Palo Alto Networks

PAN-OS® Command Line Interface (CLI) Reference Guide
Version 6.1

Contact Information

Corporate Headquarters:
Palo Alto Networks
4401 Great America Parkway
Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-us

About this Guide

This guide provides information about using the command line interface (CLI) on your Palo Alto Networks next-generation firewall or Panorama appliance. For additional information, refer to the following resources:

- For information on the additional capabilities and for instructions on configuring the features on the firewall, refer to https://www.paloaltonetworks.com/documentation.
- For access to the knowledge base, discussion forums, and videos, refer to https://live.paloaltonetworks.com.
- For contacting support, for information on the support programs, or to manage your account or devices, refer to https://support.paloaltonetworks.com.
- For the latest release notes, go to the software downloads page at https://support.paloaltonetworks.com/Updates/SoftwareUpdates.

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: June 9, 2016

Table of Contents

Chapter 1

Chapter 2

Chapter 3

Chapter 5

Chapter 1
Introduction

This chapter introduces and describes how to use the PAN-OS command line interface (CLI):

- "Understanding the PAN-OS CLI Structure" in the next section
- "Getting Started" on page 14
- "Understanding the PAN-OS CLI Commands" on page 15

Understanding the PAN-OS CLI Structure

The PAN-OS CLI allows you to access the firewall, view status and configuration information, and modify the configuration. Access to the PAN-OS CLI is provided through SSH, Telnet, or direct console access.

The PAN-OS CLI operates in two modes:

- **Operational mode**—View the state of the system, navigate the PAN-OS CLI, and enter configuration mode.
- **Configuration mode**—View and modify the configuration hierarchy.

Chapter 2 describes each mode in detail.

Getting Started

This section describes how to access and begin using the PAN-OS CLI:

- “Before You Begin” in the next section
- “Accessing the PAN-OS CLI” on page 14

Before You Begin

Verify that the firewall is installed and that a SSH, Telnet, or direct console connection is established.

> ***Note:*** *Refer to the Hardware Reference Guide for hardware installation information and to the Quick Start included with the device for information on initial device configuration.*

Use the following settings for direct console connection:

- Data rate: 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: None

Accessing the PAN-OS CLI

To access the PAN-OS CLI:

1. Open the console connection.
2. Enter the administrative user name. The default is *admin*.
3. Enter the administrative password. The default is *admin*.
4. The PAN-OS CLI opens in Operational mode, and the CLI prompt is displayed:

```
username@hostname>
```

Understanding the PAN-OS CLI Commands

This section describes how to use the PAN-OS CLI commands and display command options:

- “Understanding the PAN-OS CLI Command Conventions” in the next section
- “Understanding Command Messages” on page 16
- “Using Operational and Configuration Modes” on page 17
- “Displaying the PAN-OS CLI Command Options” on page 17
- “Using Keyboard Shortcuts” on page 18
- “Understanding Command Option Symbols” on page 19
- “Understanding Privilege Levels” on page 21
- “Referring to Device Interfaces” on page 21

Understanding the PAN-OS CLI Command Conventions

The basic command prompt incorporates the user name and model of the firewall:

```
username@hostname>
```

Example:

```
username@hostname>
```

When you enter Configuration mode, the prompt changes from > to #:

```
username@hostname>                (Operational mode)
username@hostname> configure
Entering configuration mode
[edit]
username@hostname#            (Configuration mode)
```

In Configuration mode, the current hierarchy context is shown by the [edit...] banner presented in square brackets when a command is issued. Refer to “Using the Edit Command” on page 29 for additional information on the **edit** command.

Understanding Command Messages

Messages may be displayed when you issue a command. The messages provide context information and can help in correcting invalid commands. In the following examples, the message is shown in bold.

Example: Unknown command

```
username@hostname# application-group
Unknown command: application-group
[edit network]
username@hostname#
```

Example: Changing modes

```
username@hostname# exit
Exiting configuration mode

username@hostname>
```

Example: Invalid syntax

```
username@hostname> debug 17
Unrecognized command
Invalid syntax.
username@hostname>
```

Each time you enter a command the syntax is checked. If the syntax is correct, the command is executed, and the candidate hierarchy changes are recorded. If the syntax is incorrect, an invalid syntax message is presented, as in the following example:

```
username@hostname# set zone application 1.1.2.2
Unrecognized command
Invalid syntax.
[edit]
username@hostname#
```

Using Operational and Configuration Modes

When you log in, the PAN-OS CLI opens in Operational mode. You can move between Operational and Configuration modes at any time.

- To enter Configuration mode from Operational mode, use the **configure** command:

```
username@hostname> configure
Entering configuration mode

[edit]
username@hostname#
```

- To leave Configuration mode and return to Operational mode, use the **quit** or **exit** command:

```
username@hostname# quit
Exiting configuration mode

username@hostname>
```

- To enter an Operational mode command while in Configuration mode, use the **run** command, as described in “run” on page 50.

- To direct an Operational mode command to a particular VSYS, specify the target VSYS with the following command:

```
username@hostname# set system setting target-vsys <vsys_name>
```

Displaying the PAN-OS CLI Command Options

Use ? (or **Meta-H**) to display a list of command option, based on context:

- To display a list of operational commands, enter **?** at the command prompt.

```
username@hostname> ?
  clear       Clear runtime parameters
  configure   Manipulate software configuration information
  debug       Debug and diagnose
  exit        Exit this session
  grep        Searches file for lines containing a pattern match
  less        Examine debug file content
  ping        Ping hosts and networks
  quit        Exit this session
  request     Make system-level requests
  scp         Use ssh to copy file to another host
  set         Set operational parameters
  show        Show operational parameters
  ssh         Start a secure shell to another host
  tail        Print the last 10 lines of debug file content
username@hostname>
```

- To display the available options for a specified command, enter the command followed by **?**.

  Example:

```
@localhost> ping ?
username@hostname> ping
+ bypass-routing   Bypass routing table, use specified interface
+ count           Number of requests to send (1..2000000000 packets)
+ do-not-fragment  Don't fragment echo request packets (IPv4)
+ inet             Force to IPv4 destination
+ interface         Source interface (multicast, all-ones, unrouted
packets)
+ interval         Delay between requests (seconds)
+ no-resolve       Don't attempt to print addresses symbolically
+ pattern          Hexadecimal fill pattern
+ record-route     Record and report packet's path (IPv4)
+ size            Size of request packets (0..65468 bytes)
+ source           Source address of echo request
+ tos             IP type-of-service value (0..255)
+ ttl               IP time-to-live value (IPv6 hop-limit value) (0..255
hops)
+ verbose          Display detailed output
+ wait            Delay after sending last packet (seconds)
  <host>          Hostname or IP address of remote host
username@hostname> ping
```

Using Keyboard Shortcuts

The PAN-OS CLI supports a variety of keyboard shortcuts. For a complete list, refer to Appendix A, “PAN-OS CLI Keyboard Shortcuts”.

> ***Note:*** *Some shortcuts depend upon the SSH client that is used to access the PAN-OS CLI. For some clients, the* ***Meta*** *key is the* ***Control*** *key; for some it is the* ***Esc*** *key.*

Understanding Command Option Symbols

The symbol preceding an option can provide additional information about command syntax, as described in Table 1.

Table 1. Option Symbols

Symbol	Description
*	This option is required.
>	There are additional nested options for this command.
+	There are additional command options for this command at this level.
|	There is an option to specify an “except value” or a “match value” to restrict the command.

The following example shows how these symbols are used.

Example: In the following command, the keyword from is required:

```
username@hostname> scp import configuration ?
+ remote-port   SSH port number on remote host
* from          Source (username@host:path)
username@hostname> scp import configuration
```

Example: This command output shows options designated with + and >.

```
username@hostname# set rulebase security rules rule1 ?
+ action               action
+ application          application
+ destination          destination
+ disabled             disabled
+ from                 from
+ log-end              log-end
+ log-setting          log-setting
+ log-start            log-start
+ negate-destination   negate-destination
+ negate-source        negate-source
+ schedule             schedule
+ service              service
+ source               source
+ to                   to
> profiles             profiles
  <Enter>              Finish input
[edit]
username@hostname# set rulebase security rules rule1
```

Each option listed with + can be added to the command.

The profiles keyword (with >) has additional options:

```
username@hostname# set rulebase security rules rule1 profiles ?
+ virus           Help string for virus
+ spyware         Help string for spyware
+ vulnerability   Help string for vulnerability
+ group           Help string for group
  <Enter>         Finish input
[edit]
username@hostname# set rulebase security rules rule1 profiles
```

Restricting Command Output

Some operational commands include an option to restrict the displayed output. To restrict the output, enter a pipe symbol followed by **except** or **match** and the value that is to be excluded or included:

Example:
The following sample output is for the **show system info** command:

```
username@hostname> show system info

hostname: PA-HDF
ip-address: 10.1.7.10
netmask: 255.255.0.0
default-gateway: 10.1.0.1
mac-address: 00:15:E9:2E:34:33
time: Fri Aug 17 13:51:49 2007

uptime: 0 days, 23:19:23
devicename: PA-HDF
family: i386
model: pa-4050
serial: unknown
sw-version: 1.5.0.0-519
app-version: 25-150
threat-version: 0
url-filtering-version: 0
logdb-version: 1.0.8

username@hostname>
```

The following sample displays only the system model information:

```
username@hostname> show system info | match model
model: pa-4050

username@hostname>
```

Understanding Privilege Levels

Privilege levels determine which commands the user is permitted to execute and the information the user is permitted to view. Table 2 describes the PAN-OS CLI privilege levels.

Table 2. Privilege Levels

Level	Description
superuser	Has full access to the firewall and can define new administrator accounts and virtual systems.
superreader	Has complete read-only access to the firewall.
vsys	Has full access to a selected virtual system on the firewall.
vsysreader	Has read-only access to a selected virtual system on the firewall.
device	Has full access to a selected device, except for defining new accounts or virtual systems.
devicereader	Has read-only access to a selected device.

Referring to Device Interfaces

The Ethernet interfaces are numbered from left to right and top to bottom on the firewall, as shown in Figure 1. In most of the firewall models, there is a single set of interfaces, and the numbering is of the form ethernet1/<port>.

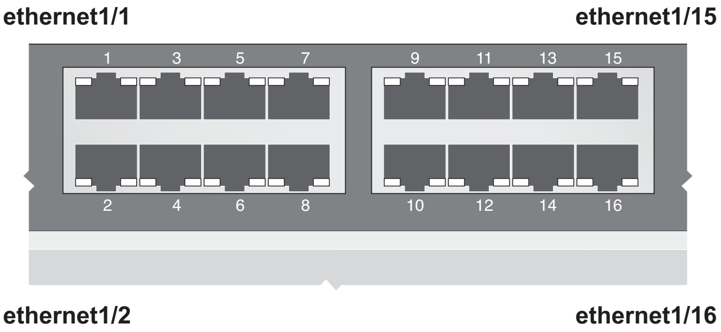


Figure 1. Firewall Ethernet Interfaces

Use these names when referring to the Ethernet interfaces within the PAN-OS CLI commands, as in the following example:

```
username@hostname# set network interface ethernet ethernet1/4 virtual-wire
```

Chapter 2
Understanding CLI Command Modes

This chapter describes the modes used to interact with the PAN-OS CLI:

- “Understanding Configuration Mode” in the next section
- “Understanding Operational Mode” on page 30

Understanding Configuration Mode

When you enter Configuration mode and enter commands to configure the firewall, you are modifying the candidate configuration. The modified candidate configuration is stored in firewall memory and maintained while the firewall is running.

Each configuration command involves an action, and may also include keywords, options, and values. Entering a command makes changes to the candidate configuration.

This section describes Configuration mode and the configuration hierarchy:

- “Using Configuration Mode Commands” in the next section
- “Using Configuration Commands with Virtual Systems” on page 25
- “Understanding the Configuration Hierarchy” on page 26
- “Navigating Through the Hierarchy” on page 28

Using Configuration Mode Commands

Use the following commands to store and apply configuration changes (see Figure 1):

- **save** command—Saves the candidate configuration in firewall non-volatile storage. The saved configuration is retained until overwritten by subsequent **save** commands. Note that this command does not make the configuration active.
- **commit** command—Applies the candidate configuration to the firewall. A committed configuration becomes the active configuration for the device.

- **set** command—Changes a value in the candidate configuration.
- **load** command—Assigns the last saved configuration or a specified configuration to be the candidate configuration.

Example: Make and save a configuration change.

```
username@hostname# rename zone untrust to untrust1 (enter a configuration command)
[edit]
username@hostname# save config to snapshot.xml
Config saved to .snapshot.xml
[edit]
username@hostname#
```

Example: Make a change to the candidate configuration.

```
[edit]
username@hostname# set network interface vlan ip 1.1.1.4/24
[edit]
username@hostname#
```

Example: Make the candidate configuration active on the device.

```
[edit]
username@hostname# commit
[edit]
username@hostname#
```

> ***Note:*** *If you exit Configuration mode without issuing the* ***save*** *or* ***commit*** *command, your configuration changes could be lost if power is lost to the firewall.*

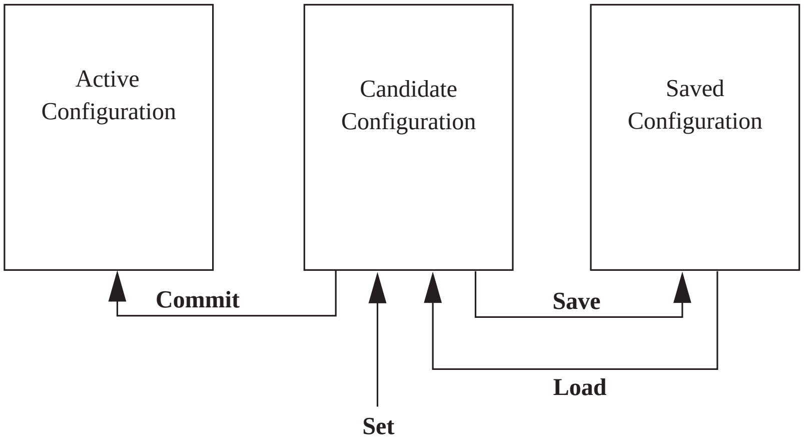


Figure 1. Configuration Mode Command Relationship

Maintaining a candidate configuration and separating the save and commit steps confers important advantages when compared with traditional CLI architectures:

- Distinguishing between the **save** and **commit** concepts allows multiple changes to be made at the same time and reduces system vulnerability.

  For example, if you want to remove an existing security policy and add a new one, using a traditional CLI command structure would leave the system vulnerable for the period of time between removal of the existing security policy and addition of the new one. With the PAN-OS approach, you configure the new security policy before the existing policy is removed, and then implement the new policy without leaving a window of vulnerability.

- You can easily adapt commands for similar functions.

  For example, if you are configuring two Ethernet interfaces, each with a different IP address, you can edit the configuration for the first interface, copy the command, modify only the interface and IP address, and then apply the change to the second interface.

- The command structure is always consistent.

  Because the candidate configuration is always unique, all the authorized changes to the candidate configuration will be consistent with each other.

Using Configuration Commands with Virtual Systems

If multiple virtual systems are enabled, you must specify a virtual system as part of the **set** command in order to see the available options, as in the following example.

```
username@hostname> configure
Entering configuration mode
[edit]
[edit]
username@hostname# set ?
> deviceconfig   deviceconfig
> mgt-config     mgt-config
> network        network configuration
> shared         shared
> vsys           vsys
[edit]
username@hostname# set vsys vsys1 ?
+ display-name              alphanumeric string [ 0-9a-zA-Z._-]
> address                   address
> address-group             address-group
> application               application
> application-filter        application-filter
> application-group         application-group
> authentication-profile    authentication-profile
> authentication-sequence   authentication-sequence
> captive-portal            captive-portal
> certificate               certificate
> certificate-profile       certificate-profile
> email-scheduler           email-scheduler
> external-list             external-list
> global-protect            GlobalProtect
> group-mapping             group-mapping
> import                    Import predefined configured resources
> local-user-database       local-user-database
> log-settings              log-settings
> ocsp-responder            ocsp-responder
> pdf-summary-report        pdf-summary-report
> profile-group             profile-group
> profiles                  profiles
> region                    region
> report-group              report-group
> reports                   reports
> response-page             response-page
> rulebase                  rulebase
> schedule                  schedule
> server-profile            server-profile
> service                   service
> service-group             service-group
> setting                   setting
> ssl-decrypt               ssl-decrypt
> threats                   threats
> ts-agent                  ts-agent
> url--override        url--override
> url-content-types         url-content-types
> user-id-agent             user-id-agent
> user-id-agent-sequence    user-id-agent-sequence
> user-id-collector         user-id-collector
> zone                      zone
<Enter>                           Finish input
```

Understanding the Configuration Hierarchy

The configuration for the firewall is organized in a hierarchical structure. To display a segment of the current hierarchy, use the **show** command. Entering **show** displays the complete hierarchy, while entering **show** with keywords displays a segment of the hierarchy.

For example, the following command displays the configuration hierarchy for the Ethernet interface segment of the hierarchy:

```
username@hostname# show network interface ethernet
ethernet {
  ethernet1/1 {
    virtual-wire;
  }
  ethernet1/2 {
    virtual-wire;
  }
  ethernet1/3 {
    layer2 {
      units {
        ethernet1/3.1;
      }
    }
  }
  ethernet1/4;
}
[edit]
username@hostname#
```

Understanding Hierarchy Paths

When you enter a command, path is traced through the hierarchy, as shown in Figure 2.

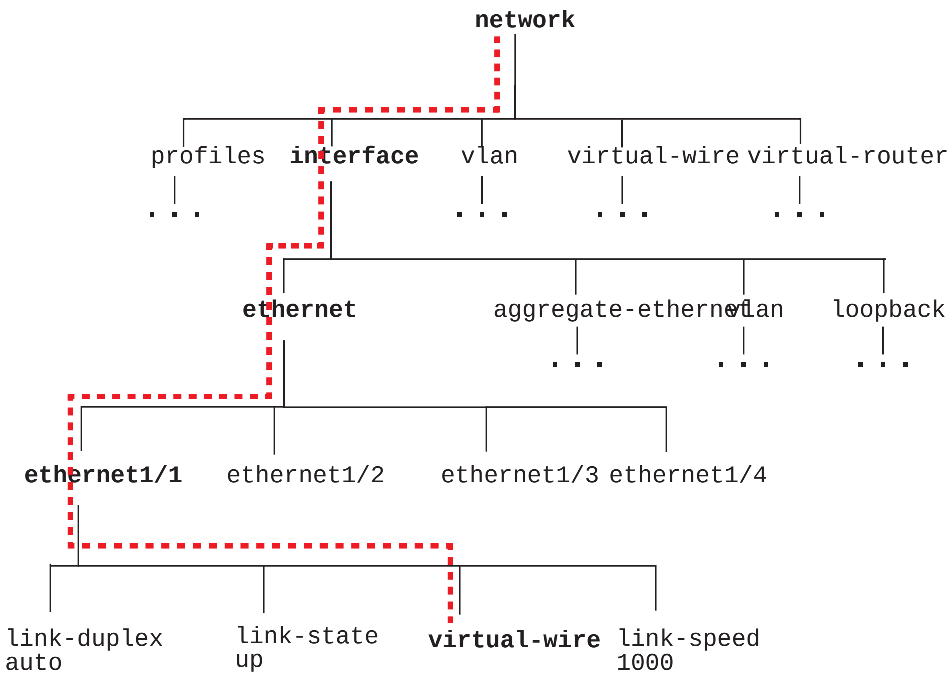


Figure 2. Sample Hierarchy Segment

For example, the following command assigns the IP address/netmask 10.1.1.12/24 to the Layer 3 interface for the Ethernet port ethernet1/4:

```
[edit]
username@hostname# set network interface ethernet ethernet1/4 layer3 ip
10.1.1.12/24

[edit]
username@hostname#
```

This command generates a new element in the hierarchy, as shown in Figure 3 and in the output of the following **show** command:

```
[edit]
username@hostname# show network interface ethernet ethernet1/4
ethernet1/4 {
    layer3 {
      ip {
        10.1.1.12/24;
      }
    }
  }
[edit]
username@hostname#
```

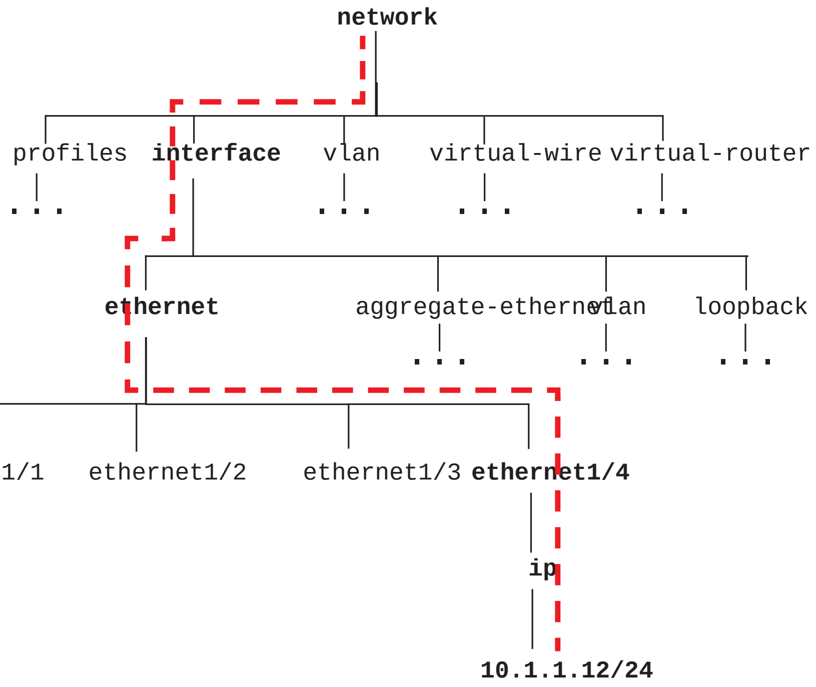


Figure 3. Sample Hierarchy Segment

Navigating Through the Hierarchy

The [edit...] banner presented below the Configure mode command prompt line shows the current hierarchy context. For example, the banner

```
[edit]
```

indicates that the relative context is the top level of the hierarchy, whereas

```
[edit network profiles]
```

indicates that the relative context is at the network profiles node.

Use the commands listed in Table 1 to navigate through the configuration hierarchy.

Table 1. Navigation Commands

Command	Description
edit	Sets the context for configuration within the command hierarchy.
up	Changes the context to the next higher level in the hierarchy.
top	Changes the context to the highest level in the hierarchy.

Using the Edit Command

Use the **edit** command to change context to lower levels of the hierarchy, as in the following examples:

- Move from the top level to a lower level:

```
[edit]  (top level)
username@hostname# edit network
[edit network]
username@hostname#  (now at the network level)

[edit network]
```

- Move from one level to a lower level:

```
[edit network]  (network level)
username@hostname# edit interface

[edit network interface]
@abce#  (now at the network interface level)
```

Using the Up and Top Commands

Use the up and top commands to move to higher levels in the hierarchy:

- **up**—changes the context to one level up in the hierarchy.

  Example:

```
[edit network interface]  (network level)
@abce# up

[edit network]
username@hostname#  (now at the network level)
```

- **top**—changes context to the top level of the hierarchy.

  Example:

```
[edit network interface vlan]  (network vlan level)
username@hostname# top

[edit]
username@hostname#  (now at network vlan level)
```

> ***Note:*** *The **set** command issued after using the **up** and **top** commands starts from the new context.*

Understanding Operational Mode

When you first log in, the PAN-OS CLI opens in Operational mode. Operational mode commands involve actions that are executed immediately. They do not involve changes to the configuration, and do not need to be saved or committed.

