</code> may be an IP address or fully qualified domain name.
shutdown	Shutdown system immediately.
telnet	Connect to <code>host</code> using a simple telnet client.
update-now	Update FortiGuard definitions.

exit

Exit the CLI.

`exit` can only be used at the root level of the CLI.

Usage

```
exit
```

get

Use `get` to display dynamic and system information.

The syntax and options for `get` are usually the same as `config`.

For example, `get firewall address` displays a result similar to the following:

```
== [ FABRIC_DEVICE ]
name: FABRIC_DEVICE
== [ all ]
name: all
== [ login.microsoft.com ]
name: login.microsoft.com
== [ login.microsoftonline.com ]
```

```
name: login.microsoftonline.com
== [ login.windows.net ]
name: login.windows.net
== [ none ]
name: none
== [ wildcard.dropbox.com ]
name: wildcard.dropbox.com
== [ wildcard.google.com ]
name: wildcard.google.com
```

For available options, see [config on page 17](#).

show

The show command displays the specified system configuration.

The syntax and options for show are the same as config.

For example, show firewall address displays a result similar to the following:

```
config firewall address
  edit "FABRIC_DEVICE"
    set comment "IPv4 addresses of Fabric Devices."
  next
  edit "all"
  next
  edit "login.microsoft.com"
    set type fqdn
    set fqdn "login.microsoft.com"
  next
  edit "login.microsoftonline.com"
    set type fqdn
    set fqdn "login.microsoftonline.com"
  next
  edit "login.windows.net"
    set type fqdn
    set fqdn "login.windows.net"
  next
  edit "none"
    set subnet 0.0.0.0 255.255.255.255
  next
  edit "wildcard.dropbox.com"
    set type fqdn
    set fqdn "*.dropbox.com"
  next
  edit "wildcard.google.com"
    set type fqdn
    set fqdn "*.google.com"
  next
end
```

For available options, see [config on page 17](#).

sysctl sh

Enter the Linux shell.

Container FortiOS allows access the Linux shell.

```
sysctl sh
```

To return to or start the Container FortiOSshell, enter `/bin/cli` at the shell prompt.



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.