Operational mode commands are of several types:

- **Network access**—Open a window to another host. SSH is supported.
- **Monitoring and troubleshooting**—Perform diagnosis and analysis. Includes **debug** and **ping** commands.
- **Display commands**—Display or clear current information. Includes **clear** and **show** commands.
- **PAN-OS CLI navigation commands**—Enter Configure mode or exit the PAN-OS CLI. Includes **configure**, **exit**, and **quit** commands.
- **System commands**—Make system-level requests or restart. Includes **set** and **request** commands.

Setting the Output Format for Configuration Commands

You can specify the output format for configuration commands by using the **set cli config-output-format** command in Operational mode. Options include the default format, XML format, and **set** command format.

The following examples show the difference in output for each of these options. For information on setting these options, refer to “set cli” on page 445.

Default option:

```
username@hostname# show system log-export-schedule
log-export-schedule {
  10.16.0.97 {
    description 10.16.0.97;
    enable yes;
    log-type threat;
    start-time 03:00;
    protocol {
      ftp {
        hostname 10.16.0.97;
        port 21;
        passive-mode yes;
        username ;
        password mZDB7rbW5y8=;
      }
}
username@hostname#
```

XML option:

```
username@hostname# show system log-export-schedule
<log-export-schedule>
  <entry name="10.16.0.97">
    <description>10.16.0.97</description>
    <enable>yes</enable>
    <log-type>threat</log-type>
    <start-time>03:00</start-time>
    <protocol>
      <ftp>
        <hostname>10.16.0.97</hostname>
        <port>21</port>
        <passive-mode>yes</passive-mode>
        <username></username>
        <password>mZDB7rbW5y8=</password>
      </ftp>
    </protocol>
  </entry>
</log-export-schedule>
[edit deviceconfig]
[edit deviceconfig]
username@hostname#
```

set command option:

```
username@hostname# show system log-export-schedule
set deviceconfig system log-export-schedule 10.16.0.97 description 10.16.0.97
set deviceconfig system log-export-schedule 10.16.0.97 enable yes
set deviceconfig system log-export-schedule 10.16.0.97 log-type threat
set deviceconfig system log-export-schedule 10.16.0.97 start-time 03:00
set deviceconfig system log-export-schedule 10.16.0.97 protocol ftp hostname
username@hostname#
```

Chapter 3

Configuration Mode Commands

This chapter contains command reference pages for the following Configuration mode commands:

- “set deviceconfig high-availability” on page 63
- “set deviceconfig setting” on page 71
- “set deviceconfig system” on page 82
- “set display-name” on page 92
- “set email-scheduler” on page 93
- “set external-list” on page 94
- “set global-protect” on page 95
- “set group-mapping” on page 101
- “set log-collector” on page 102
- “set log-collector-group” on page 105
- “set mgt-config” on page 113
- “set network dhcp” on page 116
- “set network dns-proxy” on page 118
- “set network ike” on page 120
- “set network interface” on page 124
- “set network profiles” on page 138
- “set network qos” on page 144
- “set network shared-gateway” on page 146
- “set network tunnel” on page 155
- “set network virtual-router” on page 161
- “set network virtual-router multicast” on page 163
- “set network virtual-router protocol bgp” on page 166
- “set network virtual-router protocol ospf” on page 178
- “set network virtual-router protocol ospfv3” on page 182
- “set network virtual-router protocol redist-profile” on page 186
- “set network virtual-router protocol rip” on page 189
- “set network virtual-wire” on page 191
- “set network vlan” on page 192
- “set ocsp-responder” on page 193
- “set panorama” on page 194
- “set pdf-summary-report” on page 195

- “set profile-group” on page 196
- “set profiles” on page 197
- “set region” on page 213
- “set report-group” on page 214
- “set reports” on page 215
- “set rulebase or set vsys rulebase” on page 220
- “set schedule” on page 231
- “set service” on page 232
- “set service-group” on page 233
- “set setting” on page 234
- “set shared admin-role” on page 235
- “set shared alg-override” on page 248
- “set shared authentication-profile” on page 249
- “set shared authentication-sequence” on page 251
- “set shared botnet” on page 252
- “set shared certificate” on page 254
- “set shared certificate-profile” on page 255
- “set shared email-scheduler” on page 256
- “set shared local-user-database” on page 257
- “set shared log-settings” on page 258
- “set shared override” on page 263
- “set shared pdf-summary-report” on page 264
- “set shared post-rulebase” on page 265
- “set shared pre-rulebase” on page 266
- “set shared report-group” on page 267
- “set shared reports” on page 268
- “set shared response-page” on page 273
- “set shared server-profile” on page 274
- “set shared ssl-decrypt” on page 276
- “set template” on page 277
- “set threats” on page 278

- “set ts-agent” on page 282
- “set url-admin-override” on page 283
- “set url-content-types” on page 284
- “set user-id-agent” on page 285
- “set user-id-agent-sequence” on page 286
- “set user-id-collector” on page 287
- “set vsys application” on page 290
- “set vsys import” on page 291
- “set zone” on page 293
- “show” on page 294
- “show deviceconfig setting ssl-decrypt” on page 295
- “top” on page 296
- “top” on page 296
- “up” on page 297

Changes in the configuration are retained, until overwritten, while the firewall is powered. To save a candidate configuration in non-volatile storage, use the ***save*** *command. To make a candidate configuration active, use the* ***commit*** *command.*

check

Displays the current configuration status.

Syntax

```
check
   {
   data-access-passwd {system} |
   pending-changes
   }
```

Options

> data-access-passwd — Check data access authentication status for this session
   + system — Check whether data access password exists for the system
> pending-changes — Check for uncommitted changes

Sample Output

The following command shows that there are currently no uncommitted changes.

```
username@hostname# check pending-changes
no
[edit]
username@hostname#
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

commit

Makes the current candidate configuration the active configuration on the firewall.

> *When you change a configuration setting, the current "candidate" configuration is updated, not the active configuration. The* ***commit*** *command applies the candidate configuration to the active configuration, which activates all configuration changes since the last commit.*

Syntax

```
commit {force}
   {
   partial device-and-network excluded |
   partial policy-and-objects excluded |
   partial vsys <value> |
   partial no-vsys
   }
```

Options

> force — Forces the commit command in the event of a conflict
> partial — Commits the specified part of the configuration
   + device-and-network — Excludes device and network configurations from the commit (configurations under config/mgt-config, config/devices/platform, config/devices/deviceconfig, and config/devices/network)
   + policy-and-object — Excludes policy and object configurations from the commit (configurations under (config/shared; also excludes config/devices/vsys if in single vsys mode)
   + vsys — Commits only the specified virtual system configurations
   > no-vsys — Excludes all virtual systems from the commit (configurations under config/devices/vsys)

Sample Output

The following command updates the active configuration with the contents of the candidate configuration.

```
username@hostname# commit
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

copy

Makes a copy of a node in the hierarchy along with its children, and adds the copy to the same hierarchy level.

Syntax

```
copy <node1> to <node2>
```

Options

<node1> — Specifies the node to be copied
<node2> — Specifies the name of the copy

Sample Output

The following command, executed from the rule base security level of the hierarchy, makes a copy of **`rule1`**, called **`rule2`**.

```
[edit rulebase security]
username@hostname# copy rules rule1 to rule2
[edit rulebase security]
username@hostname#
```

The following command shows the location of the new rule in the hierarchy.

```
[edit rulebase security]
username@hostname# show

security {
  rules {
    rule1 {
      source [ any 1.1.1.1/32 ];
      destination 1.1.1.2/32;
    }

    rule2 {
      source [ any 1.1.1.1/32 ];
      destination 1.1.1.2/32;
    }
  }
}
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

delete

Removes a node from the candidate configuration along with all its children.

No confirmation is requested when this command is entered.

Syntax

```
delete <node>
```

Options

<node> — Specifies the node to be deleted. For available nodes of the hierarchy, press <tab>.

Sample Output

The following command deletes the application **myapp** from the candidate configuration.

```
username@hostname# delete application myapp
[edit]
   username@hostname#
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

edit

Changes context to a lower level in the configuration hierarchy.

Syntax

```
edit <context>
```

Options

<context> — Specifies a path through the hierarchy. For available contexts in the hierarchy, press <tab>.

Sample Output

The following command changes context from the top level to the **`network profiles`** level of the hierarchy.

```
[edit]
   username@hostname# edit rulebase

[edit rulebase]
   username@hostname#
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

exit

Exits from the current PAN-OS CLI level.

- From Operational mode — Exits the PAN-OS CLI.
- From Configuration mode, top hierarchy level — Exits Configuration mode, returning to Operational mode.
- From Configuration mode, lower hierarchy levels — Changes context to one level up in the hierarchy. Provides the same result as the **up** command.

*The **exit** command is the same as the **quit** command.*

Syntax

```
exit
```

Options

None

Sample Output

The following command changes context from the network interface level to the network level.

```
[edit network interface]
username@hostname# exit
[edit network]
username@hostname#
```

The following command changes from Configuration mode to Operational mode.

```
[edit]
    username@hostname# exit
Exiting configuration mode

username@hostname>
```

Required Privilege Level

All

find

Lists CLI commands containing the specified keyword.

Syntax

```
find command keyword <value>
```

Options

<value> — Specifies a keyword.

Sample Output

The following command lists all CLI commands containing the keyword hsm.

```
username@hostname# find command keyword hsm
set profiles decryption <name> ssl-inbound-proxy block-if-hsm-unavailable <yes|no>
set profiles decryption <name> ssl-forward-proxy block-if-hsm-unavailable <yes|no>
username@hostname#
```

Required Privilege Level

All

load

Assigns the last saved configuration, or a specified configuration, to be the candidate configuration. Also, loads the last imported device state files.

Syntax

```
load
   {
   config |
     {
     key <value> |
     from <filename> |
     last-saved |
     partial |
        {
        from <filename> |
        from-xpath <value> |
        mode {merge | replace} |
        to-xpath <value>
        }
     repo device <value> {file <value> | version <value>} |
     version <value>
     }
   device-state
   }
```

Options

> config — Loads specified configuration
   + key — Key used for encryption
   > from — File name (select from the file names provided, or enter a new name)
   > last-saved — Loads the last saved configuration
   > partial — Loads partial configuration
      * from — File name (select from the file names provided, or enter a new name)
      * from-xpath — XML Path (XPath) of the source node
      * mode — Mode in which to load (merge or replace)
      * to-xpath — XML Path (XPath) of the destination's parent
   > repo — Loads device config from backup repository
      * device — Device name
      > file — Filename
      > version — Version
   > version — Selects from the provided versions
> device-state — Loads from imported device state files to GlobalProtect Portals.

Sample Output

The following command assigns **`output.xml`** to be the candidate configuration.

```
[edit]
   username@hostname# load config from output.xml

command succeeded

[edit]
   username@hostname#
```

The following command adds the “top-apps” report found in the x.xml configuration to the specified candidate configuration.

```
[edit]
   username@hostname# load config partial from x.xml from-xpath shared/reports/
   entry[@name='top-apps'] mode merge to-xpath/config/devices/
   entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/reports

command succeeded

[edit]
   username@hostname#
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

move

Relocates a node in the hierarchy along with its children to be at another location at the same hierarchy level.

Syntax

```
move <element1> {bottom | top | after <element2> | before <element2>}
```

Options

<element1> — Specifies the items to be moved. For available elements of the hierarchy, press <tab>.
<element2> — Indicates the element after or before which *element1* will be placed
after — Moves element to be after *element2*
before — Moves element to be before *element2*
bottom — Makes the element the last entry of the hierarchy level
top — Makes the element the first entry of the hierarchy level

Sample Output

The following command moves the security rule **rule1** to the top of the rule base.

```
username@hostname# move rulebase security rules rule1 top

[edit]
   username@hostname#
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

override

Overrides a node from the candidate configuration along with all its children. This is a device command that overrides a value pushed from a Panorama Template.

No confirmation is requested when this command is entered.

Syntax

```
override <node>
```

Options

<node> — Specifies the node to override. For available nodes of the hierarchy, press <tab>.

Sample Output

The following command overrides the group mapping **mygroup** from the candidate configuration.

```
username@hostname# override group-mapping mygroup
[edit]
   username@hostname#
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

quit

Exits from the current PAN-OS CLI level.

- From Operational mode — Exits the PAN-OS CLI.
- From Configuration mode, top hierarchy level — Exits Configuration mode, returning to Operational mode.
- From Configuration mode, lower hierarchy levels — Changes context to one level up in the hierarchy. Provides the same result as the **up** command.

*The **exit** and **quit** commands are interchangeable.*

Syntax

```
quit
```

Options

None

Sample Output

The following command changes context from the network interface level to the network level.

```
[edit log-settings]
username@hostname# quit

[edit]
username@hostname#
```

The following command changes from Configuration mode to Operational mode.

```
[edit]
    username@hostname# quit
Exiting configuration mode

username@hostname>
```

Required Privilege Level

All

rename

Changes the name of a node in the hierarchy.

Syntax

```
rename <node1> to <node2>
```

Options

<node1> — Indicates the original node name. For available nodes of the hierarchy, press <tab>.
<node2> — Indicates the new node name

Sample Output

The following command changes the name of a node in the hierarchy from **1.1.1.1/24** to **1.1.1.2/24**.

```
username@hostname# rename network interface vlan ip 1.1.1.1/24 to 1.1.1.2/24
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

run

Executes an Operational mode command while in Configuration mode.

For information about the syntax and options for each Operational mode command, refer to its command page in Chapter 4, “Operational Mode Commands”.

Syntax

```
run
   {
   check |
   clear |
   commit |
   commit-all |
   debug |
   delete |
   diff-all |
   ftp |
   grep |
   less |
   load |
   ls |
   netstat |
   ping |
   request |
   save |
   schedule |
   scp |
   set |
   show |
   ssh |
   tail |
   target |
   tcpdump |
   test |
   tftp |
   traceroute |
   view-pcap
   }
```

Sample Output

The following command executes a **ping** command to the IP address **`1.1.1.2`** from Configuration mode.

```
username@hostname# run ping host 1.1.1.2
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
...
username@hostname#
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

save

Saves a snapshot of the firewall configuration or the device state files from a GlobalProtect Portal.

> *This command saves the configuration on the firewall, but does not make the configuration active. Use the **commit** command to make the current candidate configuration active.*

Syntax

```
save
    {
    config to <filename> |
    device-state
    }
```

Options

> config — Saves the current configuration
    + to — File name (select from the file names provided, or enter a new name)
> device-state — Saves all files needed to restore a GlobalProtect Portal. This command is used to save the configuration and dynamic information from a firewall that is configured as a GlobalProtect Portal with the large scale VPN feature enabled. The file can then be imported to restore the Portal in the event of a failure. The export contains a list of all satellite devices managed by the Portal, the running configuration at the time of the export, and all certificate information (Root CA, Server, and Satellite certificates).

Sample Output

The following command saves a copy of the configuration to the file **`savefile`**.

```
[edit]
username@hostname# save config to savefile
Config saved to savefile

[edit]
    username@hostname#
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set address

Specifies addresses and address ranges for use in security policies. Addresses requiring the same security settings can be combined into address groups that you can refer to as a unit.

For information on configuring address groups using the CLI, refer to “set address-group” on page 53.

Syntax

```
set address <name> |
   {
   description <value> |
   fqdn <value> |
   ip-netmask <ip/netmask> |
   ip-range <ip_range>
   tag <value>
   }
```

Options

<name> — Select from the local server list or enter a name for the address (up to 63 characters)
+ description — Address description value
> fqdn — Fully Qualified Domain Name (FQDN) value
> ip-netmask — IP address and network mask (x.x.x.x/y or IPv6/netmask)
> ip-range — IP address range (x.x.x.x-y.y.y.y or IPv6-range)
> tag — Tags for address object (Select values from the local server list, or enter a name or group of names enclosed in [ ])

Required Privilege Level

superuser, vsysadmin, deviceadmin

set address-group

Configures sets of addresses that will be assigned the same security settings, to simplify the creation of security policies.

For information on configuring address groups using the CLI, refer to “set address” on page 52.

Syntax

```
set address-group <name> |
   {
   description <value> |
   dynamic {filter <value>} <value> |
   static <list of values> |
   tag <list of values>
}
```

Options

<name> — Select from the local server list or enter a name for the address group (up to 63 characters)
+ description — Address group description
> dynamic — Dynamic addressing
> static — static addressing
> tag — Tags for address object (Select values from the local server list, or enter a name or group of names enclosed in [ ])

Required Privilege Level

superuser, vsysadmin, deviceadmin

set application

Creates a custom App-ID for use throughout PAN-OS wherever an application can be specified.

Syntax

```
set application <name> |
   {
   able-to-transfer-file {no | yes} |
   alg-disable-capability <value> |
   category {business-systems | collaboration | general-internet | media | networking |
     <value>} |
   consume-big-bandwidth {no | yes} |
   data-ident {no | yes} |
   description <value> |
   evasive-behavior {no | yes} |
   file-type-ident {no | yes} |
   has-known-vulnerability {no | yes} |
   parent-app <value> |
   pervasive-use {no | yes} |
   prone-to-misuse {no | yes} |
   risk <value> |
   spyware-ident {no | yes} |
   subcategory <value> |
   tcp-timeout <value> |
   technology {browser-based | client-server | network-protocol | peer-to-peer|
     <value>} |
   timeout <value> |
   tunnel-applications {no | yes} |
   tunnel-other-application {no | yes} |
   udp-timeout <value> |
   used-by-malware {no | yes} |
   virus-ident {no | yes} |
   default |
     {
     ident-by-icmp-type <value> |
     ident-by-icmp6-type <value> |
     ident-by-ip-protocol <value> |
     port <value> |
     }
   signature <name>
     {
     comment <value> |
     order-free {no | yes} |
     scope {protocol-data-unit | session} |
     and-condition <name> {or-condition <name>}
        {
        operator equal-to |
           {
           context {unknown-req-tcp | unknown-req-udp | unknown-rsp-tcp | unknown-rsp-
              udp}
           mask <value> |
           position <value> |
           value <value>
           }
        operator pattern-match
           {
           context <value> |
           pattern <value> |
           qualifier <name> value <value>
           }
        }
     }
  }
```

Options

<name> — Enter a name for the application
+ able-to-transfer-file — Able to transfer files
+ alg-disable-capability — Disable the Application-level Gateway (ALG)
+ category — Category; select from business-systems, collaboration, general-internet, media, networking, or enter a value
+ consume-big-bandwidth — Consumes big bandwidth
+ data-ident — Data identification
+ description — Description value
+ evasive-behavior — Has evasive behavior
+ file-type-ident — File type identification
+ has-known-vulnerability — Has known vulnerability
+ parent-app — Parent application; select from list or enter a value
+ pervasive-use — Pervasively used
+ prone-to-misuse — Prone to misuse
+ risk — Risk value (1-5)
+ spyware-ident — Spyware identification
+ subcategory — Subcategory; select from the list or enter a value
   - business-systems subcategories are auth-service, database, erp-crm, general-business, management, office-programs, software-update, or storage-backup
   - collaboration subcategories are email, instant-messaging, internet-conferencing, social-networking, voip-video, or web-posting
   - general-internet subcategories are file-sharing or internet-utility
   - media subcategories are audio-streaming, gaming, or photo-video
   - networking subcategories are encrypted-tunnel, infrastructure, ip-protocol, proxy, remote-access. or routing
+ tcp-timeout — TCP timeout in seconds (0-604800); setting to 0 applies the default timeout
+ technology — Technology; select from browser-based, client-server, network-protocol, peer-to-peer, or enter a value
+ timeout — Timeout in seconds (0-604800); setting to 0 applies the default timeout
+ tunnel-applications — Tunnel applications
+ tunnel-other-application — Tunnel other applications
+ udp-timeout — UDP timeout in seconds (0-604800); setting to 0 applies the default timeout
+ used-by-malware — Used by malware
+ virus-ident — Virus identification
> default — Default application
   > ident-by-icmp-type — Identification by ICMP type (0-255,...)
   > ident-by-icmp6-type — Identification by ICMP6 type (0-255,...)
   > ident-by-ip-protocol — Identification by IP protocol (0-255,...)
   > port — Protocol port specification : {tcp|udp}/{dynamic|port range list} (e.g. tcp/8080, tcp/80,443, tcp/1-1024,10000, udp/dynamic), or list of values enclosed in [ ]
> signature — Signature application
   + comment — Comment value
   + order-free — Order free (no or yes)
   + scope — Scope (protocol data unit transaction or session)

> and-condition — And-condition name
> or-condition — Or-condition name
> operator — Operator choices
> equal-to — Equal-to choices
+ context — Context (unknown TCP request, unknown UDP request, unknown TCP response, or unknown UDP response)
+ mask — Mask 4-byte hexidecimal value
+ position — Position value
+ value — Value 4-byte hexidecimal value
> pattern-match — Pattern-match choices
+ context — Context (file-html-body, file-office-content, file-pdf-body, ftp-req-params, ftp-rsp-banner, http-req-headers, http-req-host-header, http-req-mime-form-data, http-req-params, http-req-uri-path, http-rsp-headers, imap-req-cmd-line, imap-req-first-param , imap-req-params-after-first-param, rtsp-req-headers, rtsp-req-uri-path, smtp-req-argument, smtp-rsp-content, ssl-req-client-hello, ssl-rsp-certificate, ssl-rsp-server-hello, telnet-req-client-data, telnet-rsp-server-data, or enter a value)
+ pattern — Pattern value
> qualifier — Qualifier name and value (some contexts include available options; press <tab> to view available options)

Sample Output

The following command configures an application that detects web traffic going to a specified website.

```
username@hostname# set application specifiedsite category collaboration subcategory
    social-networking technology browser-based signature s1 and-condition a1 or-
    condition o1 operator pattern-match context http-req-host-header pattern
    www.specifiedsite.com
username@hostname#
```

The following example demonstrates configuring an application that detects blog posting activity on a specified blog.

```
username@hostname# set application specifiedblog_posting category collaboration
    subcategory web-posting technology browser-based signature s1 and-condition a1 or-
    condition o1 operator pattern-match context http-req-host-header pattern
    specifiedblog.com qualifier http-method value POST
username@hostname# set application specifiedblog_posting category collaboration
    subcategory web-posting technology browser-based signature s1 and-condition a2 or-
    condition o2 operator pattern-match context http-req-params pattern post_title
    qualifier http-method value POST
username@hostname# set application specifiedblog_posting category collaboration
    subcategory web-posting technology browser-based signature s1 and-condition a3 or-
    condition o3 operator pattern-match context http-req-params pattern post_author
    qualifier http-method value POST
username@hostname#
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set application-filter

Specifies application filters to simplify repeated searches.

Syntax

```
set application-filter <name>
   {
   category {business-systems | collaboration | general-internet | media | networking |
     unknown | <member_value>} |
   evasive yes |
   excessive-bandwidth-use yes |
   has-known-vulnerabilities yes |
   pervasive yes |
   prone-to-misuse yes |
   risk <value> |
   subcategory <member_value> |
   technology {browser-based | client-server | network-protocol | peer-to-peer|
     <member_value>} |
   transfers-files yes |
   tunnels-other-apps yes |
   used-by-malware yes
   }
```

Options

<name> — Enter a name for the application filter
+ category — Category; select from business systems, collaboration, general internet, media, networking, unknown, or enter a value or list of values enclosed in [ ]
+ evasive — Configure to filter for evasive applications
+ excessive-bandwidth-use — Configure to filter for excessive bandwidth use
+ has-known-vulnerabilities — Configure to filter for applications with known vulnerabilities
+ pervasive — Configure to filter for pervasive applications
+ prone-to-misuse — Configure to filter for applications prone to misuse
+ risk — Risk value (1-5)
+ subcategory — Subcategory; select from the list or enter a value or list of values enclosed in [ ]
  - business-systems subcategories are auth-service, database, erp-crm, general-business, management, office-programs, software-update, or storage-backup
  - collaboration subcategories are email, instant-messaging, internet-conferencing, social-networking, voip-video, or web-posting
  - general-internet subcategories are file-sharing or internet-utility
  - media subcategories are audio-streaming, gaming, or photo-video
  - networking subcategories are encrypted-tunnel, infrastructure, ip-protocol, proxy, remote-access. or routing
  - unknown subcategories include all of the above
+ technology — Technology; select from browser-based, client-server, network-protocol, peer-to-peer, or enter a value or list of values enclosed in [ ]
+ transfers-files — Configure to filter for applications that transfer files
+ tunnels-other-apps — Configure to filter for applications that tunnel other applications
+ used-by-malware — Configure to filter for applications used by malware

Required Privilege Level

superuser, vsysadmin, deviceadmin

set application-group

Specifies a set of applications that require the same security settings, to simplify the creation of security policies.

For information on enabling application settings using the CLI, refer to “set application” on page 54.

Syntax

```
set application-group <name> <member_value>
```

Options

<name> — Enter a name for the application group
<value> — Select from the list of predefined applications, filters, and groups, or enter a value or list of values enclosed in [ ]

Required Privilege Level

superuser, vsysadmin, deviceadmin

set captive-portal

Configures a captive portal on the firewall. You can set up and customize a captive portal to direct user authentication by way of an authentication profile or authentication sequence. Captive portal is used in conjunction with the User-ID Agent to extend user identification functions beyond the Active Directory domain. Users are directed to the portal and authenticated, thereby creating a user-to-IP address mapping

Syntax

```
set captive-portal
   {
   authentication-profile <value> |
   client-certificate-profile <value> |
   enable-captive-portal {no | yes} |
   idle-timer <value> |
   redirect-host {<ip/netmask> | <host_name>} |
   server-certificate <value> |
   timer <value> |
   mode |
     {
     redirect |
        {
        session-cookie
           {
           enable {no | yes} |
           roaming {no | yes} |
           timeout <value>
           }
        }
     transparent
     }
   ntlm-auth
     {
     attempts <value> |
     reversion-time <value> |
     timeout <value>
     }
   }
```

Options

+ authentication-profile — Authentication profile name
+ client-certificate-profile — Profile for authenticating client certificates
+ enable-captive-portal — Enable the captive portal
+ idle-timer — Idle timer in minutes (1-1440)
+ redirect-host — IP address/network mask or host name for redirect for NTLM or captive portal
+ server-certificate — SSL server certificate file name
+ timer — Expiration timer in minutes (1-1440)
> mode — Captive portal mode
    > redirect — Redirect configuration
        > session-cookie — Session cookie configuration
            + enable — Enable session cookie

```
                + roaming — Enable/disable IP roaming
                + timeout — Expiration timer in minutes (60-10080)
      transparent — Transparent option
> ntlm-auth — NT LAN Manager Authentication
      + attempts — Number of authentication attempts through each NTLM agent (1-10)
      + reversion-time — Time to wait to retry higher priority agent (60-3600)
      + timeout — Time to wait for authentication through NTLM agent (1-60)
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set device-group

(Panorama only) Configures device groups for management by Panorama.

For information about the syntax and options for each configuration available for device groups, refer to its command page in this chapter.

Syntax

```
set device-group <name>
    {
    description <value> |
    address |
    address-group |
    application |
    application-filter |
    application-group |
    devices <serial_number> {vsys <name>} |
    external-list |
    log-settings |
    master-device {device <name> | vsys <name>} |
    post-rulebase |
    pre-rulebase  |
    profile-group |
    profiles |
    region |
    schedule |
    service |
    service-group |
    threats |
    }
```

Options

+ description — Device group description text
> address — [*refer to "set address" on page 52*]
> address-group — [*refer to "set address-group" on page 53*]
> application — [*refer to "set application" on page 54*]
> application-filter — [*refer to "set application-filter" on page 57*]
> application-group — [*refer to "set application-group" on page 58*]
> devices — Device serial numbers
    > vsys — Option to specify a virtual system
> external-list — [*refer to "set external-list" on page 94*]
> log-settings — [*refer to "set shared log-settings" on page 258*]
> master-device — Device from which user and user groups will be retrieved
    + device — Master device name
    + vsys — Virtual system name
> post-rulebase — [*refer to "set shared post-rulebase" on page 265*]
> pre-rulebase — [*refer to "set shared pre-rulebase" on page 266*]
> profile-group — [*refer to "set profile-group" on page 196*]
> profiles — [*refer to "set profiles" on page 197*]
> region — [*refer to "set region" on page 213*]
> schedule — [*refer to "set schedule" on page 231*]

> service — [*refer to "set service" on page 232*]
> service-group — [*refer to "set service-group" on page 233*]
> threats — [*refer to "set threats" on page 278*]

Required Privilege Level

superuser, vsysadmin, deviceadmin

set deviceconfig high-availability

Configures High Availability (HA) on the device. Changes are retained, until overwritten, while the firewall is powered.

Syntax

```
set deviceconfig
   {
      high-availability {
          enabled yes|no;
          interface {
            ha1 {
              port <value>;
              link-speed auto|10|100|1000;
              link-duplex auto|full|half;
              encryption {
                enabled yes|no;
              }
              ip-address <ip/netmask>;
              netmask <value>;
              gateway <ip/netmask>;
              monitor-hold-time 1000-60000;
            }
            ha1-backup {
              port <value>;
              link-speed auto|10|100|1000;
              link-duplex auto|full|half;
              ip-address <ip/netmask>;
              netmask <value>;
              gateway <ip/netmask>;
            }
            ha2 {
              port <value>;
              link-speed auto|10|100|1000;
              link-duplex auto|full|half;
              ip-address <ip/netmask>;
              netmask <value>;
              gateway <ip/netmask>;
            }
            ha2-backup {
              port <value>;
              link-speed auto|10|100|1000;
              link-duplex auto|full|half;
              ip-address <ip/netmask>;
              netmask <value>;
              gateway <ip/netmask>;
            }
            ha3 {
              port <value>;
            }
```

```
}
group {
  REPEAT...
  <name> {
    description <value>;
    election-option {
      device-priority 0-255;
      preemptive yes|no;
      heartbeat-backup yes|no;
      timers {
          recommended;
          OR...
          aggressive;
          OR...
          advanced {
            promotion-hold-time 0-60000;
            hello-interval 8000-60000;
            heartbeat-interval 1000-60000;
            flap-max 0-16;
            preemption-hold-time 1-60;
            monitor-fail-hold-up-time 0-60000;
            additional-master-hold-up-time 0-60000;
          }
      }
    }
    peer-ip <ip/netmask>;
    peer-ip-backup <ip/netmask>;
    state-synchronization {
      enabled yes|no;
      transport ethernet|ip|udp;
      ha2-keep-alive {
        enabled yes|no;
        action log-only|split-datapath;
        threshold 5000-60000;
      }
    }
    configuration-synchronization {
      enabled yes|no;
    }
    mode {
        active-passive {
          passive-link-state shutdown|auto;
          monitor-fail-hold-down-time 1-60;
        }
        OR...
        active-active {
          device-id 0|1;
          tentative-hold-time 10-600;
          network-configuration {
            sync {
              virtual-router yes|no;
              qos yes|no;
            }
          }
```

```
virtual-address {
  REPEAT...
  <name> {
    ip {
      REPEAT...
      <name> {
          floating {
            device-priority {
              device-0 0-255;
              device-1 0-255;
              failover-on-link-down yes|no;
            }
          }
          OR...
          arp-load-sharing {
              ip-modulo;
              OR...
              ip-hash {
                hash-seed 0-4294967295;
              }
          }
      }
    }
    ipv6 {
      REPEAT...
      <name> {
          floating {
            device-priority {
              device-0 0-255;
              device-1 0-255;
              failover-on-link-down yes|no;
            }
          }
          OR...
          arp-load-sharing {
              ip-modulo;
              OR...
              ip-hash {
                hash-seed 0-4294967295;
              }
          }
      }
    }
  }
}
session-owner-selection {
    primary-device;
    OR...
    first-packet {
      session-setup {
          primary-device;
          OR...
          first-packet;
          OR...
```

```
                ip-modulo;
                OR...
                ip-hash {
                  hash-key source|source-and-destination;
                  hash-seed 0-4294967295;
                }
            }
          }
      }
    }
}
monitoring {
  path-monitoring {
    enabled yes|no;
    failure-condition any|all;
    path-group {
      virtual-wire {
        REPEAT...
        <name> {
          enabled yes|no;
          failure-condition any|all;
          source-ip <ip/netmask>;
          destination-ip [ <destination-ip1> <destination-ip2>... ];
          ping-interval 200-60000;
          ping-count 3-10;
        }
      }
      vlan {
        REPEAT...
        <name> {
          enabled yes|no;
          failure-condition any|all;
          source-ip <ip/netmask>;
          destination-ip [ <destination-ip1> <destination-ip2>... ];
          ping-interval 200-60000;
          ping-count 3-10;
        }
      }
      virtual-router {
        REPEAT...
        <name> {
          enabled yes|no;
          failure-condition any|all;
          destination-ip [ <destination-ip1> <destination-ip2>... ];
          ping-interval 200-60000;
          ping-count 3-10;
        }
      }
    }
  }
  link-monitoring {
    enabled yes|no;
    failure-condition any|all;
    link-group {
```

```
              REPEAT...
              <name> {
                enabled yes|no;
                failure-condition any|all;
                interface [ <interface1> <interface2>... ];
              }
            }
          }
        }
      }
    }
  }
}
}
```

Options

- > high-availability
  - + enabled — enabled (no or yes)
  - > group — HA group configuration
    - <*value*> — Group number (between 1 and 63)
    - + description — group description
    - + peer-ip — Peer IP address
    - + peer-ip-backup — Backup Peer IP address
    - > configuration-synchronization — Configuration synchronization
    - > election-option — HA election options
      - + device-priority — highest = 0, lowest = 255, default = 100
      - + heartbeat-backup — Use management port as backup path for heartbeat messages
      - + hello-interval — Interval in milliseconds to send Hello messages (8000-60000 ms), default = 8000
      - + preemptive — Configure on both HA peers to allow preemption by Passive or Active-Secondary device based on device-priority, default = no
      - > timers — Configure timers for high-availability
        - > Advanced
          - + additional-master-hold-up-time — Interval in milliseconds to wait before honoring a path or link monitor failure on the Active or Active-Primary device, default 500
          - + flap-max — Flaps before entering suspended state, 0 = infinite flaps, default 3
          - + heartbeat-interval — Interval in milliseconds to send Heartbeat pings, default 1000
          - + hello-interval — Interval in milliseconds to send Hello messages, default 8000
          - + monitor-fail-hold-up-time — Interval in milliseconds to wait before honoring a path or link monitor failure on this device, default 0
          - + preemption-hold-time — Interval in minutes to stay Passive before preempting Active device or to stay Active-Secondary before preempting Active-Primary device, default 1
          - + promotion-hold-time — Interval in milliseconds to state change from Passive to Active or Active-Secondary to Active-Primary, default 2000
        - + Aggressive — Use aggressive HA timer settings
        - + Recommended — Use recommended HA timer settings
    - > mode — Operational mode configuration
      - > active-active — Active-Active mode
        - + device-id — Device ID in HA group, 0 or 1
        - + packet-forwarding — Forward packet via HA3 link if session is owned by peer device (no or yes)
        - > network-configuration — Network configuration synchronization options
          - > sync –– Synchronization options
            - + qos –– Synchronize interface QoS configuration
            - + virtual-router –– Synchronize virtual router configuration
        - > tentative-hold-time –– Number of seconds that the firewall will remain in the tentative state if a failure occurs

```
      in an active/active configuration. During the tentative period the firewall will attempt to build routing
      adjacencies and populate its route table before it will process any packets (10-600; default = 60)
    > session-owner-selection — Firewall session owner selection options
      > first-packet — Session is owned by the device that receives the first packet of the session
        > session-setup — Session setup load-sharing options
          > ip-hash — Use hashing on source and destination addresses
            + hash-key — Address(es) to use as hash key
              - source — Source address only
              - source-and-destination — Source and destination addresses
            + hash-seed  User-specified hash seed (between 0 and 4294967295)
          - ip-modulo — Use modulo operations on source and destination addresses
          - primary-device — Use Active-Primary device to setup session
      - primary-device — Session is owned by the device in Active-Primary state
    > virtual-address — Virtual address configuration (Layer 3 interface name)
      > ip — Interface virtual IP address (IP/netmask or address object)
        > arp-load-sharing — ARP-based load-sharing
          > ip-hash — Hash based on IP address
            + hash-seed — User-specified hash seed
          - ip-modulo — IP address modulo number of devices, default option
        > floating — Floating address bound to one virtual device at any given time
          > device-priority  Virtual device priority
            + device-0 — Device 0 priority, highest: 0, lowest: 255
            + device-1 — Device 1 priority, highest: 0, lowest: 255
            + failover-on-link-down — Failover address if link state is down (no or yes)
      > ipv6 — Interface virtual IPv6 address (IP/netmask or address object)
        > arp-load-sharing — ARP-based load-sharing
          > ip-hash — Hash based on IP address
            + hash-seed — User-specified hash seed
          - ip-modulo — IP address modulo number of devices, default option
        > floating — Floating address bound to one virtual device at any given time
          > device-priority  Virtual device priority
            + device-0 — Device 0 priority, highest: 0, lowest: 255
            + device-1 — Device 1 priority, highest: 0, lowest: 255
            + failover-on-link-down — Failover address if link state is down (no or yes)
  > active-passive — Active-Passive mode
    + monitor-fail-hold-down-time — Interval in minutes to stay in non-functional state following a link/path
      monitor failure (between 1 and 60); default = 1
    + passive-link-state — Link mode of data-plane interfaces while in Passive state
      - auto — Link put into automatically configured mode
      - shutdown — Link put into powered off state
> monitoring — Monitoring configuration
  > link-monitoring — Link monitoring configuration
    + enabled — Link monitoring enabled
    + failure-condition — Condition to determine failure, default = any (failure on any link group)
    > link-group — Monitored link group configuration
      + interface - Interface(s) to monitor (member value or list of values enclosed in [ ])
  > path-monitoring — Path monitoring configuration
    + enabled — Path monitoring enabled
    + failure-condition — Condition to determine failure, default = any (failure on any path group)
    > path-group — Monitored path group
      > virtual-router — Monitor within virtual-router (alpha-numeric string [a-zA-Z0-9:@./_-])
        + destination-ip — Destination IP addresses to monitor
        + enabled — Monitoring enabled
        + failure-condition — Condition to determine failure, default = any (failure on any monitored IP)
```

```
                > virtual-wire — Monitor within virtual-wire (alphanumeric string [a-zA-Z0-9:@./_-])
                    + destination-ip — Destination IP addresses to monitor
                    + enabled — Monitoring enabled
                    + failure-condition — Condition to determine failure, default = any (failure on any monitored IP)
                    + source-ip — Source IP address to send monitoring packet
                > vlan — Monitor within VLAN (alphanumeric string [a-zA-Z0-9:@./_-])
                    + destination-ip — Destination IP addresses to monitor
                    + enabled — Monitoring enabled
                    + failure-condition — Condition to determine failure, default = any (failure on any monitored IP)
                    + source-ip — Source IP address to send monitoring packet
    > state-synchronization — State synchronization
        + enabled — enabled (no or yes)
        + transport — transport layer configuration
            - ethernet — Layer2 transport via Ethernet
                + enabled — no | yes
            - ip — Layer3 transport via IP protocol 99
                + enabled — no | yes
            - udp — Layer4 transport via UDP/29281
                + enabled — no | yes
> interface — HA interface configuration
    > ha1 — HA1 interface (control link)
        + gateway — Gateway for the HA1 interface (x.x.x.x)
        + ip-address — IP address for the HA1 interface (x.x.x.x)
        + link-duplex — Interface link duplex (auto-negotiation, full duplex, or half duplex)
        + link-speed — Interface link speed (10Mbps, 100Mbps, 1000Mbps, or auto-negotiation)
        + monitor-hold-time — Hold time in milliseconds to allow HA1 link flapping (between 1000 and 60000); default =
            3000
        + netmask — IP netmask for the HA1 interface (x.x.x.x)
        + port — Interface name or management (dedicated management port as HA1 interface); default = management
        > encryption — HA1 interface encryption settings
            + enabled — no | yes
    > ha1-backup — Backup HA1 interface (control link)
        + gateway — Gateway for the HA1 interface (x.x.x.x)
        + ip-address — IP address for the HA1 interface (x.x.x.x)
        + link-duplex — Interface link duplex (auto-negotiation, full duplex, or half duplex)
        + link-speed — Interface link speed (10Mbps, 100Mbps, 1000Mbps, or auto-negotiation)
        + netmask — IP netmask for the HA1 interface (x.x.x.x)
        + port — Interface name or management (dedicated management port as backup HA1 interface)
    > ha2 — HA2 interface (runtime object synchronization link)
        + gateway — Gateway for the HA2 interface (x.x.x.x)
        + ip-address — IP address for the HA2 interface (x.x.x.x)
        + link-duplex — Interface link duplex (auto-negotiation, full duplex, or half duplex)
        + link-speed — Interface link speed (10Mbps, 100Mbps, 1000Mbps, or auto-negotiation)
        + netmask — IP netmask for the HA2 interface (x.x.x.x)
        + port — Interface name
    > ha2-backup — Backup HA2 interface (runtime object synchronization link)
        + gateway — Gateway for the HA2 interface (x.x.x.x)
        + ip-address — IP address for the HA2 interface (x.x.x.x)
        + link-duplex — Interface link duplex (auto-negotiation, full duplex, or half duplex)
        + link-speed — Interface link speed (10Mbps, 100Mbps, 1000Mbps, or auto-negotiation)
        + netmask — IP netmask for the HA2 interface (x.x.x.x)
        + port — Interface name
    > ha3 — HA3 interface (packet forwarding link in Active-Active mode)
        + port — Interface name
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set deviceconfig setting

Specifies general device settings on the firewall.

Syntax

```
set deviceconfig
   {
   setting |
     {
     application |
        {
        bypass-exceed-queue {no | yes} |
        cache {no | yes} |
        cache-threshold <value> |
        dump-unknown {off | on} |
        heuristics {no | yes} |
        identify-unknown-traffic-by-port {no | yes} |
        notify-user {no | yes} |
        supernode {no | yes} |
        use-cache-for-identification {no | yes} |
        traceroute {no | yes} |
        {
           enable {no | yes} |
           ttl-threshold <value>
        }
        }
     config rematch {no | yes} |
     ctd |
        {
        tcp-bypass-exceed-queue {no | yes} |
        udp-bypass-exceed-queue {no | yes} |
        cap-portal-ask-timeout <value> |
        cap-portal-max-session <value> |
        extended-capture-segment <value> |
        http-proxy-use-transaction {no | yes} |
        skip-block-http-range {no | yes} |
        strip-x-fwd-for {no | yes} |
        url-admin-timeout <minutes> |
        url-coach-timeout <minutes> |
        url-lockout-timeout <minutes> |
        url-wait-timeout <seconds> |
        x-forwarded-for {no | yes}
        }
     custom-logo |
        {
        hide-panorama-header-background {no | yes} |
        login-screen {content <value> | file-name <value>} |
        main-ui {content <value> | file-name <value>} |
        pdf-report-footer {content <value> | file-name <value>} |
        pdf-report-header {content <value> | file-name <value>}
        }
```

```
global-protect {keepalive <value> | timeout <value> | worker-threads <value>} |
icmpv6-rate-limit |
   {
   bucket-size <value> |
   packet-rate <value>
   }
jumbo-frame mtu <value> |
logging |
   {
   log-suppression {no | yes} |
   max-log-rate <value> |
   max-packet-rate <value>
   }
logrcvr container-page-timeout <value> |
management |
   {
   auto-acquire-commit-lock {no | yes} |
   get-only-new-logs-on-convert-to-primary {no | yes} |
   enable-certificate-expiration-check {no | yes} |
   enable-syslog-high-dp-load {no | yes} |
   hostname-type-in-syslog {FQDN | hostname | ipv4-address | ipv6-address } |
   idle-timeout <value> |
   max-audit-versions <value> |
   max-backup-versions <value> |
   max-rows-in-csv-export <value> |
   max-rows-in-pdf-report <value> |
   only-active-primary-logs-to-local-disk {no | yes} |
   panorama-ssl-send-retries <value> |
   panorama-tcp-receive-timeout <value> |
   panorama-tcp-send-timeout <value> |
   send-hostname-in-syslog {no | yes}|
   share-unused-objects-with-devices {no | yes} |
   shared-objects-take-precedence {no | yes} |
   traffic-stop-on-logdb-full {no | yes} |
   admin-lockout |
      {
      failed-attempts <value> |
      lockout-time <value>
      }
   browse-activity-report-setting
      {
      average-browse-time <value> |
      page-load-threshold <value>
      }
   chassis-quota
      log-card
         {
         dailythsum <value> |
         dailytrsum <value> |
         hipmatch <value> |
         hourlythsum <value> |
         hourlytrsum <value> |
         ip-tag <value> |
         threat <value> |
         threat-pcaps <value> |
         thsum <value> |
         traffic <value> |
         trsum <value> |
         userid <value> |
         weeklythsum <value> |
         weeklytrsum <value> |
         }
      mgmt-card
         {
         alarm <value> |
         application-pcaps <value> |
         appstat <value> |
         config <value> |
         debug-filter-pcaps <value> |
         dlp-logs <value> |
         hip-reports <value> |
         system <value> |
      }
   common-criteria-alarm-generation |
      {
      enable-alarm-generation {no | yes} |
      enable-audible-alarms {no | yes} |
      enable-cli-alarm-notification {no | yes} |
      enable-web-alarm-notification {no | yes} |
      encrypt-decrypt-fail-count <value> |
      log-databases-alarm-threshold {alarm | config | hipmatch | system | threat
         | traffic} <value>
      rule-group-limits {count <value> | tags <value> | time-interval <value>} |
      security-policy-limits {count <value> | time-interval <value>}
      }
   disable-predefined-report <value> |
   disk-quota |
      {
      alarm <value> |
      application-pcaps <value> |
      appstat <value> |
      config <value> |
      dailythsum <value> |
      dailytrsum <value> |
      debug-filter-pcaps <value> |
      dlp-logs <value> |
      hip-reports <value> |
      hipmatch <value> |
      hourlythsum <value> |
      hourlytrsum <value> |
      system <value> |
      threat <value> |
      threat-pcaps <value> |
      thsum <value> |
      traffic <value> |
      trsum <value> |
      userid <value>|
      weeklythsum <value> |
      weeklytrsum <value>
      }
   log-forwarding-from-device {buffered {no | yes}} |
   storage-partition
      {
      nfsv3 {copy-on-setup {no | yes} | log-directory <value> | port <value> |
         protocol {tcp | udp} | read-size <value> | server <value> | write-size
         <value>}
      internal
      }
   }
nat |
   {
   reserve-ip {no | yes} |
   reserve-time <seconds>
   }
nat64 ipv6-min-network-mtu <value> |
packet ip-frag-limit {no | yes} |
pow |
   {
   wqe-inuse-check {no | yes} |
   wqe-swbuf-check {no | yes} |
   wqe-swbuf-ref {no | yes} |
   wqe-tag-check {no | yes}
   }
session |
   {
   accelerated-aging-enable {no | yes} |
   accelerated-aging-scaling-factor <value> |
   accelerated-aging-threshold <value> |
   ipv6-firewalling {no | yes} |
   offload {no | yes} |
   resource-limit-behavior {bypass | drop} |
   scan-scaling-factor <value> |
   scan-threshold <value> |
   tcp-reject-non-syn {no | yes} |
   timeout-captive-portal <value> |
   timeout-default <value> |
   timeout-discard-default <value> |
   timeout-discard-tcp <value> |
   timeout-discard-udp <value> |
   timeout-icmp <value> |
   timeout-scan <value> |
   timeout-tcp <value> |
   timeout-tcp-half-closed <value> |
   timeout-tcp-time-wait <value> |
   timeout-tcp-unverified-rst <value> |
   timeout-tcphandshake <value> |
   timeout-tcpinit <value> |
   timeout-udp <value>
   }
ssl-decrypt |
   {
   answer-timeout <seconds> |
   block-timeout-cert {no | yes} |
   block-unknown-cert {no | yes} |
   cert-status-timeout <seconds> |
   crl {no | yes} |
   crl-receive-timeout <seconds> |
   fwd-proxy-server-cert-key-size {0 | 1024 | 2048} |
   notify-user {no | yes} |
   ocsp {no | yes} |
   ocsp-receive-timeout <seconds> |
   url-proxy {no | yes}
   }
tcp |
   {
   asymmetric-path {bypass | drop} |
   bypass-exceed-oo-queue {no | yes} |
   check-timestamp-option {no | yes} |
   urgent-data {clear | oobinline}
   }
url
   {
   dynamic-url {no | yes} |
   dynamic-url-timeout <hours> |
   }
util assert-crash-once {no | yes} |
wildfire |
   {
   active-vm <vm-name> |
   auto-submit {no | yes} |
   cloud-server {<ip/netmask> | <hostname>} |
   vm-network-enable {no | yes} |
   vm-network-use-tor {no | yes} |
   analyzer-network-connection {enable | disable} |
   disable-pdf-sniffer {no | yes} |
   disable-server-select {no | yes} |
   disable-signature-verify {no | yes} |
   file-idle-timeout <value> |
   file-size-limit {apk | flash | jar | ms-office | pdf | pe} <value> |
   file-upload-rate <value> |
   report-benign-file {no | yes} |
   session-info-select {
      exclude-app-name {no | yes} |
      exclude-dest-ip {no | yes} |
      exclude-dest-port {no | yes} |
      exclude-email-recipient {no | yes} |
      exclude-email-sender {no | yes} |
      exclude-email-subject {no | yes} |
      exclude-filename {no | yes} |
      exclude-src-ip {no | yes} |
      exclude-src-port {no | yes} |
      exclude-url {no | yes} |
      exclude-username {no | yes} |
      exclude-vsys-id {no | yes}
      }
   }
```

```
zip
   {
   enable {no | yes} |
   sw {no | yes}
   }
}
```

Options

> setting
    > application
        + bypass-exceed-queue — Set whether to skip inspection of session if queue limit is exceeded
        + cache — Set if application cache should be enabled. This will enable or disable the App-ID cache for all purposes, which include: help in identifying some evasive applications, caching App-IDs for application identification, enable Policy Based Forwarding (PBF) based on application, and to improve performance under certain traffic mix conditions. As of PAN-OS 5.0.2, you can disable just the App-ID portion of this feature. See the use-cache-for-identification option.
        + cache-threshold — Set application cache threshold (between 1 and 65535)
        + dump-unknown — Set if unknown application capture should be enabled
        + heuristics — Set if heuristics detection should be enabled
        + identify-unknown-traffic-by-port — Set if unknown traffic should be identified by source or destination port
        + notify-user — Set if user should be notified when web-application is blocked
        + supernode — Set if supernode detection should be enabled
        + use-cache-for-identification — As of PAN-OS 5.0.2, the App-ID cache will not be used for security policies purposes by default. This command (added in 5.0.2), will allow you to enable the App-ID cache. For more information on this feature, refer to the security advisory PAN-SA-2013-001.
        > traceroute — enable or disable application identification for traceroute, specify TTL threshold value for traceroute identification
    > config rematch — (no or yes)
    > ctd
        + tcp-bypass-exceed-queue — Set whether to skip inspection of TCP session if queue limit is exceeded
        + udp-bypass-exceed-queue — Set whether to skip inspection of UDP session if queue limit is exceeded
        + cap-portal-ask-timeout— Set captive portal timeout (seconds)
        + cap-portal-max-session — Set maximum number of captive portal sessions
        + extended-capture-segment— Set number of segments of threat packet capture (1-50, default 5)
        + http-proxy-use-transaction — Set whether to use transaction for stats for http proxy sessions
        + skip-block-http-range — Whether to skip the blocking of HTTP range requests
        + strip-x-fwd-for — Set whether to strip x-forwarded-for in http header. When this option is selected, the firewall zeroes out the header value before forwarding the request, and the forwarded packets do not contain internal source IP information.
        + url-admin-timeout — Set URL admin continue timeout in minutes (1-86400)
        + url-coach-timeout — Set URL coach continue timeout in minutes (1-86400)
        + url-lockout-timeout — Set URL admin override lockout timeout in minutes (1-86400)
        + url-wait-timeout — Set URL category query timeout in seconds (1-60)
        + x-forwarded-for — Enable/disable parsing of x-forwarded-for attribute
    > custom-logo
        + hide-panorama-header-background — (Panorama only) Whether to hide Panorama header background
        > login-screen — Import custom logo for login screen (from content or file)
            + content — Upload custom login screen page (base64 encoded)
            + name — File name alphanumeric string [0-9a-zA-Z./_-]
        > main-ui — Import custom logo for main user interface (from content or file)
            + content — Upload custom main user interface page (base64 encoded)
            + name — File name alphanumeric string [0-9a-zA-Z./_-]
        > pdf-report-footer — Import custom logo for PDF report footers (from content or file)

```
        + content — Upload custom PDF report footer page (base64 encoded)
        + name — File name alphanumeric string [ 0-9a-zA-Z./_-]
    > pdf-report-header — Import custom logo for PDF report headers (from content or file)
        + content — Upload custom lPDF report header page (base64 encoded)
        + name — File name alphanumeric string [ 0-9a-zA-Z./_-]
>global-protect
    + keepalive — Seconds to keep alive GlobalProtect gateways (3-150)
    + timeout — Seconds before time out of GlobalProtect gateways (3-150)
    + worker-threads — Number of users that can simultaneously connect to the GlobalProtect Portal (10-100)
> icmpv6-rate-limit
    + bucket-size — Token-bucket size for ICMPv6 error rate limiting (10-65535)
    + packet-rate — ICMPv6 error packet limit per second (1-65535)
> jumbo-frame
    + mtu — device MTU excluding Ethernet header (512-9216)
> logging
    + log-suppression — Enable/disable log suppression
    + max-log-rate — Set maximum logging rate (0-50000)
    + max-packet-rate — Set maximum packet logging rate (0-2560)
> logrcvr container-page-timeout — Container page timeout in seconds (1-60)
> management
    + auto-acquire-commit-lock — Automatically add a commit lock when modifying configuration
    + get-only-new-logs-on-convert-to-primary — (Panorama only) When Panorama becomes the primary, get only new logs
        from device
    + enable-certificate-expiration-check — Check for expired certificates and stop using them
    + enable-syslog-high-dp-load — Issue a system log if one of the CPUs is under a severe load
    + hostname-type-in-syslog — Specify how the host is identified in syslog messages (FQDN hostname, ipv4-address,
        ipv6-address)
    + idle-timeout — Default administrative session idle timeout in minutes (1-1440; 0 = never)
    + log-forwarding-from-device-buffered — (Panorama only) Set to enable log buffering between the device and
        Panorama; if enabled, logs are retained despite a temporary connection loss; default = yes
    + max-audit-versions — Maximum number of audited versions of config to preserve (1-1048576)
    + max-backup-versions — Maximum number of versions of config to back up per device (1-1048576)
    + max-rows-in-csv-export — Maximum number of rows in exported csv files (1-1048576)
    + max-rows-in-pdf-report — Maximum number of rows in user activity report (1-1048576)
    + only-active-primary-logs-to-local-disk — (Panorama only) Only active primary Panorama will receive logs from
        device and store in local disk. Set to perform all logging only on the Active-Primary Panorama instance; if not set,
        both Panorama instances will receive and store all logs; default = no (this setting affects only logging to Panorama's
        internal log store and does not affect NFS mounts)
    + panorama-ssl-send-retries — Retry count for SSL sends to Panorama (1-64)
    + panorama-tcp-receive-timeout — Receive timeout for TCP connection to Panorama (1-120)
    + panorama-tcp-send-timeout — Send timeout for TCP connection to Panorama (1-120)
    + send-hostname-in-syslog — Send hostname as part of syslog
    + share-unused-objects-with-devices — (Panorama only) During device-group commit, send address and service objects
        unused in rules to the devices
    + shared-objects-take-precedence — (Panorama only) Objects defined in shared section will take higher precedence
    + traffic-stop-on-logdb-full — Stop traffic if logdb is full with unexported logs
    > admin-lockout — Administrative login lockout settings
        + failed-attempts — Number of failed login attempts to trigger lock-out (0-10)
        + lockout-time — Number of minutes to lock-out (0-60)
    > browse-activity-report-setting — Settings for the URL filtering report with browse durations
        + average-browse-time — Average time in seconds for a browse session (0-300)
        + page-load-threshold — Average time in seconds to load a URL page (0-60)
    > chassis-quota
        >log-card —
        + dailythsum — Daily threat summary quota percentage
        + dailytrsum — Daily traffic summary quota percentage
        + hipmatch — HIP match quota percentage
        + hourlythsum — Hourly threat summary quota percentage
        + hourlytrsum — Hourly traffic summary quota percentage
        + ip-tag — IP tag quota percentage
        + threat — Threat logs quota percentage
        + threat-pcaps — Threat packet capture quota percentage
        + thsum — Threat summary quota percentage
        + traffic — Traffic logs quota percentage
        + trsum — Traffic summary quota percentage
        + userid — User ID logs quota percentage
        + weeklythsum — Weekly threat summary quota percentage
        + weeklytrsum — Weekly traffic summary quota percentage
    >mgmt-card —
        + alarm — Alarm logs quota percentage
        + application-pcaps — Application packet capture quota percentage
        + appstat — Application statistics quota percentage
        + config — Configuration logs quota percentage
        + debug-filter-pcaps — Debug filter packet capture quota percentage
        + dlp-logs — Data filter packet capture quota percentage
        + hip-reports — Host information profile quota percentage
        + system — System logs quota percentage
> common-criteria-alarm-generation
    + enable-alarm-generation — Enable Common Criteria (CC) alarms generation
    + enable-audible-alarms — Enable audio sound for alarms
    + enable-cli-alarm-notification — Enable alarms notification on admin console
    + enable-web-alarm-notification — Enable alarms notification on Web
    + encrypt-decrypt-fail-count — Encryption/Decryption failure counts limit (1-4294967295)
    > log-databases-alarm-threshold — Log databases % full threshold value for alarms generation
        + alarm — alarm logs database % full threshold value for alarm  generation (1-100)
        + config — configuration logs database % full threshold value for alarm  generation (1-100)
        + hipmatch — hipmatch logs database % full threshold value for alarm  generation (1-100)
        + system — system logs database % full threshold value for alarm  generation (1-100)
        + threat — threat logs database % full threshold value for alarm  generation (1-100)
        + traffic — traffic logs database % full threshold value for alarm  generation (1-100)
    > rule-group-limits — Security rule group violation notification threshold (count 1-4294967295; time-interval 30-86400). Security rule group limits are the number of times, and time in which, the rule groups that are tagged with "tags" are matched.
        + tags — Tags for rule group member value or list of values
    > security-policy-limits — Security rule violation notification threshold (count 1-4294967295; time-interval 30-86400). Security policy limits affect each individual rule in the security policy.  If any rule hits the specified count within the time-interval, an alarm is generated.
> disable-predefined-reports — Specify the predefined report to disable
> disk-quota — Quotas for logs, packet captures etc. (percentages between 0 and 90.0)
    + alarm — Alarm logs quota percentage
    + application-pcaps — Application packet capture quota percentage
    + appstat — Application statistics quota percentage
    + config — Configuration logs quota percentage
    + dailythsum — Daily threat summary quota percentage
    + dailytrsum — Daily traffic summary quota percentage
    + debug-filter-pcaps — Debug filter packet capture quota percentage
    + dlp-logs — DLP log data quota percentage
    + hip-reports — Host information profile quota percentage
```

```
        + hipmatch — HIP match quota percentage
        + hourlythsum — Hourly threat summary quota percentage
        + hourlytrsum — Hourly traffic summary quota percentage
        + system — System logs quota percentage
        + threat — Threat logs quota percentage
        + threat-pcaps — Threat packet capture quota percentage
        + thsum — Threat summary quota percentage
        + traffic — Traffic logs quota percentage
        + trsum — Traffic summary quota percentage
        + userid — User ID logs quota percentage
        + weeklythsum — Weekly threat summary quota percentage
        + weeklytrsum — Weekly traffic summary quota percentage
    > log-forwarding-from-device — Log forwarding options from device
        + buffered — Turn log buffering on or off
    > storage-partition — Storage parameters for logging
        > nfsv3 — Use NFS v3
            + copy-on-setup — Whether to copy on setup
            + log-directory — Directory to mount
            + port — Port number (0-65535)
            + protocol — Protocol (TCP or UDP)
            + read-size — Read size (256-32768)
            + server — Server IP address and network mask or FQDN
            + write-size — Write size (256-32768)
        internal — Use internal hard disk
> nat
    + reserve-ip — Reserve translated IP for specified time
    + reserve-time — Reserve time value in seconds (1-604800)
> nat64
    + ipv6-min-network-mtu — NAT64 minimum IPv6 maximum transmission unit (MTU) in the network (1280-9216)
> packet
    + ip-frag-limit — Enables/disables the IP packet fragmentation limit
> pow
    + wqe-inuse-check — Enable/disable Work Queue Element (WQE) in-use check
    + wqe-swbuf-check — Enable/disable WQE SWBuf trailer check
    + wqe-swbuf-ref — Enable/disable WQE SWBuf reference in clone
    + wqe-tag-check — Enable/disable WQE session ID tag check
> session
    + accelerated-aging-enable — Enable/disable accelerated session aging
    + accelerated-aging-scaling-factor — Set accelerated session aging scaling factor (power of 2) (2-16)
    + accelerated-aging-threshold — Set accelerated aging threshold in percentage of session utilization (50-99)
    + ipv6-firewalling — Enables/disables IPv6 firewalling
    + offload — Enables/disables hardware session offloading
    + resource-limit-behavior — Behavior when resource limit is reached (bypass or drop)
    + scan-scaling-factor — Sets scan scaling factor (2-16)
    + scan-threshold — Resource utilization threshold to trigger session scan (50-99)
    + tcp-reject-non-syn — Reject non-SYN TCP packet for session setup
    + timeout-captive-portal — Sets captive-portal session timeout value in seconds (1-15999999)
    + timeout-default — Sets session default timeout value in seconds (1-604800)
    + timeout-discard-default — Sets timeout of non-TCP/UDP session in discard state (1-604800)
    + timeout-discard-tcp — Sets timeout of TCP session in discard state (1-604800)
    + timeout-discard-udp — Sets timeout of UDP session in discard state (1-604800)
    + timeout-icmp — Sets ICMP timeout value in seconds (1-604800)
    + timeout-scan — Application trickling timeout value in seconds (5-30)
    + timeout-tcp — Sets TCP timeout value in seconds (1-5999999)
    + timeout-tcp-half-closed — Sets TCP half-closed session timeout (after receiving first FIN) value in seconds (1-604800, default 120)
    + timeout-tcp-time-wait — Sets TCP time wait timeout (after receiving second FIN or a RST) value in seconds (1-600, default 15)
    + timeout-tcp-unverified-rst — Sets TCP unverified RST timeout (after receiving a RST with unverified sequence number) value in seconds (1-600, default 30)
    + timeout-tcphandshake — Sets the TCP handshake session timeout value (before 3-way handshaking is completed), in seconds (1-60)
    + timeout-tcpinit — Sets TCP initial session timeout (before 3-way handshaking is completed) value in seconds (1-60)
    + timeout-udp — Sets UDP timeout value in seconds (1-604800)
> ssl-decrypt
    + answer-timeout — Sets user reply timeout value in seconds (1-86400)
    + block-timeout-cert — Sets whether to block a session if certificate status can't be retrieved within timeout
    + block-unknown-cert — Sets whether to block a session if certificate status is unknown
    + cert-status-timeout — Sets cert status query timeout value in seconds (0-60)
    + crl — Sets whether to use CRL to check certificate status
    + crl-receive-timeout — Sets CRL receive timeout value in seconds (1-60)
    + fwd-proxy-server-cert-key-size — Sets the key size used in SSL/TLS Forward Proxy certificates that PAN-OS generates for the connection between the firewall and the client. The value options are:
        0 — PAN-OS determines the key size to use based on the key size that the destination server uses. If the destination server uses a 1024-bit RSA key, PAN-OS generates a certificate with that key size and an SHA-1 hashing algorithm. If the destination server uses a key size that exceeds 1024 bits (for example, 2048 bits or 4096 bits), PAN-OS generates a certificate that uses a 2048-bit RSA key and SHA-256 algorithm. This is the default setting.
        1024 — PAN-OS generates certificates that use a 1024-bit RSA key and SHA-1 hashing algorithm regardless of the key size that the destination server uses. As of December 31, 2013, public certificate authorities (CAs) and popular browsers have limited support for X.509 certificates that use keys of fewer than 2048 bits. In the future, depending on security settings, when presented with such keys the browser might warn the user or block the SSL/TLS session entirely.
        2048 — PAN-OS generates certificates that use a 2048-bit RSA key and SHA-256 hashing algorithm regardless of the key size that the destination server uses. Public CAs and popular browsers support 2048-bit keys, which provide better security than the 1024-bit keys.
    + notify-user — Sets if user notification should be enabled
    + ocsp — Sets whether to use OCSP to check certificate status
    + ocsp-receive-timeout — Sets OCSP receive timeout value in seconds (1-60)
    + url-proxy — Sets proxy for SSL sessions if the IP’s URL category is blocked
> tcp
    + asymmetric-path — Actions for TCP sliding window tracking errors, also controls enable/disable TCP sequence number check for FIN/RST
        bypass — Bypass inspection for the session that has TCP sliding window tracking errors
        drop — Drop offending packets that violated TCP sliding window tracking, enable TCP sequence number check for FIN/RST
    + bypass-exceed-oo-queue — Whether to skip inspection of session if out-of-order packets limit is exceeded
    + check-timestamp-option — Whether to drop packets with invalid timestamp options
    + urgent-data — Clears urgent flag in TCP header
        clear — Always clear urgent data pointers (default)
        oobinline — Assume host process OOB data inline with normal data
> url
    + dynamic-url —(for BrightCloud only) Enable this option if you are using URL categories as part of your match criteria for security policies and would like to enable dynamic lookups as part of that process. This is a global setting that will allow the URL lookup during a policy match to query the cloud server if a URL profile is not configured in the policy.
    + dynamic-url-timeout — (for BrightCloud only) Dynamic URL entry timeout, in hours (1-720)
> util
```

+ assert-crash-once — Enables/disables assert crash only once

> wildfire

+ analyzer-network-connection — Enable analyzer connection
+ active-vm — Specify a VM to use for malware analysis (there are four VMs available, one Windows XP and three Window 7 images with different versions of Microsoft Office)
+ auto-submit— Automatically send malware information to the public cloud
+ cloud-server — IP address or hostname for cloud server
+ disable-signature-verify — Disable file signature verification
+ file-idle-timeout — Set file caching idle timeout (seconds)
+ file-size-limit — Sets the limit of file size in MB that will be forwarded (specify type of file and limit)
+ apk — Limit for apk files (1-10 MB)
+ jar — Limit for jar files (1-10 MB)
+ ms-office — Limit for ms-office files (200-10000 KB)
+ pdf — Limit for pdf files (100-500 KB)
+ pe — Limit for pe files (1-10 MB)
+ file-upload-rate — Number of files uploaded per minute (1-5)
+ report-benign-file — Collect reports from cloud for benign files

> session-info-select — Select fields excluded from session info while forwarding

+ exclude-app-name — Excludes application name
+ exclude-dest-ip — Excludes destination IP address
+ exclude-dest-port — Excludes destination port
+ exclude-email-recipient — Excludes email recipient address from the WildFire log
+ exclude-email-sender — Excludes email sender address from the WildFire log
+ exclude-email-subject — Excludes email subject from the WildFire log
+ exclude-filename — Excludes file name
+ exclude-src-ip — Excludes source IP address
+ exclude-src-port — Excludes source port
+ exclude-url — Excludes url
+ exclude-username — Excludes user name
+ exclude-vsys-id — Excludes vsys id
+ vm-network-enable — (yes or no)
+ vm-network-use-tor (yes or no)

> zip

+ enable — Enables/disables zip engine. The zip engine is used to decompress compressed content in traffic to identify the contents of the compressed files in order to scan for threats.
+ sw — Enables/disables zip hardware engine. In environments where there is lot of traffic that contains compressed files, offloading to hardware will help ensure that the firewall can keep up with the decompression of traffic for analysis.

Sample Output

The following command locks an administrative user out for **15** minutes after **5** failed login attempts.

```
username@hostname# set deviceconfig setting management admin-lockout 5 lockout-time 15
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set deviceconfig system

Specifies system-related settings on the firewall.

Syntax

```
set deviceconfig
   {
   system
     {
     authentication-profile <value> |
     certificate-profile <value> |
     common-name-for-certificate <value> |
     default-gateway <ip_address> |
     deployment-update-schedule <name> <type> recurring <hourly/daily/weekly> [<day-
        of-week>] at <time> action <action> <list of device serial numbers>
     domain <value> |
     domain-lookup-url <value> |
     fqdn-forcerefresh-time <value> |
     fqdn-refresh-time <value> |
     hostname <value> |
     ip-address <ip_address> |
     ip-address-lookup-url <value> |
     ipv6-address <ip/netmask> |
     ipv6-default-gateway <value> |
     locale {en_US | ja_JP | zh_CN | zh_TW} |
     login-banner <value> |
     mtu <value> |
     netmask <value> |
     ntp-server-1 <value> |
     ntp-server-2 <value> |
     panorama-server <value> |
     panorama-server-2 <value> |
     secure-proxy-password <value> |
     secure-proxy-port <value> |
     secure-proxy-server <value> |
     secure-proxy-user <value> |
     server-verification {no | yes} |
     speed-duplex <value> |
     syslog-certificate <value> |
     timezone <value> |
     update-server <value> |
     web-server-certificate <value> |
     config-bundle-export-schedule |
        {
        description <value> |
        enable {no | yes} |
        start-time <value> |
        protocol
           {
           ftp {hostname <value> | passive-mode {no | yes} | password <value> | path
              <value> | port <value> | username <value>} |
           scp {hostname <value> | password <value> | path <value> | port <value> |
              username <value>}
           }
        }
     dns-setting |
        {
        dns-proxy-object <value> |
        servers {primary <value> | secondary <value>}
        }
     geo-location |
        {
        latitude <coordinate> |
        longitude <coordinate>
        }
     log-export-schedule <schedule_name>
        {
        description <value> |
        enable {no | yes} |
        log-type {data | hipmatch | threat | traffic | url}
        start-time <value> |
        protocol ftp
           {
           hostname <value> |
           passive-mode {no | yes} |
           password <value> |
           path <value> |
           port <value> |
           username <value> |
        protocol scp
           {
           hostname <value> |
           password <value> |
           path <value> |
           port <value> |
           username <value>
           }
        }
     log-link <value> url <value> |
     permitted-ip <value> |
     route |
        {
        destination <IP/FQDN> source address <ip> interface <value> |
        service
           {
           crl-status source address <ip> interface <value> |
           dns source address <ip> interface <value> |
           email source address <ip> interface <value> |
           netflow source address <ip> interface <value> |
           ntp source address <ip> interface <value> |
           paloalto-updates source address <ip> interface <value> |
           panorama source address <ip> interface <value> |
           proxy source address <ip> interface <value> |
           radius source address <ip> interface <value> |
           snmp source address <ip> interface <value> |
           syslog source address <ip> interface <value> |
           uid-agent source address <ip> interface <value> |
           url-updates source address <ip> interface <value> |
           wildfire source address <ip> interface <value> |
           {<value>
              source address <ip> interface <value> |
              source-v6 address <ipv6> interface <value> |
           }
        }
     service |
        {
        disable-http {no | yes} |
        disable-http-ocsp {no | yes} |
        disable-https {no | yes} |
        disable-icmp {no | yes} |
        disable-snmp {no | yes} |
        disable-ssh {no | yes} |
        disable-telnet {no | yes} |
        disable-userid-service {no | yes}
        disable-userid-syslog-listener-ssl {no | yes}
        disable-userid-syslog-listener-udp {no | yes}
        }
     snmp-setting |
        {
        access-setting version |
           {
           v2c snmp-community-string <value> |
           v3
              {
              users <user_name> |
                 {
                 authpwd <value> |
                 privpwd <value> |
                 view <value>
                 }
              views <view_name> view <value>
              }
        snmp-system
           {
           contact <value> |
           location <value> |
           send-event-specific-traps {no | yes}
           }
        }
     update-schedule
        {
        anti-virus recurring |
           {
           sync-to-peer {no | yes} |
           threshold <value> |
           daily at <value> action {download-and-install | download-only} |
           hourly at <value> action {download-and-install | download-only} |
           weekly
              {
              at <value> |
              day-of-week {friday | monday | saturday | sunday | thursday | tuesday |
                 wednesday} |
              action {download-and-install | download-only}
              }
        }
        app-profile recurring |
           {
           sync-to-peer {no | yes} |
           threshold <value> |
           daily at <value> action {download-and-install | download-only} |
           hourly at <value> action {download-and-install | download-only} |
           weekly
              {
              at <value> |
              day-of-week {friday | monday | saturday | sunday | thursday | tuesday |
                 wednesday} |
              action {download-and-install | download-only}
              }
           }
        global-protect-datafile recurring |
           {
           daily at <value> action download-and-install |
           hourly at <value> action download-and-install |
           weekly
              {
              at <value> |
              day-of-week {friday | monday | saturday | sunday | thursday | tuesday |
                 wednesday} |
              action download-and-install
              }
           }
        statistics-service |
           {
           application-and-threat-reports |
              {
              application-usage {no | yes} |
              attackers {no | yes} |
              attacking-countries {no | yes}
              }
           device software-crash-info {no | yes} |
           unknown-application-reports |
              {
              unknown-applications-by-destination-addresses {no | yes} |
              unknown-applications-by-destination-ports {no | yes}
              }
           url-reports
              {
              dataplane-cache-url {no | yes} |
              malware-categories-by-url {no | yes} |
              unknown-categories-by-url {no | yes}
              }
           }
        threats recurring |
           {
           sync-to-peer {no | yes} |
           threshold <value> |
           daily at <value> action {download-and-install | download-only} |
           hourly at <value> action {download-and-install | download-only} |
           weekly
              {
              at <value> |
              day-of-week {friday | monday | saturday | sunday | thursday | tuesday |
                 wednesday} |
              action {download-and-install | download-only}
              }
           }
        url-database recurring
           {
           daily at <value> action download-and-install |
           weekly
              {
              at <value> |
              day-of-week {friday | monday | saturday | sunday | thursday | tuesday |
                 wednesday} |
              action download-and-install
              {
           {
        wf-private recurring |
           {
           sync-to-peer {no | yes} |
           every-15-mins {
              action {download-and-install | download-only} at <value>;
              }
           every-30-mins {
              action {download-and-install | download-only} at <value>;
              {
           every-5-mins {
              action {download-and-install | download-only} at <value>;
                 }
           every-mins {
              action {download-and-install | download-only} at <value>;
                 {
              {
           {
           }
        wildfire recurring |
           {
           sync-to-peer {no | yes} |
           every-15-mins {
              action {download-and-install | download-only} at <value>;
              }
           every-30-mins {
              action {download-and-install | download-only} at <value>;
              {
           every-hour {
              action {download-and-install | download-only} at <value>;
                 }
```

```
            every-mins {
               action {download-and-install | download-only} at <value>;
                  {
               {
            }
         }
      }
   }
```

Options

> system
  + authentication-profile — Authentication profile to use for non-local administrators (RADIUS method is supported)
  + certificate-profile — Profile for verifying client certificates
  + common-name-for-certificate — Common name recognized by devices, if different from IP address
  + default-gateway — Default gateway IP address
  + domain — Domain value
  + domain-lookup-url — Domain lookup URL
  + fqdn-forcerefresh-time — Seconds for Periodic Timer to force refresh FQDN object entries (14400-86400)
  + fqdn-refresh-time — Seconds for Periodic Timer to refresh expired FQDN object entries (600-14399)
  + hostname — Hostname value
  + ip-address — IP address for the management interface
  + ip-address-lookup-url — IP address lookup URL
  + ipv6-address — IPv6/netmask for the management interface
  + ipv6-default-gateway — IPv6 for the default gateway
  + locale — System default locale (US, Japan, CN, or TW)
  + login-banner — Login banner text
  + mtu — Maximum Transmission Unit (MTU) for the management interface
  + netmask — IP address or IPv6 for the management interface network mask
  + ntp-server-1 — First Network Time Protocol (NTP) server IP address
  + ntp-server-2 — Second Network Time Protocol server IP address
  + panorama-server — First Panorama server IP address or FQDN
  + panorama-server-2 — Second Panorama server IP address or FQDN
  + secure-proxy-password — Secure Proxy password to use
  + secure-proxy-port — Port for secure proxy server (1-65535)
  + secure-proxy-server — Secure Proxy server to use
  + secure-proxy-user — Secure Proxy user name to use
  + server-verification— Verify update server identity (yes or no)
  + speed-duplex — Speed and duplex for the management interface (100Mbps-full-duplex, 100Mbps-half-duplex, 10Mbps-full-duplex, 10Mbps-half-duplex, 1Gbps-full-duplex, 1Gbps-half-duplex, or auto-negotiate)
  + timezone — Time zone name (press <tab> for a list of time zones)
  + update-server — Palo Alto Networks update server
  + web-server-certificate — Certificate for secure web GUI
  > config-bundle-export-schedule — (Panorama only) Schedule for exporting configuration bundles
    + description — Description text
    + enable — Enable export
    + start-time — Time to start the scheduled export hh:mm (e.g., 03:30)
    > protocol — Protocol to use for export
      > ftp — Use FTP protocol for export
        + hostname — FTP hostname
        + passive-mode — Enable FTP Passive Mode
        + password — FTP password
        + path — FTP server path
        + port — FTP port (1-65535)

```
            + username — FTP username
        > scp — Use SCP protocol for export
            + hostname — SCP hostname
            + password — SCP password
            + path — SCP server path
            + port — SCP port (1-65535)
            + username — SCP username
> dns-setting
    > dns-proxy-object — DNS proxy object to use for resolving FQDNs
    > servers — Primary and secondary DNS servers
        + primary — Primary DNS server IP address
        + secondary — Secondary DNS server IP address
> geo-location — Device geographic location
    + latitude — Latitude coordinate
    + longitude — Longitude coordinate
> log-export-schedule — Schedule for exporting logs
    + description — description text
    + enable — Enable no or yes
    + log-type — Type of log (data, hipmatch, threat, traffic, or URL)
    + start-time — Time to start the scheduled export hh:mm (e.g. 03:30)
    > protocol — Use ftp or scp protocol for export
        + hostname — ftp hostname
        + passive-mode — Passive mode (no or yes) (ftp only)
        + password — ftp password
        + path — server path
        + port — ftp port (1-65535)
        + username — ftp username
> log-link — Link to external log (option to provide URL format of link)
> permitted-ip — Permitted IP address (x.x.x.x/y) or IPv6/netmask
> route
    > destination — Destination IP address or FQDN
        > source
            + address — Source IP address to use to reach destination
            + interface — Source interface to use to reach destination
    > service —
        crl-status — CRL servers
        dns — DNS server(s)
        email — SMTP gateway(s)
        mdm — Mobile Security Manager
        netflow — Netflow server(s)
        ntp — NTP server(s)
        paloalto-updates — Palo Alto update server
        panorama — Panorama server
        proxy — Proxy server
        radius — RADIUS server
        snmp — SNMP server(s)
        source — IPv4 source
        source-v6 — IPv6 source
        syslog — Syslog server(s)
        uid-agent — UID agent(s)
        url-updates — URL update server
        vmmonitor — VM monitor
        wildfire — WildFire service
        + address — Source IP address (value)
        + interface — Source interface (value)
> service
    + disable-http — Disable HTTP (no or yes)
    + disable-http-ocsp — Disable Online Certificate Status Protocol (OCSP) over HTTP (no or yes)
    + disable-https — Disable HTTPS (no or yes)
    + disable-icmp — Disable ICMP (no or yes)
    + disable-snmp — Disable SNMP (no or yes)
    + disable-ssh — Disable SSH (no or yes)
    + disable-telnet — Disable Telnet (no or yes)
    + disable-userid-service — Disable user ID service (no or yes)
    + disable-userid-syslog-listener-ssl — Disable user ID syslog listener service (no or yes)
    + disable-userid-syslog-listener-udp — Disable user ID UDP listener service (no or yes)
> snmp-setting
    > access-setting — Access setting version
        version v2c
            + snmp-community-string — SNMP community string value
        version v3
            > users — User name
                + authpwd — Authentication Protocol Password
                + privpwd — Privacy Protocol Password
                + view — SNMP View Name
            > views — View name
                view — OID subtree name
    > snmp-system
        + contact — Email contact information
        + location — System location
        + send-event-specific-traps — Whether to use event-specific trap definitions
> update-schedule — Schedule for downloading/installing updates
    > app-profile— Application profile database
        + sync-to-peer — Synchronize content with HA peer after download/install
        + threshold — Ignore if release date is new (1-120 hours)
        > daily — Schedule update everyday
            + action — Action (download and install or download and do not install)
            + at — Time specification hh:mm (e.g. 20:10)
        > hourly — Schedule update every hour
            + action — Action (download and install or download and do not install)
            + at — Minutes past the hour
        > weekly — Schedule update once a week
            + action — Action (download and install or download and do not install)
            + at — Time specification hh:mm (e.g. 20:10)
            + day-of-week — Day of the week (Friday, Monday, Saturday, Sunday, Thursday, Tuesday, Wednesday)
    > anti-virus — Anti-virus database
        + sync-to-peer — Synchronize content with HA peer after download/install
        + threshold — Ignore if release date is new (1-120 hours)
        > daily — Schedule update everyday
            + action — Action (download and install or download and do not install)
            + at — Time specification hh:mm (e.g. 20:10)
        > hourly — Schedule update every hour
            + action — Action (download and install or download and do not install)
            + at — Minutes past the hour
        > weekly — Schedule update once a week
            + action — Action (download and install or download and do not install)
            + at — Time specification hh:mm (e.g. 20:10)
            + day-of-week — Day of the week (Friday, Monday, Saturday, Sunday, Thursday, Tuesday, Wednesday)
```

```
> global-protect-datafile — GlobalProtect data file update
    > daily — Schedule update everyday
        + action — Action (download and install)
        + at — Time specification hh:mm (e.g. 20:10)
    > hourly — Schedule update every hour
        + action — Action (download and install)
        + at — Minutes past the hour
    > weekly — Schedule update once a week
        + action — Action (download and install)
        + at — Time specification hh:mm (e.g. 20:10)
        + day-of-week — Day of the week (Friday, Monday, Saturday, Sunday, Thursday, Tuesday, Wednesday)
> statistics-service — Participates in anonymous statistics upload service
    > application-and-threat-reports — Uploads application and/or threat report statistics
        + application-usage — Application usage statistics (no or yes)
        + attackers — Threats by destination ports (no or yes)
        + attacking-countries — Threats by attacking countries (no or yes)
    > device — Uploads device statistics
        + software-crash-info — Back traces of crashes (no or yes)
    > unknown-application-reports — Uploads unknown application reports statistics
        + unknown-applications-by-destination-addresses — Unknown applications by destination IP addresses (no or yes)
        + unknown-applications-by-destination-ports — Unknown applications by destination ports (no or yes)
    > url-reports — Uploads URL reports statistics
        + dataplane-cache-url — Upload dataplane cache URLs (no or yes)
        + malware-categories-by-url — Upload malware categories by URLs (no or yes)
        + unknown-categories-by-url — Upload unknown categories by URLs (no or yes)
> threats — Threat-detection database
    + sync-to-peer — Synchronize content with HA peer after download/install
    + threshold — Ignore if release date is new (1-120 hours)
    > daily — Schedule update everyday
        + action — Action (download and install or download and do not install)
        + at — Time specification hh:mm (e.g. 20:10)
    > weekly — Schedule update once a week
        + action — Action (download and install or download and do not install)
        + at — Time specification hh:mm (e.g. 20:10)
        + day-of-week — Day of the week (Friday, Monday, Saturday, Sunday, Thursday, Tuesday, Wednesday)
> url-database — URL filtering database (for BrightCloud only)
    > daily — Schedule update everyday
        + action — Action (download and install)
        + at — Time specification hh:mm (e.g. 20:10)
    > weekly — Schedule update once a week
        + action — Action (download and install)
        + at — Time specification hh:mm (e.g. 20:10)
        + day-of-week — Day of the week (Friday, Monday, Saturday, Sunday, Thursday, Tuesday, Wednesday)
> wildfire — Wildfire database
    + sync-to-peer — Synchronize content with HA peer after download/install
    + threshold — Ignore if release date is new (1-120 hours)
    > daily — Schedule update everyday
        + action — Action (download and install or download and do not install)
        + at — Time specification hh:mm (e.g. 20:10)
    > hourly — Schedule update every hour
        + action — Action (download and install or download and do not install)
        + at — Minutes past the hour
    > weekly — Schedule update once a week
```

+ action — Action (download and install or download and do not install)
+ at — Time specification hh:mm (e.g. 20:10)
+ day-of-week — Day of the week (Friday, Monday, Saturday, Sunday, Thursday, Tuesday, Wednesday)

Required Privilege Level

superuser, vsysadmin, deviceadmin

set display-name

Configures a system name that will be used as an identifier in other commands.

Syntax

```
set display-name <name>
```

Options

<name> — Specifies the display name for the system

Required Privilege Level

superuser, vsysadmin, deviceadmin

set email-scheduler

Specifies settings for email delivery of PDF summary reports.

Syntax

```
set email-scheduler <name>
   {
   email-profile <value> |
   recipient-emails <value> |
   report-group <value> |
   recurring
     {
     weekly {friday | monday | saturday | sunday | thursday | tuesday | wednesday} |
     daily |
     disabled
     }
   }
```

Options

<name> — Specifies the name for the email scheduler
+ email-profile — Email profile value
+ recipient-emails — Recipient emails value
+ report-group — Report group value
> recurring — Recurring frequency
    > weekly — Once a week; specify the day
    - daily — Every day
    - disabled — No scheduling

Required Privilege Level

superuser, vsysadmin, deviceadmin

set external-list

Specifies settings for external lists of blocked sites. Managed devices can import the list on a scheduled basis. The source of a list can be a file server or web server. After specifying a dynamic block list object, you can then use it as a source or destination for security policies.

Syntax

```
set external-list <name>
   {
   description <value> |
   type ip |
   url <value> |
   recurring
     {
     daily at <value> |
     hourly at <value> |
     monthly {at <value> | day-of-month <value>} |
     weekly {at <value> | day-of-week <value>}
     }
   }
```

Options

<name> — Specifies the name for the external list
+ description — Description of the object
+ type — Specifies type of list (IP addresses)
+ url — URL or server path to the list
> recurring — Schedule for importing the list
   > daily — Recurring every day, time specification hh:mm (e.g. 20:10)
   > hourly — Recurring every hour, time specification mm (e.g. 10)
   > monthly — Recurring monthly
     + at — Time specification hh:mm (e.g. 20:10)
     + day-of-month — Day of the month (1-31)
   > weekly — Recurring once a week
     + at — Time specification hh:mm (e.g. 20:10)
     + day-of-month — Day of the week (Friday, Monday, Saturday, Sunday, Thursday, Tuesday, Wednesday)

Required Privilege Level

superuser, vsysadmin, deviceadmin

set global-protect

Configures GlobalProtect on the firewall. GlobalProtect provides security for client systems, such as laptops, that are used in the field by allowing easy and secure login from anywhere in the world.

For more information, refer to the *GlobalProtect Administrator's Guide*.

Syntax

```
set global-protect
   {
   global-protect-gateway <name> |
      {
      authentication-profile <value> |
      certificate-profile <value> |
      remote-user-tunnel <value> |
      satellite-tunnel <value> |
      server-certificate <value> |
      tunnel-mode {no | yes} |
      hip-notification <name> {match-message <value> | not-match-message <value>} |
      local-address |
         {
         interface <value> |
         floating-ip <ip_address> |
         ip <ip_address>
         }
      roles default
         {
         inactivity-logout {days | hours | minutes} |
         login-lifetime {days | hours | minutes}
         }
      }
   global-protect-mdm <name> |
      {
      client-certificate <value> |
      disabled {no | yes} |
      host <value> |
      port <value> |
      root-ca <value> |
      }
   global-protect-portal <name> |
      {
      client-config |
         {
         agent-user-override-key <value> |
         client-certificate <value> |
         configs <value>
            {
            client-certificate {my-fwd-trust | my-fwd-untrust} |
            connect-method {on-demand | pre-logon | user-logon} |
            mdm-address <value> |
            mdm-enrollment-port <value> |
            refresh-config {no | yes} |
            refresh-config-interval <value> |
            use-sso {no | yes} |
            agent-config |
                {
                can-continue-if-portal-cert-invalid {no | yes};
                client-upgrade {disabled | manual | prompt | transparent};
                rediscover-network {no | yes};
                resubmit-host-info {no | yes};
                }
            agent-ui |
                {
                agent-user-override {disabled | with-comment | with-passcode | with-
                   ticket} |
                agent-user-override-timeout <value> |
                can-change-portal {no | yes} |
                can-save-password {no | yes} |
                enable-advanced-view {no | yes} |
                max-agent-user-overrides <value> |
                passcode <value> |
                show-agent-icon {no | yes} |
                welcome-page
                   {
                   display {no | yes} |
                   page <value>
                   }
                }
            authentication-modifier
                {
                cookie-auth-config-refresh cookie lifetime <value> |
                diff-passwd-ext-gateway-conn manual-gateway-only {no | yes}
                }
            gateways |
                {
                cutoff-time <value> |
                external list <value> {priority <value>} |
                internal list <value>
                }
            hip-collection |
                {
                max-wait-time <value> |
                custom-checks |
                   {
                   mac-os |
                      {
                      plist <name> key <value> |
                      process-list <member_value>
                      }
                   windows
                      {
                      process-list <member_value> |
                      registry-key <name> registry-value <value>
                      }
                exclusion category {anti-spyware | antivirus | disk-backup | disk-
```

```
                  encryption | firewall | patch-management}
                  {
                  vendor <name> |
                  product <name>
                  }
               }
            internal-host-detection
               {
               hostname <value> |
               ip-address <ip_address>
               }
            os <value> |
            source-user {any | pre-logon | <value>} |
            third-party-vpn-clients <member_value> |
            }
         root-ca <value> |
         }
      portal-config |
         {
         authentication-profile <value> |
         certificate-profile <value> |
         custom-help-page {factory-default | <value>} |
         custom-login-page {factory-default | <value>} |
         server-certificate <value> |
         local-address
            {
            interface <value> |
            floating-ip <ip_address> |
            ip <ip_address>
            }
         }
      satellite-config
         {
         certificate-life-time <value> |
         certificate-renewal-period <value> |
         issuing-certificate <value> |
         ocsp-responder <value> |
         configs |
            {
            config-refresh-interval <value> |
            devices <value> |
            gateways <value> {description <value> | priority <value>} |
            source-user {any | <value>}
            }
         root-ca <value>
         }
      }
    redirect {location <value> | off | on}
    }
```

Options

> global-protect-gateway — GlobalProtect gateway configuration

    + authentication-profile — Authentication profile used for this GlobalProtect gateway

```
    + certificate-profile — Profile for authenticating client certificates
    + remote-user-tunnel — GlobalProtect user tunnel
    + satellite-tunnel — GlobalProtect satellite tunnel
    + server-certificate — SSL server certificate file name
    + tunnel-mode — Tunnel mode configuration
    > hip-notification — Host PC health evaluation
       + match-message — Display message for matching result
       + not-match-message — Display message for non-matching result
    > local-address — Local IP configuration
       + interface — Local gateway end-point
       > floating-ip — Floating IP address in HA Active-Active configuration
       > ip — Specify exact IP address if interface has multiple addresses
    > roles — Role-based user management for GlobalProtect gateway users
       > inactivity-logout — GlobalProtect gateway session timeout due to inactivity
          > days — Specify lifetime in days (1-30)
          > hours — Specify lifetime in hours (1-720)
          > minutes — Specify lifetime in minutes (3-43200)
       > login-lifetime — GlobalProtect gateway  user login lifetime before re-authentication
          > days — Specify lifetime in days (1-3650)
          > hours — Specify lifetime in hours (1-87600)
          > minutes — Specify lifetime in minutes (3-5256000)
> global-protect-mdm — GlobalProtect Mobile Security Manager configuration
    + client-certificate — Specify client certificate
    + disabled — Specify whether configuration is disabled (yes or no)
    + host — Specify IP address or hostname for GlobalProtect Mobile Security Manager
    + port — Specifies the port on which the Mobile Security Manager listens for gateway connections. Do not change this port
       from the default.
    + root-ca — Specifies the root CA certificate for the Mobile Security Manager, if the gateway does not trust it.
> global-protect-portal — GlobalProtect portal configuration
    > client-config — Portal client configuration
       + agent-user-override-key — Agent user override ticket key
       + client-certificate — SSL client certificate
       > configs — GlobalProtect portal client configurations
          + client-certificate — SSL client certificate
          + connect-method — Gateway connect method (on-demand, pre-logon, or user-logon)
          + mdm-address — IP address or hostname for GlobalProtect Mobile Security Manager
          + mdm-enrollment-port — Mobile Security Manager enrollment port
          + refresh-config — Enable portal configuration refresh
          + refresh-config-interval — Interval for refreshing portal configuration (1-168)
          + use-sso — Use single sign-on
          > agent-config — GlobalProtect agent configuration
             + can-continue-if-portal-cert-invalid — Can continue if portal certificate is invalid
             + client-upgrade — GlobalProtect agent upgrade mode (disabled, manual, prompt, or transparent)
             + rediscover-network — Enable agent rediscover network
             + resubmit-host-info — Enable agent resubmit host info
          > agent-ui — Agent user interface configuration
             + agent-user-override — Agent override policy (disabled, with comment, with passcode, or with ticket)
             + agent-user-override-timeout — Agent user override duration, in minutes (0-65535)
             + can-change-portal — User can change portal address
             + can-save-password — User can save password
             + enable-advanced-view — Enable advanced view
             + max-agent-user-overrides — Max agent user overrides (0-65535)
             + passcode — Passcode required for override
             + show-agent-icon — Show GlobalProtect icon
```

```
            > welcome-page — Agent login welcome page
                + display — Enable display of response page
                + page — Specify page location
        > authentication-modifier — Modification of authentication
            > cookie-auth-config-refresh — Use cookie authentication for config refresh (specify number of days for cookie-lifetime)
            > diff-passwd-ext-gateway-conn — Use different password for external gateway connection (specify no or yes for manual-gateway)
             none— No authentication modifier
        > gateways — GlobalProtect gateways configuration
            + cutoff-time — Gateway discovery cutoff time, in seconds (0-10)
            > external — External gateways
                > list — IP address or Fully Qualified Domain Name (FQDN) host name (x.x.x.x/y or IPv6/netmask or host name or list of values enclosed in [ ])
                    + priority — Priority of GlobalProtect gateway (1-5)
            > internal — Internal gateways
                > list — IP address or Fully Qualified Domain Name (FQDN) host name (x.x.x.x/y or IPv6/netmask or host name or list of values enclosed in [ ])
        > hip-collection — Host information profile collection instructions
            + max-wait-time — Max wait time for HIP collection to complete, in seconds (10-60)
            > custom-checks — Custom checks by operating system
                > mac-os — Mac OS-specific custom checks
                    > plist — Preference list name
                        + key — Key value (member value or list of values enclosed in [ ])
                    + process-list — Process list (member value or list of values enclosed in [ ])
                > windows — Windows-specific custom checks
                    + process-list — Process list (member value or list of values enclosed in [ ])
                    > registry-key — Registry key name
                        + registry-value — Registry value (member value or list of values enclosed in [ ])
            > exclusion — Exclusion categories
                > category — Category name (anti-spyware, antivirus, disk backup, disk encryption, firewall, or patch management)
                    > vendor — Vendor name (press <tab> for list)
                        + product — Product name (member value or list of values enclosed in [ ])
        > internal-host-detection — Internal host detection settings
            + hostname — Host name of the IP in DNS record
            + ip-address — Internal IP address of a host (x.x.x.x)
        > source-user — Source user (any, pre-logon client machine, or specify user or list of users enclosed in [ ])
        > third-party-vpn-clients — Third party VPN clients configuration; specify member value or list of values enclosed in [ ]
    > root-ca — Trusted CAs of gateways; specify value or list of values enclosed in [ ]
> portal-config — Portal configuration
    + authentication-profile — Authentication profile used for this GlobalProtect
    + client-certificate-profile — Profile for authenticating client certificates
    + custom-help-page — Custom help page; select factory default or enter a value
    + custom-login-page — Custom login page; select factory default or enter a value
    + server-certificate — SSL server certificate file name
    > local-address — Local IP configuration
        + interface — Local gateway end-point
        > floating-ip — Floating IP address in HA Active-Active configuration
        > ip — Specify exact IP address if interface has multiple addresses
> satellite-config — Satellite configuration
    + certificate-life-time — Issued GlobalProtect satellite certificate lifetime, in days (7-365)
    + certificate-renewal-period — GlobalProtect satellite certificate renewal period, in days (3-30)
```

```
        + issuing-certificate — Issuing certificate to issue GlobalProtect satellite certificate
        + ocsp-responder — Online Certificate Status Protocol (OCSP) responder
        > configs — GlobalProtect satellite per device|user|user group configuration
            + config-refresh-interval — GlobalProtect satellite configuration refresh interval, in hours (1-48)
            > devices — GlobalProtect satellite PAN device serial number or list of values enclosed in [ ]
            > gateways — GlobalProtect gateways (IP or FQDN)
                + description — User-friendly description of the gateway
                + priority — Priority of GlobalProtect gateway (1-25)
            > source-user — Source user (any or list of values enclosed in [ ])
        > root-ca — Trusted CAs of gateways; specify value or list of values enclosed in [ ]
> redirect — GlobalProtect portal configuration
    > location — Location to fetch GlobalProtect Agent binary file (path: http://host/directory-path)
    > off — Disables redirect (allows Agent download from GlobalProtect Portal only)
    > on — Enables hosting GlobalProtect Agent download files on a server other than the GlobalProtect Portal
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set group-mapping

Configures group mapping and Lightweight Directory Access Protocol (LDAP) settings for use in authentication profiles.

Syntax

```
set group-mapping <name>
   {
   disabled {no | yes} |
   group-filter <value> |
   server-profile <name> |
   update-interval <value> |
   user-filter <value> |
   container-object <value> |
   group-include-list <value> |
   group-member <member_value> |
   group-name <member_value> |
   group-object <member_value> |
   last-modify-attr <member_value> |
   user-name <member_value> |
   user-object <member_value>
   }
```

Options

<name> — Specifies the LDAP server group mapping
+ disabled — Disabled (no or yes)
+ group-filter — LDAP search filter for group
+ server-profile — LDAP server object name
+ update-interval — Interval for updating group membership, in seconds (60-86400; default = 3600 seconds)
+ user-filter — LDAP search filter for user
> container-object — Container object class
> group-include-list — Specify the list of user groups to include in the policy (value or list of values enclosed in [ ])
> group-member — Group member attribute (value or list of values enclosed in [ ])
> group-name — Group name attribute (value or list of values enclosed in [ ])
> group-object — Group object class (value or list of values enclosed in [ ])
> last-modify-attr — Last modify timestamp attribute
> user-name — User name attribute (value or list of values enclosed in [ ])
> user-object — User object class (value or list of values enclosed in [ ])

Required Privilege Level

superuser, vsysadmin, deviceadmin

set log-collector

(Panorama only) Configures distributed log collecting across devices, managed by Panorama.

For more information, refer to the *Panorama Administrator's Guide*.

Syntax

```
set log-collector <name>
   {
   authentication-setting |
     {
     admin-lockout {failed-attempts <value> | lockout-time <value>} |
     users admin {phash <value>}
     }
   deviceconfig system |
     {
     default-gateway <ip_address> |
     domain <value> |
     hostname <value> |
     ip-address <ip_address> |
     ipv6-address <ip/netmask> |
     ipv6-default-gateway <value> |
     login-banner <value> |
     netmask <value> |
     mtu <value> |
     ntp-server-1 <value> |
     ntp-server-2 <value> |
     panorama-server <value> |
     panorama-server-2 <value> |
     speed-duplex <value> |
     syslog certificate <value> |
     timezone <value> |
     dns-setting servers {primary <value> | secondary <value>} |
     eth1 |
        {
        + default-gateway <value> |
        + ip-address <value> |
        + ipv6-address <value> |
        + ipv6-default-gateway <value> |
        + mtu <value> |
        + netmask <value> |
        + speed-duplex <value> |
        > permitted-ip <value> |
        > service
           {
           disable-icmp {no | yes} |
           }
        }
     eth2 |
        {
        + default-gateway <value> |
        + ip-address <value> |
        + ipv6-address <value> |
        + ipv6-default-gateway <value> |
        + mtu <value> |
        + netmask <value> |
        + speed-duplex <value> |
        > permitted-ip <value> |
        > service
           {
           disable-icmp {no | yes} |
           }
        }
     geo-location |
        {
        latitude <coordinate> |
        longitude <coordinate>
        }
     logging-functions
        {
        collector-group-communication {mgt | <value>} |
        device-log-collection {mgt | <value>} |
        }
     permitted-ip <value> |
     service
        {
        disable-icmp {no | yes} |
        disable-snmp {no | yes} |
        disable-ssh {no | yes} |
        }
  disk-settings disk-pair <value> |
  }
```

Options

<name> — Specifies the log collector device
> authentication-setting — Authentication settings
    > admin-lockout — Administrative login lockout settings
        + failed-attempts — Number of failed login attempts to trigger lock-out (0-10)
        + lockout-time — Number of minutes to lock-out (0-60)
    > users — Admin users
        + phash — Password hash value
> deviceconfig — Device system configurations
    + default-gateway — Default gateway IP address
    + domain — Domain value
    + hostname — Hostname value
    + ip-address — IPv4 address for the management interface
    + ipv6-address — IPv6/netmask for the management interface
    + ipv6-default-gateway — IPv6 for the default gateway
    + login-banner — Login banner text
    + netmask — IPv4 network mask for the management interface
    + mtu — Maximum Transmission Unit (MTU) for the management interface
    + ntp-server-1 — First Network Time Protocol (NTP) server IP address
    + ntp-server-2 — Second Network Time Protocol server IP address
    + panorama-server — First Panorama server IP address or FQDN

```
    + panorama-server-2 — Second Panorama server IP address or FQDN
    + speed-duplex — Speed and duplex for the management interface (100Mbps-full-duplex, 100Mbps-half-duplex, 10Mbps-
       full-duplex, 10Mbps-half-duplex, 1Gbps-full-duplex, 1Gbps-half-duplex, or auto-negotiate)
    + syslog-certificate — The certificate for secure forwarding of logs to an external syslog server.
    + timezone — Time zone name (press <tab> for a list of time zones)
    > dns-setting — Device DNS settings
       > servers — Primary and secondary DNS servers
          + primary — Primary DNS server IP address
          + secondary — Secondary DNS server IP address
    > eth1 — Settings of the eth1 interface
       + default-gateway — IPv4 address of the default gateway for the eth1 interface
       + ip-address — IPv4 address for the eth1 interface
       + ipv6-address — IPv6 address for the eth1 interface
       + ipv6-default-gateway — IPv6 address of the default gateway for the eth1 interface
       + mtu — Maximum Transmission Unit (MTU) for the eth1 interface
       + netmask — IPv4 netmask for the eth1 interface
       + speed-duplex — Speed and duplex for the eth1 interface
       > permitted-ip — IP addresses that can access the eth1 interface
       > service — Enable or disable services for eth1 interface
          + disable-icmp — Disables Internet Control Message Protocol (ICMP) for the eth1 interface
    > eth2 — Settings of the eth2 interface
       + default-gateway — IPv4 address of the default gateway for the eth2 interface
       + ip-address — IPv4 address for the eth2 interface
       + ipv6-address — IPv6 address for the eth2 interface
       + ipv6-default-gateway — IPv6 address of the default gateway for the eth2 interface
       + mtu — Maximum Transmission Unit (MTU) for the eth2 interface
       + netmask — IPv4 netmask for the eth2 interface
       + speed-duplex — Speed and duplex for the eth2 interface
       > permitted-ip — IP addresses that can access the eth2 interface
       > service — Enable or disable services for eth2 interface
          + disable-icmp — Disables Internet Control Message Protocol (ICMP) for the eth2 interface
    > geo-location — Device geographic location
       + latitude — Latitude coordinate
       + longitude — Longitude coordinate
    > logging-functions — Interfaces for log collection and communication among Collector Groups
       + collector-group-communication — Assign an interface (mgmt, eth1, or eth2) for Collector Group communication
       + device-log-collection — Assign an interface (mgmt, eth1, or eth2) for log collection
    > permitted-ip — Permitted IP address (x.x.x.x/y) or IPv6/netmask
    > service — Device services settings
       + disable-icmp — Disable ICMP (no or yes)
       + disable-snmp — Disable SNMP (no or yes)
       + disable-ssh — Disable SSH (no or yes)
> disk-settings — Disk pair settings
    > disk-pair — Set/delete RAID disk pair number (A-D)
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set log-collector-group

(Panorama only) Defines log collector groups under Panorama management. Collector groups are used to assign Panorama-managed firewalls to log collectors that will be used to offload the work of log collection that would normally be handled by the Panorama management server.

For more information, refer to the *Panorama Administrator’s Guide*.

Syntax

```
set log-collector-group {default | <name>}
   {
   general-setting management |
     {
     min-retention-period <value> |
     disk-quota
        {
        alarm <value> |
        appstat <value> |
        config <value> |
        dailythsum <value> |
        dailytrsum <value>
        hipmatch <value> |
        hourlythsum <value> |
        hourlytrsum <value>
        system <value> |
        threat <value> |
        thsum <value> |
        traffic <value> |
        trsum <value>
        weeklythsum <value> |
        weeklytrsum <value>
        }
     }
   log-settings |
     {
     config |
        {
        any |
           {
           send-email |
              {
              using-email-setting {PAN_Email | <value>} |
              }
           send-snmptrap |
              {
              using-snmptrap-setting {PAN_SNMP | <value>} |
              }
           send-syslog |
              {
              using-syslog-setting {PAN_Syslog | <value>} |
              }
```

```
            }
         }
      email <name> |
      hipmatch |
         {
         any |
            {
            send-email |
               {
               using-email-setting {PAN_Email | <value>} |
               }
            send-snmptrap |
               {
               using-snmptrap-setting {PAN_SNMP | <value>} |
               }
            send-syslog |
               {
               using-syslog-setting {PAN_Syslog | <value>} |
               }
            }
         }
      snmptrap <name> |
      syslog <name> |
      system |
         {
         critical |
            {
            send-email |
               {
               using-email-setting {PAN_Email | <value>} |
               }
            send-snmptrap |
               {
               using-snmptrap-setting {PAN_SNMP | <value>} |
               }
            send-syslog |
               {
               using-syslog-setting {PAN_Syslog | <value>} |
               }
            }
         high |
            {
            send-email |
               {
               using-email-setting {PAN_Email | <value>} |
               }
            send-snmptrap |
               {
               using-snmptrap-setting {PAN_SNMP | <value>} |
               }
            send-syslog |
               {
               using-syslog-setting {PAN_Syslog | <value>} |
               }
            }
         informational |
            {
            send-email |
               {
               using-email-setting {PAN_Email | <value>} |
               }
            send-snmptrap |
               {
               using-snmptrap-setting {PAN_SNMP | <value>} |
               }
            send-syslog |
               {
               using-syslog-setting {PAN_Syslog | <value>} |
               }
            }
         low |
            {
            send-email |
               {
               using-email-setting {PAN_Email | <value>} |
               }
            send-snmptrap |
               {
               using-snmptrap-setting {PAN_SNMP | <value>} |
               }
            send-syslog |
               {
               using-syslog-setting {PAN_Syslog | <value>} |
               }
            }
         medium |
            {
            send-email |
               {
               using-email-setting {PAN_Email | <value>} |
               }
            send-snmptrap |
               {
               using-snmptrap-setting {PAN_SNMP | <value>} |
               }
            send-syslog |
               {
               using-syslog-setting {PAN_Syslog | <value>} |
               }
            }
         }
      threat |
         {
         critical |
            {
            send-email |
               {
               using-email-setting {PAN_Email | <value>} |
            }
        send-snmptrap |
            {
            using-snmptrap-setting {PAN_SNMP | <value>} |
            }
        send-syslog |
            {
            using-syslog-setting {PAN_Syslog | <value>} |
            }
        }
    high |
        {
        send-email |
            {
            using-email-setting {PAN_Email | <value>} |
            }
        send-snmptrap |
            {
            using-snmptrap-setting {PAN_SNMP | <value>} |
            }
        send-syslog |
            {
            using-syslog-setting {PAN_Syslog | <value>} |
            }
        }
    informational |
        {
        send-email |
            {
            using-email-setting {PAN_Email | <value>} |
            }
        send-snmptrap |
            {
            using-snmptrap-setting {PAN_SNMP | <value>} |
            }
        send-syslog |
            {
            using-syslog-setting {PAN_Syslog | <value>} |
            }
        }
    low |
        {
        send-email |
            {
            using-email-setting {PAN_Email | <value>} |
            }
        send-snmptrap |
            {
            using-snmptrap-setting {PAN_SNMP | <value>} |
            }
        send-syslog |
            {
            using-syslog-setting {PAN_Syslog | <value>} |
            }
```

```
      }
   medium |
      {
      send-email |
         {
         using-email-setting {PAN_Email | <value>} |
         }
      send-snmptrap |
         {
         using-snmptrap-setting {PAN_SNMP | <value>} |
         }
      send-syslog |
         {
         using-syslog-setting {PAN_Syslog | <value>} |
         }
      }
   }
traffic |
   {
   any |
      {
      send-email |
         {
         using-email-setting {PAN_Email | <value>} |
         }
      send-snmptrap |
         {
         using-snmptrap-setting {PAN_SNMP | <value>} |
         }
      send-syslog |
         {
         using-syslog-setting {PAN_Syslog | <value>} |
         }
      }
   }
wildfire |
   {
   benign |
      {
      send-email |
         {
         using-email-setting {PAN_Email | <value>} |
         }
      send-snmptrap |
         {
         using-snmptrap-setting {PAN_SNMP | <value>} |
         }
      send-syslog |
         {
         using-syslog-setting {PAN_Syslog | <value>} |
         }
      }
   malicious |
      {
             send-email |
                {
                using-email-setting {PAN_Email | <value>} |
                }
             send-snmptrap |
                {
                using-snmptrap-setting {PAN_SNMP | <value>} |
                }
             send-syslog |
                {
                using-syslog-setting {PAN_Syslog | <value>} |
                }
             }
          }
       }
    logfwd-setting |
       {
       collectors <value> |
       devices <value>
       }
    monitoring-setting
       {
       snmp-setting |
          {
          access-setting version |
             {
             v2c snmp-community-string <value> |
             v3
                {
                users <user_name> |
                   {
                   authpwd <value> |
                   privpwd <value> |
                   view <value>
                   }
                views <view_name> view <value>
                   {
                   mask <value> |
                   oid <value> |
                   option {exclude | include}
                   }
                }
          snmp-system
             {
             contact <value> |
             location <value> |
             }
          }
       }
    }
```

Options

<name> — Specifies the log collector group

```
> general-setting      general-setting
      + min-retention-period   Minimum retention period in days before purging oldest logs (1-30)
      > disk-quota — Quotas for logs (percentages between 0 and 90.0)
          + alarm — Alarm logs quota percentage
          + appstat — Application statistics quota percentage
          + config — Configuration logs quota percentage
          + dailythsum — Daily threat summary quota percentage
          + dailytrsum — Daily traffic summary quota percentage
          + hipmatch — HIP match quota percentage
          + hourlythsum — Hourly threat summary quota percentage
          + hourlytrsum — Hourly traffic summary quota percentage
          + system — System logs quota percentage
          + threat — Threat logs quota percentage
          + thsum — Threat summary quota percentage
          + traffic — Traffic logs quota percentage
          + trsum — Traffic summary quota percentage
          + weeklythsum — Weekly threat summary quota percentage
          + weeklytrsum — Weekly traffic summary quota percentage
> logfwd-setting — Settings for forwarding logs from firewalls to Panorama
      > collectors — List of serial numbers of preferred primary Log Collectors belonging to this Collector Group
      > devices — The serial numbers of the firewalls assigned to the Log Collectors in this Collector Group
> log-settings — Settings for log forwarding to external services
      > config any — The external servers to which Panorama forwards the configuration logs that firewalls send to the Collector
          Group.
          > send-email using-email-setting — The server profile name of the email server to which Panorama forwards the
               configuration logs that firewalls send to the Collector Group.
          > send-snmptrap using-snmptrap-setting — The server profile name of the SNMP trap server to which Panorama
               forwards the configuration logs that firewalls send to the Collector Group.
          > send-syslog using-syslog-setting — The server profile name of the Syslog server to which Panorama forwards the
               configuration logs that firewalls send to the Collector Group.
      > email — The server profile name of the email server to which Panorama forwards the logs that firewalls send to the
          Collector Group.
      > hipmatch any — The external servers to which Panorama forwards the Host Information Profile (HIP) logs that firewalls
          send to the Collector Group.
          > send-email using-email-setting — The server profile name of the email server to which Panorama forwards the HIP
               match logs that firewalls send to the Collector Group.
          > send-snmptrap using-snmptrap-setting — The server profile name of the SNMP trap server to which Panorama
               forwards the HIP match logs that firewalls send to the Collector Group.
          > send-syslog using-syslog-setting — The server profile name of the Syslog server to which Panorama forwards the HIP
               match logs that firewalls send to the Collector Group.
      > snmptrap — The server profile name of the Simple Network Management Protocol (SNMP) trap server to which Panorama
          forwards the logs that firewalls send to the Collector Group.
      > syslog — The server profile name of the Syslog server to which Panorama forwards the logs that firewalls send to the
          Collector Group.
      > system — The external servers to which Panorama forwards the system logs that firewalls send to the Collector Group. You
          can specify a server for each log level: critical, high, informational, low, or medium.
          > send-email using-email-setting — The server profile name of the email server to which Panorama forwards the system
               logs that firewalls send to the Collector Group.
          > send-snmptrap using-snmptrap-setting — The server profile name of the SNMP trap server to which Panorama
               forwards the system logs that firewalls send to the Collector Group.
          > send-syslog using-syslog-setting — The server profile name of the Syslog server to which Panorama forwards the
               system logs that firewalls send to the Collector Group.
      > threat — The external servers to which Panorama forwards the threat logs that firewalls send to the Collector Group. You
          can specify a server for each log level: critical, high, informational, low, or medium.
```

```
        > send-email using-email-setting — The server profile name of the email server to which Panorama forwards the threat logs that firewalls send to the Collector Group.
        > send-snmptrap using-snmptrap-setting — The server profile name of the SNMP trap server to which Panorama forwards the threat logs that firewalls send to the Collector Group.
        > send-syslog using-syslog-setting — The server profile name of the Syslog server to which Panorama forwards the threat logs that firewalls send to the Collector Group.
    > traffic any — The external servers to which Panorama forwards the traffic logs that firewalls send to the Collector Group.
        > send-email using-email-setting — The server profile name of the email server to which Panorama forwards the traffic logs that firewalls send to the Collector Group.
        > send-snmptrap using-snmptrap-setting — The server profile name of the SNMP trap server to which Panorama forwards the traffic logs that firewalls send to the Collector Group.
        > send-syslog using-syslog-setting — The server profile name of the Syslog server to which Panorama forwards the traffic logs that firewalls send to the Collector Group.
    > wildfire — The external servers to which Panorama forwards the WildFire logs that firewalls send to the Collector Group. You can specify a server for each log type: benign or malicious.
        > send-email using-email-setting — The server profile name of the email server to which Panorama forwards the WildFire logs that firewalls send to the Collector Group.
        > send-snmptrap using-snmptrap-setting — The server profile name of the SNMP trap server to which Panorama forwards the WildFire logs that firewalls send to the Collector Group.
        > send-syslog using-syslog-setting — The server profile name of the Syslog server to which Panorama forwards the WildFire logs that firewalls send to the Collector Group.
> monitoring-setting — Monitoring settings
    > snmp-setting
        > access-setting — Access setting version
            version v2c
                + snmp-community-string — SNMP community string value
            version v3
                > users — User name
                    + authpwd — Authentication Protocol Password
                    + privpwd — Privacy Protocol Password
                    + view — SNMP View Name
                > views — View name
                    view — OID subtree name
                        + mask — Subtree mask in hex
                        + oid — OID of a MIB node
                        + option — Exclude/include option
        > snmp-system
            + contact — Email contact information
            + location — System location
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set mgt-config

Configures management accounts on the firewall.

Syntax

```
set mgt-config
   {
   access-domain <name> {vsys <name>} |
   devices <serial_number> |
     {
     disable-config-backup {no | yes} |
     hostname <value> |
     ip <value>
     }
   password-complexity |
     {
     block-repeated-characters <value> |
     block-username-inclusion {no | yes} |
     enabled {no | yes} |
     minimum-length <value> |
     minimum-lowercase-letters <value> |
     minimum-numeric-letters <value> |
     minimum-special-characters <value> |
     minimum-uppercase-letters <value> |
     new-password-differs-by-characters <value> |
     password-change-on-first-login {no | yes} |
     password-change-period-block <value> |
     password-history-count <value> |
     password-change
        {
        expiration-period <value> |
        expiration-warning-period <value> |
        post-expiration-admin-login-count <value> |
        post-expiration-grace-period <value>
        }
     }
   password-profile <name> |
     {
     password-change
        {
        expiration-period <value> |
        expiration-warning-period <value> |
        post-expiration-admin-login-count <value> |
        post-expiration-grace-period <value>
        }
     }
   users <name>
     {
     authentication-profile <profile_name> |
     client-certificate-only {no | yes} |
     password-profile <value> |
     public-key <value> |
     permissions role-based |
        {
        deviceadmin <name> |
        devicereader <name> |
        custom |
           {
           profile <name> |
           vsys <name>
           }
        superreader yes |
        superuser yes |
        vsysadmin <name> {vsys <name> | [list of values]} |
        vsysreader <name> {vsys <name> | [list of values]}
        }
     phash <value> |
     preferences |
        {
        disable-dns {no | yes} |
        saved-log-query
           {
           alarm <name> query <query_value> |
           config <name> query <query_value> |
           data <name> query <query_value> |
           system <name> query <query_value> |
           threat <name> query <query_value> |
           traffic <name> query <query_value> |
           url <name> query <query_value>
           }
        }
     password
  }
```

Options

> access-domain — Groups used for restricting administrative access
   + vsys — Virtual system name or list of values enclosed in [ ]
> devices — (Panorama only) Device serial number
   + disable-config-backup — Enable config back up for this device
   + hostname — Device ost name
   + ip — Device IP address
> password-complexity — Password complexity settings
   + block-repeated-characters — Block repeated characters count (0-15)
   + block-username-inclusion — Block inclusion of username and it's reverse
   + enabled — Enable minimal password complexity enforcement
   + minimum-length — Minimum password length (0-15)
   + minimum-lowercase-letters — Minimum lowercase letters in the password (0-15)
   + minimum-numeric-letters — Minimum numeric characters in the password (0-15)
   + minimum-special-characters — Minimum special characters (non-alphanumeric) in the password (0-15)
   + minimum-uppercase-letters — Minimum uppercase letters in the password (0-15)
   + new-password-differs-by-characters — New Password must differ by the count chars (0-15)
   + password-change-on-first-login — Password must change on first time login
   + password-change-period-block — Password change block period, in days (0-365)
   + password-history-count — Save password history for password changes, in days (0-150)

```
  > password-change — Password change settings
    + expiration-period — Password expiry, in days (0-365)
    + expiration-warning-period — Password expiry warning period, in days (0-30)
    + post-expiration-admin-login-count — Password post-expiry admin login count (0-3)
    + post-expiration-grace-period — Password post-expiry grace period (0-30)
> password-profile — Password profile name
  > password-change — Password change settings
    + expiration-period — Password expiry, in days (0-365)
    + expiration-warning-period — Password expiry warning period, in days (0-30)
    + post-expiration-admin-login-count — Password post-expiry admin login count (0-3)
    + post-expiration-grace-period — Password post-expiry grace period (0-30)
> users — Select from the list of defined users or enter a new name
  + authentication-profile — Authentication profile or sequence name
  + client-certificate-only — Is client certificate authentication enough? (no or yes)
  + password-profile — Password profile name
  + public-key — Public key for SSH authentication
  > permissions — Role-based permissions
    + deviceadmin — Device name(s) (localhost.localdomain) or list of values enclosed in [ ]
    + devicereader — Device name(s) (localhost.localdomain) or list of values enclosed in [ ]
    > custom — Custom role-based permissions
      + profile — Select from the list of defined profiles or enter a new name
      + vsys — Virtual system name or list of values enclosed in [ ] (available only when virtual systems are enabled)
    > superreader — Assign superreader role to specified user
    > superuser — Assign superuser role to specified user
    > vsysadmin — Virtual system administrator (available only when virtual systems are enabled)
      + vsys — virtual system name(s) (localhost.localdomain) or list of values enclosed in [ ]
    > vsysreader — Virtual system reader (available only when virtual systems are enabled)
      + vsys — virtual system name(s) (localhost.localdomain) or list of values enclosed in [ ]
  > phash — phash value
  > preferences — Preferences for specified user
    + disable-dns — Disable Domain Name System (DNS)
    > saved-log-query — Query a saved log
      > alarm — Alarm log name and query value
      > config — Configuration log name and query value
      > data — Data log name and query value
      > system — System log name and query value
      > threat — Threat log name and query value
      > traffic — Traffic log name and query value
      > url — URL log name and query value
  password — Option to provide a password
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network dhcp

Configures the network Dynamic Host Configuration Protocol (DHCP) server or DHCP relay settings.

Syntax

```
set network dhcp interface <interface_value>
   {
   relay |
      {
      ip |
         {
         enabled {no | yes} |
         server <ip_address>
         }
      ipv6 server
         {
         enabled {no | yes} |
         server <ip/netmask> {interface <value>}
         }
      }
   server
      {
      mode {auto | disabled | enabled} |
      probe-ip {no | yes} |
      ip-pool {<ip_range> | <ip/netmask> | <value>} |
      option |
         {
         dns-suffix {inherited | <ip_address>} |
         gateway <ip_address> |
         pop3-server {inherited | <ip/netmask>} |
         smtp-server {inherited | <ip/netmask>} |
         dns |
            {
            primary {inherited | <ip/netmask>} |
            secondary {inherited | <ip/netmask>}
            }
         inheritance source <value> |
         lease {timeout <value> | unlimited}
         nis |
            {
            primary {inherited | <ip/netmask>} |
            secondary {inherited | <ip/netmask>}
            }
         ntp |
            {
            primary {inherited | <ip/netmask>} |
            secondary {inherited | <ip/netmask>}
            }
         wins
            {
```

```
            primary {inherited | <ip/netmask>} |
            secondary {inherited | <ip/netmask>}
            }
         }
      reserved <ip_address> {mac <mac_address>}
      }
   }
```

Options

<interface_value> — Interface for DHCP configuration

> relay — Relay configuration

> ip — DHCP IP configuration

+ enabled — Enable configuration

+ server — Relay server IP address (x.x.x.x or IPv6 or list enclosed in [ ])

> ipv6 — DHCP IPv6 configuration

+ enabled — Enable configuration

> server — Relay server IPv6 address (x.x.x.x or IPv6 or list enclosed in [ ])

+ interface — Specify outgoing interface when using an IPv6 multicast address for your DHCPv6 server

> server — Server configuration

+ mode — Mode (automatic, disable DHCP server, or enable DHCP server)

+ probe-ip — Ping the IP when allocating a new IP

> ip-pool — IP subnets or ranges (x.x.x.x-y.y.y.y or IPv6-range or x.x.x.x/y or IPv6/netmask or list of values enclosed in [ ])

> option — Server configuration options

+ dns-suffix — DNS suffix (inherited or specify SMTP server IP address)

+ gateway — Default gateway (x.x.x.x or IPv6)

+ pop3-server — Post Office Protocol 3 (POP3) server (inherited or specify IP address and network mask)

+ smtp-server — Simple Mail Transfer Protocol (SMTP) server (inherited or specify IP address and network mask)

> dns — Primary and secondary Domain Name System (DNS) server IP address(es) (inherited or specify IP address and network mask)

> inheritance — Inherit settings from specified interface

+ source — Dynamic interface name

> lease — Lease, unlimited or timeout in minutes (0-1000000)

> nis — Primary and secondary Network Information Service (NIS) server IP address(es) (inherited or specify IP address and network mask)

> ntp — Primary and secondary Network Time Protocol (NTP) server IP address(es) (inherited or specify IP address and network mask)

> wins — Primary and secondary Windows Internet Name Service (WINS) server IP address(es) (inherited or specify IP address and network mask)

> reserved — Reserved IP address or IPv6 address

+ mac — Media Access Control (MAC) address (xx:xx:xx:xx:xx:xx)

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network dns-proxy

Configures Domain Name System (DNS) proxy on the firewall. The firewall supports the selective directing of DNS queries to different DNS servers based on full or partial domain names. TCP or UDP DNS queries are sent through the configured interface. UDP queries fail over to TCP when a DNS query answer is too long for a single UDP packet.

If the domain name is not found in the DNS proxy cache, the domain name is searched for a match based on configuration of the entries in the specific DNS proxy object (on the interface on which the DNS query arrived) and forwarded to a name server based on the match results. If no match is found, the default name servers are used.

Syntax

```
set network dns-proxy <name>
    {
    enabled {no | yes} |
    cache |
       {
       enabled {no | yes} |
       size <value> |
       timeout <value> |
       }
    default |
       {
       primary {inherited | <ip/netmask>} |
       secondary {inherited | <ip/netmask>} |
       inheritance source <interface_name>
       }
    domain-servers <name> |
       {
       cacheable {no | yes} |
       domain-name <value> |
       primary <ip_address> |
       secondary <ip_address>
       }
    interface <interface_name> |
    static-entries <name> {address <ip_address> | domain <value>} |
    tcp-queries |
       {
       enabled {no | yes} |
       max-pending-requests <value>
       }
    udp-queries retries {attemps <value> | interval <value>}
    }
```

Options

<name> — DNS proxy name
+ enabled — Enable or disable processing of DNS requests on interface(s) on this object
> cache — Specify DNS cache related settings

    + enabled — Turn on/off caching for this DNS object
    + size — Max number of entries stored in cache (1024-10240)

```
    + timeout — Time in hours after which cache is cleared (4-24)
> default — Specify DNS default settings
    + primary — Primary DNS Name server IP address (inherited or specify IP address and network mask)
    + secondary — Secondary DNS Name server IP address (inherited or specify IP address and network mask)
    > inheritance — Inherit settings from specified interface
       + source — Dynamic interface name
> domain-servers — Specify domain names to name servers mappings
    + cacheable — Turn on/off caching of domains resolved by this mapping
    + domain-name — Domain names that will be matched (dotted domain name with optional wildcards or list of names
       enclosed in [ ])
    + primary — Primary DNS Name server IP address (x.x.x.x or IPv6)
    + secondary — Secondary DNS Name server IP address (x.x.x.x or IPv6)
> interface — Interface(s) enabled for DNS Proxy (name or list of names enclosed in [ ])
> static-entries — Specify static domain name to name server mappings
    + address — IP addresses for specified domain name (x.x.x.x or IPv6 or list of values enclosed in [ ])
    + domain — Fully qualified domain name for specified IP address
> tcp-queries — Specify TCP queries related settings
    + enabled — Turn on/off forwarding of TCP DNS queries
    + max-pending-requests — Upper limit on number of concurrent TCP DNS requests (1024-2048)
> udp-queries — Specify UDP queries related settings
    > retries — Tune DNS query forwarding retry parameters
       + attempts — Maximum number of retries before trying next name server (1-30)
       + interval — Time in seconds for another request to be sent (1-30)
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network ike

Configures the Internet Key Exchange (IKE) protocol for securing IPSec tunnels.

Syntax

```
set network ike
   {
   crypto-profiles |
     {
     ike-crypto-profiles {default | <name>} |
        {
        dh-group {group1 | group14 | group2 | group5 | <list>} |
        encryption {3des | aes128 | aes192 | aes256 | <list>} |
        hash {md5 | sha1 | sha256 | sha384 | sha512 | <list>} |
        lifetime {days | hours | minutes | seconds} <value>
        }
     ipsec-crypto-profiles {default | <name>} |
        {
        dh-group {group1 | group14 | group2 | group5 | no-pfs} |
        ah authentication {md5 | sha1 | sha256 | sha384 | sha512 | <list>} |
        esp |
           {
           authentication {md5 | sha1 | sha256 | sha384 | sha512 | none | <list>} |
           encryption {3des | aes128 | aes192 | aes256 | null | <list>} |
           }
        lifesize {gb | kb | mb | tb} <value> |
        lifetime {days | hours | minutes | seconds} <value>
        }
     }
   gateway <name>
     {
     authentication

     certificate {
        local-certificate <cert-name-string>;
        certificate-profile <profile-name-string>;
        strict-validation-revocation <yes|no>;
        allow-id-payload-mismatch <yes|no>;
     }

     pre-shared-key key <value> |
     local-address |
        {
        interface <value> |
        floating-ip <ip_address> |
        ip <ip_address>
        }
     local-id |
        {
        id <value> |
        type {fqdn | ipaddr | ufqdn | <value>}
```

```
            }
         peer-address {ip <ip_address> | dynamic} |
         peer-id |
            {
            id <value> |
            type {dn | fqdn | ipaddr | keyid | ufqdn} |
            matching {exact | wildcard} |
            }
         protocol ikev1 |
            {
            exchange-mode {aggressive | auto | main} |
            ike-crypto-profile {default | <name>} |
            dpd
               {
               enable {no | yes} |
               interval <value> |
               retry <value>
               }
            }
         protocol-common
            {
            passive-mode {no | yes} |
            nat-traversal
            {
               enable {no | yes}
               keep-alive-interval {value} |
               udp-checksum-enable {no | yes}
            fragmentation {enable <yes|no>}
            }
         }
      }
```

Options

> crypto-profiles — IKE/IPsec Security Association (SA) Proposal Configuration

> ike-crypto-profiles — IKE SA proposals; specify default or enter a name

+ dh-group — Phase-1 Diffie-Hellman (DH) group; select from the following options, or enter a list of values enclosed in [ ]

group1 — 768-bit Modular Exponentiation (MODP) Group
group14 — 2048-bit MODP Group, NIST rating 112-bit strength
group2 — 1024-bit MODP Group, NIST rating 80-bit strength
group5 — 1536-bit MODP Group

+ encryption — Encryption algorithm; select from the following options, or enter a list of values enclosed in [ ]

3des — National Institute of Standards and Technology (NIST) rating 112-bit strength
aes128 — NIST rating 128-bit strength
aes192 — NIST rating 192-bit strength
aes256 — NIST rating 256-bit strength

+ hash — Hashing algorithm; select from the following options, or enter a list of values enclosed in [ ]

md5 — Below 80-bit strength
sha1 — NIST rating 128-bit strength
sha256 — NIST rating 256-bit strength
sha384 — NIST rating over 256-bit strength
sha512 — NIST rating over 256-bit strength

> lifetime — IKE SA lifetime

```
            > days — Specify lifetime in days (1-65535)
            > hours — Specify lifetime in hours (1-65535)
            > minutes — Specify lifetime in minutes (3-65535)
            > seconds — Specify lifetime in seconds (180-65535)
    > ipsec-crypto-profiles — Internet Protocol Security (IPsec) SA proposals
        + dh-group — Phase-2 DH group (PFS DH group)
            group1 — 768-bit MODP Group
            group14 — 2048-bit MODP Group, NIST rating 112-bit strength
            group2 — 1024-bit MODP Group, NIST rating 80-bit strength
            group5 — 1536-bit MODP Group
            no-pfs — Disable PFS feature
        > ah — AH only
            + authentication — Authentication algorithm; select from the following options, or enter a list of values enclosed in [ ]
                md5 — Below 80-bit strength
                sha1 — NIST rating 128-bit strength
                sha256 — NIST rating 256-bit strength
                sha384 — NIST rating over 256-bit strength
                sha512 — NIST rating over 256-bit strength
        > esp — ESP options
            + authentication — Authentication algorithm; select from the following options, or enter a list of values enclosed in [ ]
                md5 — below 80-bit strength
                none — none
                sha1 — NIST rating 128-bit strength
                sha256 — NIST rating 256-bit strength
                sha384 — NIST rating over 256-bit strength
                sha512 — NIST rating over 256-bit strength
            + encryption — Encryption algorithm; select from the following options, or enter a list of values enclosed in [ ]
                3des — NIST rating 112-bit strength
                aes128 — NIST rating 128-bit strength
                aes192 — NIST rating 192-bit strength
                aes256 — NIST rating 256-bit strength
                null — Null
        > lifesize — IPSec SA lifesize; specify in gigabytes (GB), kilobytes (KB), megabytes (MB), or terabytes (TB) (1-65535)
        > lifetime — IPSec SA lifetime
            > days — Specify lifetime in days (1-65535)
            > hours — Specify lifetime in hours (1-65535)
            > minutes — Specify lifetime in minutes (3-65535)
            > seconds — Specify lifetime in seconds (180-65535)
> gateway — IKE gateway configuration
    > authentication — Authentication method
        > certificate — Use RSA digital signature authentication
            + allow-id-payload-mismatch — Permit peer identification and certificate payload identification mismatch (yes or no)
            + certificate-profile — Specify profile for certificate validation during IKE negotiation
            + local-certificate — Specify local certificate name
            + strict-validation-revocation — Enable strict validation of peer's extended key use (yes or no)
        > pre-shared-key — Use pre-shared key for mutual authentication
            + key — String used as pre-shared key
    > local-address — Tunnel local IP configuration
        + interface — Local gateway end-point
        > floating-ip — Floating IP address in HA Active-Active configuration
        > ip — Specify exact IP address if interface has multiple addresses
    > local-id — Optionally how peer gateway will identify local gateway instead of using IP address
        + id — Local ID string
        + type — Type; select from list, or specify other value
            fqdn — FQDN (hostname)
            ipaddr — IP address
            ufqdn — User FQDN (email address)
    > peer-address — Peer gateway address
        > ip — Peer gateway has static IP address (x.x.x.x or IPv6)
        dynamic — Peer gateway has dynamic IP address
    > peer-id — Optionally how local gateway will identify peer gateway instead of using IP address
        + id — Local ID string
        + type — Type; select from list, or specify other value
            fqdn — FQDN (hostname)
            ipaddr — IP address
            ufqdn — User FQDN (email address)
    > protocol — IKE Protocol settings
        > ikev1 — IKEv1 setting
            + exchange-mode — Exchange mode
                aggressive — Use aggressive mode
                auto — Choose IKE exchange mode automatically
                main — Use main mode
            + ike-crypto-profile — IKE SA crypto profile name (default or enter a name)
            > dpd — Dead-Peer-Detection settings
                + enable — Enable Dead-Peer-Detection
                + interval — Sending interval for probing packets, in seconds (2-100)
                + retry — Number of retries before disconnection (2-100)
    > protocol-common — IKE Protocol settings common to IKEv1 and IKEv2 (IKEv2 to be supported in a future release)
        + passive-mode — Enable passive mode (responder only)
        > fragmentation— IKE fragmentation setting
            + enable — Enable IKE fragmentation (yes or no)
        > nat-traversal — NAT-Traversal settings
            + enable — Enable NAT-Traversal (yes or no)
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network interface

Configures network interfaces on the firewall.

Syntax

```
set network interface
   {
   aggregate-ethernet <interface_name> |
     {
     comment <value> |
     ha |
        {
        lacp |
           {
           enable {no | yes} |
           fast-failover {no | yes} |
           max-ports <value> |
           mode {active | passive} |
           system-priority <value> |
           transmission-rate {fast | slow} |
           }
        }
     layer2 |
        {
        lacp |
           {
           enable {no | yes} |
           fast-failover {no | yes} |
           max-ports <value> |
           mode {active | passive} |
           system-priority <value> |
           transmission-rate {fast | slow} |
           high-availability |
              use-same-system-mac |
              {
              enable {no | yes} |
              mac-address <mac-address> |
              }
           }
        netflow-profile <name> |
        units <name_value>
           {
           comment <value> |
           tag <value>
           }
        }
     layer3 |
        {
        adjust-tcp-mss {no | yes} |
        interface-management-profile <value> |
        lacp |
           {
           enable {no | yes} |
           fast-failover {no | yes} |
           max-ports <value> |
           mode {active | passive} |
           system-priority <value> |
           transmission-rate {fast | slow} |
           high-availability |
              use-same-system-mac |
              {
              enable {no | yes} |
              mac-address <mac-address> |
              }
           }
        mtu <value> |
        netflow-profile <name> |
        untagged-sub-interface {no | yes} |
        arp {<ip address/netmask> | <address object>} {hw-address <mac_address>} |
        dhcp-client |
           {
           create-default-route {no | yes} |
           default-route-metric <value> |
           enable {no | yes}
           }
        ip {<ip address/netmask> | <address object>} |
        ipv6 |
           {
           enabled {no | yes} |
           interface-id {EUI-64 | <value>} |
           address {<ip address/netmask> | <address object>} {anycast | prefix} |
           neighbor-discovery
              {
              dad-attempts <value> |
              enable-dad {no | yes} |
              ns-interval <seconds> |
              reachable-time <seconds> |
              neighbor {<ip address/netmask> | <address object>} {hw-address
                 <mac_address>} |
              router-advertisement
                 {
                 enable {no | yes} |
                 enable-consistency-check {no | yes} |
                 hop-limit {unspecified | <value>} |
                 lifetime <value> |
                 link-mtu {unspecified | <value>} |
                 managed-flag {no | yes} |
                 max-interval <value> |
                 min-interval <value> |
                 other-flag {no | yes} |
                 reachable-time {unspecified | <value>} |
                 retransmission-timer {unspecified | <value>}
                 }
              }
           }
```

```
            units <name_value>
               {
               comment <value> |
               tag <value>
               }
            }
         virtual-wire |
            {
            netflow-profile <name> |
            units <name_value>
               {
               comment <value> |
               tag <value> |
               ip-classifier {<ip-range> | {<ip address/netmask> | <address object>}}
               }
            }
         decrypt-mirror |
         ha
         }
      ethernet <interface_name> |
         {
         comment <value> |
         lacp |
            {
            port-priority <value> |
            }
         link-duplex {auto | <value>} |
         link-speed {auto | <value>} |
         link-state {auto | down | up} |
         aggregate-group <value> |
         layer2 |
            {
            netflow-profile <name> |
            units <name_value>
               {
               comment <value> |
               tag <value>
               }
            }
         layer3 |
            {
            adjust-tcp-mss {no | yes} |
            interface-management-profile <value> |
            mtu <value> |
            netflow-profile <name> |
            untagged-sub-interface {no | yes} |
            arp {<ip address/netmask> | <address object>} {hw-address <mac_address>} |
            dhcp-client |
               {
               create-default-route {no | yes} |
               default-route-metric <value> |
               enable {no | yes}
               }
            ip {<ip address/netmask> | <address object>} |
            ipv6 |
               {
               enabled {no | yes} |
               interface-id {EUI-64 | <value>} |
               address {<ip address/netmask> | <address object>}
                  {
                  enable-on-interface {no | yes} |
                  advertise |
                     {
                     auto-config-flag {no | yes} |
                     enable {no | yes} |
                     onlink-flag {no | yes} |
                     preferred-lifetime {infinity | <value>} |
                     valid-lifetime {infinity | <value>}
                     }
                  anycast |
                  prefix
                  }
               neighbor-discovery
                  {
                  dad-attempts <value> |
                  enable-dad {no | yes} |
                  ns-interval <seconds> |
                  reachable-time <seconds> |
                  neighbor {<ip address/netmask> | <address object>} {hw-address
                     <mac_address>}
                  router-advertisement
                     {
                     enable {no | yes} |
                     enable-consistency-check {no | yes} |
                     hop-limit {unspecified | <value>} |
                     lifetime <value> |
                     link-mtu {unspecified | <value>} |
                     managed-flag {no | yes} |
                     max-interval <value> |
                     min-interval <value> |
                     other-flag {no | yes} |
                     reachable-time {unspecified | <value>} |
                     retransmission-timer {unspecified | <value>}
                     }
                  }
               }
            pppoe |
               {
               access-concentrator <value> |
               authentication {CHAP | PAP | auto} |
               create-default-route {no | yes} |
               default-route-metric <value> |
               enable {no | yes} |
               password <value> |
               service <value> |
               username <value> |
               passive enable {no | yes} |
               static-address ip {<ip address/netmask> | <address object>}
```

```
            }
         units <name_value>
            {
            comment <value> |
            tag <value>
            }
         }
      log-card
         {
         default-gateway <ip> |
         ip-address <ip> |
         ipv6-address <ipv6> |
         ipv6-default-gateway <ip> |
         netmask <ip> |
         }
      tap {netflow-profile <name>} |
      virtual-wire |
         {
         netflow-profile <name> |
         units <name_value>
            {
            comment <value> |
            tag <value> |
            ip-classifer {<ip-range> | {<ip address/netmask> | <address object>}}
            }
         }
      decrypt-mirror
      ha
      }
   loopback |
      {
      adjust-tcp-mss {no | yes} |
      comment <value> |
      interface-management-profile <value> |
      mtu <value> |
      netflow-profile <name> |
      ip <ip_address> |
      ipv6 |
         {
         enabled {no | yes} |
         interface-id {EUI-64 | <value>} |
         address <ip_address>
            enable-on-interface {no | yes} |
            anycast |
            prefix
         {
      units <name_value>
      }
   tunnel |
      {
      comment <value> |
      interface-management-profile <value> |
      mtu <value> |
      netflow-profile <name> |
    ip {<ip address/netmask> | <address object>} |
    ipv6 |
      {
      enabled {no | yes} |
      interface-id {EUI-64 | <value>} |
      address {<ip address/netmask> | <address object>}
        enable-on-interface {no | yes} |
        anycast |
        prefix
      {
    units <name_value>
    }
  vlan
    {
    adjust-tcp-mss {no | yes} |
    comment <value> |
    interface-management-profile <value> |
    mtu <value> |
    netflow-profile <name> |
    arp <ip_address> |
      {
      hw-address <mac_address> |
      interface <value>
      }
    dhcp-client |
      {
      create-default-route {no | yes} |
      default-route-metric <value> |
      enable {no | yes}
      }
    ip {<ip address/netmask> | <address object>} |
    ipv6 |
      {
      enabled {no | yes} |
      interface-id {EUI-64 | <value>} |
      address {<ip address/netmask> | <address object>}
        {
        enable-on-interface {no | yes} |
        advertise |
          {
          auto-config-flag {no | yes} |
          enable {no | yes} |
          onlink-flag {no | yes} |
          preferred-lifetime {infinity | <value>} |
          valid-lifetime {infinity | <value>}
          }
        anycast |
        prefix
        }
      neighbor-discovery
        {
        dad-attempts <value> |
        enable-dad {no | yes} |
        ns-interval <seconds> |
        reachable-time <seconds> |
        neighbor {<ip address/netmask> | <address object>} {hw-address
          <mac_address>}
        router-advertisement
          {
          enable {no | yes} |
          enable-consistency-check {no | yes} |
          hop-limit {unspecified | <value>} |
          lifetime <value> |
          link-mtu {unspecified | <value>} |
          managed-flag {no | yes} |
          max-interval <value> |
          min-interval <value> |
          other-flag {no | yes} |
          reachable-time {unspecified | <value>} |
          retransmission-timer {unspecified | <value>}
          }
        }
      }
    units <name_value>
    }
  }
```

Options

> aggregate-ethernet — Aggregate interface name (ae1-ae8)

+ comment — Comment text for identifying the aggregate interface

> ha — HA (high availability) interface

> lacp — Link Aggregation Control Protocol (LACP) settings. The interface must be of type HA3.

+ enable — Enable (**yes**) or disable (**no**) Link Aggregation Control Protocol (LACP) for the aggregate group. LACP is disabled by default.

+ fast-failover — Enter **yes** if, when an interface goes down, you want the firewall to fail over to an operational interface within one second. If you enter **no**, failover occurs at the standard IEEE 802.1AX-defined speed (at least three seconds).

+ max-ports — The value you enter specifies the number of interfaces (1-8) that can be active at any given time in an LACP aggregate group. The value cannot exceed the number of interfaces you assign to the group. If the number of assigned interfaces exceeds the number of active interfaces, the firewall uses the port priorities of the interfaces to determine which are in standby mode. You set port priorities when configuring individual interfaces for the group.

+ mode — Select the LACP mode of the firewall: **active** or **passive**. In active mode, the firewall actively queries the LACP status (available or unresponsive) of peer devices. In passive mode (the default), the firewall passively responds to LACP status queries from peer devices. Between any two LACP peers, it is recommended that one be active and the other passive. LACP cannot function if both peers are passive.

+ system-priority — The number you enter determines whether the firewall or its peer overrides the other with respect to port priorities (see the **max-ports** description). Note that the lower the number, the higher the priority. The range is 1-65535 and the default is 32768.

+ transmission-rate — Enter the rate at which the firewall exchanges queries and responses with peer devices: **fast** (every second) or **slow** (every 30 seconds). The default is **slow**.

> layer2 — Layer 2 interface

+ netflow-profile — NetFlow server profile name

> lacp — Link Aggregation Control Protocol (LACP) settings. The interface must be of type HA3.

+ enable — Enable (**yes**) or disable (**no**) Link Aggregation Control Protocol (LACP) for the aggregate group. LACP is disabled by default.

+ fast-failover — Enter **yes** if, when an interface goes down, you want the firewall to fail over to an operational interface within one second. If you enter **no**, failover occurs at the standard IEEE 802.1AX-defined speed (at least three seconds).

+ max-ports — The value you enter specifies the number of interfaces (1-8) that can be active at any given time in an LACP aggregate group. The value cannot exceed the number of interfaces you assign to the group. If the number of assigned interfaces exceeds the number of active interfaces, the firewall uses the port priorities of the interfaces to determine which are in standby mode. You set port priorities when configuring individual interfaces for the group.

+ mode — Select the LACP mode of the firewall: **active** or **passive**. In active mode, the firewall actively queries the LACP status (available or unresponsive) of peer devices. In passive mode (the default), the firewall passively responds to LACP status queries from peer devices. Between any two LACP peers, it is recommended that one be active and the other passive. LACP cannot function if both peers are passive.

+ system-priority — The number you enter determines whether the firewall or its peer overrides the other with respect to port priorities (see the **max-ports** description). Note that the lower the number, the higher the priority. The range is 1-65535 and the default is 32768.

+ transmission-rate — Enter the rate at which the firewall exchanges queries and responses with peer devices: **fast** (every second) or **slow** (every 30 seconds). The default is **slow**.

> high-availability use-same-system-mac — Firewalls in a high availability (HA) pair have the same system priority value. However, in an active/passive deployment, the system ID for each can be the same or different, depending on whether you assign the same MAC address. When the LACP peers (also in HA mode) are virtualized (appearing to the network as a single device), using the same system MAC address for the firewalls is a best practice to minimize latency during failover. When the LACP peers are not virtualized, using the unique MAC address of each firewall is the best practice to minimize failover latency. If the firewalls are not in active/passive HA mode, PAN-OS ignores this field. (Firewalls in an active/active deployment require unique MAC addresses so PAN-OS automatically assigns them.) LACP uses the MAC address to derive a system ID for each LACP peer. If the firewall pair and peer pair have identical system priority values, LACP uses the system ID values to determine which overrides the other with respect to port priorities. If both firewalls have the same MAC address, both will have the same system ID, which will be higher or lower than the system ID of the LACP peers. If the HA firewalls have unique MAC addresses, it is possible for one to have a higher system ID than the LACP peers while the other has a lower system ID.

+ enable — Specify whether to use (**yes** or **no**) the same system MAC address for both firewall HA peers.

+ mac-address — If you enabled the **use-same-system-mac** option, enter the MAC address of both firewall HA peers. If you enter a MAC address other than the one the firewall generates automatically, you must ensure it is globally unique.

> units — Logical interface configuration (name.x)

+ comment — Comment text

+ tag — 802.1q VLAN tag (1-4094)

> layer3 — Layer 3 interface

+ adjust-tcp-mss — Set if TCP MSS value should be reduced based on mtu

+ interface-management-profile — Interface management profile

> lacp — Link Aggregation Control Protocol (LACP) settings. The interface must be of type HA3.

+ enable — Enable (**yes**) or disable (**no**) Link Aggregation Control Protocol (LACP) for the aggregate group. LACP is disabled by default.

+ fast-failover — Enter **yes** if, when an interface goes down, you want the firewall to fail over to an operational interface within one second. If you enter **no**, failover occurs at the standard IEEE 802.1AX-defined speed (at least three seconds).

+ max-ports — The value you enter specifies the number of interfaces (1-8) that can be active at any given time in an LACP aggregate group. The value cannot exceed the number of interfaces you assign to the group. If the number of assigned interfaces exceeds the number of active interfaces, the firewall uses the port priorities of the interfaces to determine which are in standby mode. You set port priorities when configuring individual interfaces for the group.

+ mode — Select the LACP mode of the firewall: **active** or **passive**. In active mode, the firewall actively queries the LACP status (available or unresponsive) of peer devices. In passive mode (the default), the firewall passively responds to LACP status queries from peer devices. Between any two LACP peers, it is recommended that one be active and the other passive. LACP cannot function if both peers are passive.

+ system-priority — The number you enter determines whether the firewall or its peer overrides the other with respect to port priorities (see the **max-ports** description). Note that the lower the number, the higher the priority. The range is 1-65535 and the default is 32768.

+ transmission-rate — Enter the rate at which the firewall exchanges queries and responses with peer devices: **fast** (every second) or **slow** (every 30 seconds). The default is **slow**.

> high-availability use-same-system-mac — Firewalls in a high availability (HA) pair have the same system priority value. However, in an active/passive deployment, the system ID for each can be the same or different, depending on whether you assign the same MAC address. When the LACP peers (also in HA mode) are virtualized (appearing to the network as a single device), using the same system MAC address for the firewalls is a best practice to minimize latency during failover. When the LACP peers are not virtualized, using the unique MAC address of each firewall is the best practice to minimize failover latency. If the firewalls are not in active/passive HA mode, PAN-OS ignores this field. (Firewalls in an active/active deployment require unique MAC addresses so PAN-OS automatically assigns them.) LACP uses the MAC address to derive a system ID for each LACP peer. If the firewall pair and peer pair have identical system priority values, LACP uses the system ID values to determine which overrides the other with respect to port priorities. If both firewalls have the same MAC address, both will have the same system ID, which will be higher or lower than the system ID of the LACP peers. If the HA firewalls have unique MAC addresses, it is possible for one to have a higher system ID than the LACP peers while the other has a lower system ID. In the latter case, when failover occurs on the firewalls, port prioritization switches between the LACP peers and the firewall that becomes active.

+ enable — Specify whether to use (**yes** or **no**) the same system MAC address for both firewall HA peers.

+ mac-address — If you enabled the **use-same-system-mac** option, enter the MAC address or both firewall HA peers.

+ mtu — Maximum Transfer Unit, up to 9216 in Jumbo-Frame mode, up to 1500 otherwise

+ netflow-profile — NetFlow server profile name

+ untagged-sub-interface — Enable untagged sub-interface

> arp — ARP configuration IP address and network mask (x.x.x.x/y)

+ hw-address — MAC address (xx:xx:xx:xx:xx:xx)

> dhcp-client — Dynamic Host Configuration Protocol (DHCP) client configuration

+ create-default-route — Automatically create default route pointing to server

+ default-route-metric — Metric of the default route created (1-65535)

+ enable — Enable the DHCP client

> ip — Interface IP address and network mask (x.x.x.x/y)

> ipv6 — Interface IPv6 configuration

+ enabled — Enable IPv6 on the interface

+ interface-id — 64-bit Extended Unique Identifier (EUI-64), or user-defined 64-bit identifier (in hex)

> address — IPv6 address or IP address and network mask (x.x.x.x/y)

+ enable-on-interface — Configure this address on interface

> advertise — Configure router advertisement prefix option

+ auto-config-flag — Set the Auto Address Configuration Flag (A-bit) of the prefix in Router Advertisement messages

+ enable — Enable advertising this prefix in router advertisements

+ onlink-flag — Set the On-Link Flag (L-bit) of the prefix in Router Advertisement messages

+ preferred-lifetime — Preferred Lifetime of the prefix advertised in Router Advertisement messages (infinity, or between 0-4294967294 seconds)

+ valid-lifetime — Valid Lifetime of the prefix advertised in Router Advertisement messages (infinity, or between 0-4294967294 seconds)

anycast — Anycast address

prefix — Use this as prefix to form full address with interface id/EUI-64 (64-bit extended unique identifier)

> neighbor-discovery — Neighbor Discovery configuration

+ dad-attempts — Number of consecutive neighbor solicitation messages sent for duplicate address detection (0-10)

+ enable-dad — Enable duplicate address detection

+ ns-interval — Interval (in seconds) between consecutive neighbor solicitation messages (1-3600)

+ reachable-time — Time (in seconds) that the Reachable status for a neighbor can be maintained (10-3600)

```
                > neighbor — Static entries in neighbor cache IP address and network mask (x.x.x.x/y)
                    + hw-address — MAC address (xx:xx:xx:xx:xx:xx)
                > router-advertisement — Router advertisement configuration
                    + enable — Enable router advertisement
                    + enable-consistency-check — Check consistency of RA messages from other routers
                    + hop-limit — Current Hop Limit advertised in Router Advertisement messages (unspecified, or between
                        1-255)
                    + lifetime — Router Lifetime advertised in Router Advertisement messages, in seconds (0-9000)
                    + link-mtu — Value of MTU option in Router Advertisement messages (unspecified, or between 1280-
                        9216)
                    + managed-flag — Set the Managed Configuration Flag (M-bit) in Router Advertisement messages
                    + max-interval — Maximum interval between consecutive unsolicited Router Advertisement messages, in
                        seconds (4-1800)
                    + min-interval — Minimum interval between consecutive unsolicited Router Advertisement messages, in
                        seconds (3-1350)
                    + other-flag — Set the Other Stateful Configuration Flag (O-bit) in Router Advertisement messages
                    + reachable-time — Reachable Time (in milliseconds) advertised in Router Advertisement messages
                        (unspecified, or between 0-3600000)
                    + retransmission-timer — Retransmission Timer (in milliseconds) advertised in Router Advertisement
                        messages (unspecified, or between 0-4294967295)
        > units — Logical interface (name.x)
            + comment — Comment text
            + tag — 802.1q VLAN tag (1-4094)
    > virtual-wire — Virtual-wire interface
        + netflow-profile — NetFlow server profile name
        > units — Logical interface (name.x)
            + comment — Comment text
            + tag — 802.1q VLAN tag (1-4094)
            > ip-classifier Internet Protocol classifier, either IP range (ip1-ip2), IP/network mask, or list of values between [ ]
    ha — Interface for high-availability functions
> ethernet — Ethernet interface alphanumeric string [ 0-9a-zA-Z./_-] (format: ethernetx/x)
    + comment — Comment text for identifying the interface
    > lacp port-priority — The firewall only uses this field if you enabled Link Aggregation Control Protocol (LACP) for the
        aggregate group (see aggregate-ethernet). An aggregate group might have more interfaces than it supports in
        active states. (In the aggregate group configuration, the Max Ports parameter determines the number of active interfaces).
        In this case, the port priority assigned to each interface determines whether it is active or standby. The lower the numeric
        value, the higher the priority. The range is 1-65535 and the default is 32768.
    + link-duplex — Interface link duplex setting or auto-detect
    + link-speed — Interface link speed or auto-detect
    + link-state — Interface link state (auto-detect, force to down, or force to up)
    > aggregate-group — Aggregate interface group name
    > layer2 — Layer 2 interface
        + netflow-profile — NetFlow server profile name
        > units — Logical interface configuration (name.x)
            + comment — Comment text
            + tag — 802.1q VLAN tag (1-4094)
    > layer3 — Layer 3 interface
        + adjust-tcp-mss — Set if TCP MSS value should be reduced based on mtu
        + interface-management-profile — Interface management profile
        + mtu — Maximum Transfer Unit, up to 9216 in Jumbo-Frame mode, up to 1500 otherwise
        + netflow-profile — NetFlow server profile name
        + untagged-sub-interface — Enable untagged sub-interface
        > arp — ARP configuration IP address and network mask (x.x.x.x/y)
            + hw-address — MAC address (xx:xx:xx:xx:xx:xx)
```

```
> dhcp-client — Dynamic Host Configuration Protocol (DHCP) client configuration
    + create-default-route — Automatically create default route pointing to server
    + default-route-metric — Metric of the default route created (1-65535)
    + enable — Enable the DHCP client
> ip — Interface IP address and network mask (x.x.x.x/y)
> ipv6 — Interface IPv6 configuration
    + enabled — Enable IPv6 on the interface
    + interface-id — 64-bit Extended Unique Identifier (EUI-64), or user-defined 64-bit identifier (in hex)
    > address — IPv6 address or IP address and network mask (x.x.x.x/y)
        + enable-on-interface — Configure this address on interface
        > advertise — Configure router advertisement prefix option
            + auto-config-flag — Set the Auto Address Configuration Flag (A-bit) of the prefix in Router Advertisement messages
            + enable — Enable advertising this prefix in router advertisements
            + onlink-flag — Set the On-Link Flag (L-bit) of the prefix in Router Advertisement messages
            + preferred-lifetime — Preferred Lifetime of the prefix advertised in Router Advertisement messages (infinity, or between 0-4294967294 seconds)
            + valid-lifetime — Valid Lifetime of the prefix advertised in Router Advertisement messages (infinity, or between 0-4294967294 seconds)
        anycast — Anycast address
        prefix — Use this as prefix to form full address with interface id/EUI-64 (64-bit extended unique identifier)
    > neighbor-discovery — Neighbor Discovery configuration
        + dad-attempts — Number of consecutive neighbor solicitation messages sent for duplicate address detection (0-10)
        + enable-dad — Enable duplicate address detection
        + ns-interval — Interval (in seconds) between consecutive neighbor solicitation messages (1-3600)
        + reachable-time — Time (in seconds) that the Reachable status for a neighbor can be maintained (10-3600)
        > neighbor — Static entries in neighbor cache IP address and network mask (x.x.x.x/y)
            + hw-address — MAC address (xx:xx:xx:xx:xx:xx)
        > router-advertisement — Router advertisement configuration
            + enable — Enable router advertisement
            + enable-consistency-check — Check consistency of RA messages from other routers
            + hop-limit — Current Hop Limit advertised in Router Advertisement messages (unspecified, or between 1-255)
            + lifetime — Router Lifetime advertised in Router Advertisement messages, in seconds (0-9000)
            + link-mtu — Value of MTU option in Router Advertisement messages (unspecified, or between 1280-9216)
            + managed-flag — Set the Managed Configuration Flag (M-bit) in Router Advertisement messages
            + max-interval — Maximum interval between consecutive unsolicited Router Advertisement messages, in seconds (4-1800)
            + min-interval — Minimum interval between consecutive unsolicited Router Advertisement messages, in seconds (3-1350)
            + other-flag — Set the Other Stateful Configuration Flag (O-bit) in Router Advertisement messages
            + reachable-time — Reachable Time (in milliseconds) advertised in Router Advertisement messages (unspecified, or between 0-3600000)
            + retransmission-timer — Retransmission Timer (in milliseconds) advertised in Router Advertisement messages (unspecified, or between 0-4294967295)
> pppoe — Point-to-Point Protocol over Ethernet (PPPOE) configuration
    + access-concentrator — Desired access concentrator
    + authentication — Authentication protocol
        CHAP — Challenge Handshake Authentication Protocol
        PAP — Password Authentication Protocol
        auto — Auto-select CHAP or PAP
    + create-default-route — Automatically create default route pointing to peer
```

```
         + default-route-metric — Metric of the default route created (1-65535)
         + enable — Enable (no or yes)
         + password — Password for PPP authentication (Note: For HA pairs, password is synced to peer upon commit)
         + service — Desired service
         + username — Username for PPP authentication
         > passive — Device awaits PPP request from peer
         > static-address — Use static interface address IP address and network mask (x.x.x.x/y)
      > units — Logical interface (name.x)
         + comment — Comment text
         + tag — 802.1q VLAN tag (1-4094)
   > > tap — Tap mode interface
      + netflow-profile — NetFlow server profile name
   > virtual-wire — Virtual-wire interface
      + netflow-profile — NetFlow server profile name
      > units — Logical interface (name.x)
         + comment — Comment text
         + tag — 802.1q VLAN tag (1-4094)
         > ip-classifier Internet Protocol classifier, either IP range (ip1-ip2), IP/network mask, or list of values between [ ]
   decrypt-mirror — Interface to mirror decrypted packet. Creates a copy of decrypted traffic from a firewall and sends it to a
      traffic collection tool that can receive raw packet captures-such as NetWitness or Solera-for archiving and analysis. For
      organizations that require comprehensive data capture for forensic and historical purposes or data leak prevention (DLP)
      functionality.
   ha — Interface for high-availability functions
> loopback — Loopback interface
   + adjust-tcp-mss — Set if TCP MSS value should be reduced based on mtu
   + comment — Comment text for identifying the loopback interface
   + interface-management-profile — Interface management profile
   + mtu — Maximum Transfer Unit, up to 9216 in Jumbo-Frame mode, up to 1500 otherwise
   > ip — Interface IP address (x.x.x.x)
   > ipv6 — Interface IPv6 configuration
      + enabled — Enable IPv6 on the interface
      + interface-id — 64-bit Extended Unique Identifier (EUI-64), or user-defined 64-bit identifier (in hex)
      > address — IP address (x.x.x.x)
         + enable-on-interface — Configure this address on interface
         anycast — Anycast address
         prefix — Use this as prefix to form full address with interface id/EUI-64 (64-bit extended unique identifier)
   > units — Logical interface alphanumeric string [ 0-9a-zA-Z./_-] (loopback.x)
> tunnel — Tunnel interface
   + comment — Comment text for identifying the tunnel interface
   + interface-management-profile — Interface management profile
   + mtu — Maximum Transfer Unit, up to 9216 in Jumbo-Frame mode, up to 1500 otherwise
   + netflow-profile — NetFlow server profile name
   > ip — Interface IP address and network mask (x.x.x.x/y)
   > ipv6 — Interface IPv6 configuration
      + enabled — Enable IPv6 on the interface
      + interface-id — 64-bit Extended Unique Identifier (EUI-64), or user-defined 64-bit identifier (in hex)
      > address — IP address and network mask (x.x.x.x/y)
         + enable-on-interface — Configure this address on interface
         anycast — Anycast address
         prefix — Use this as prefix to form full address with interface id/EUI-64 (64-bit extended unique identifier)
   > units — Logical interface alphanumeric string [ 0-9a-zA-Z./_-] (tunnel.x)
> vlan — VLAN interface
   + adjust-tcp-mss — Set if TCP MSS value should be reduced based on mtu
   + comment — Comment text for identifying the VLAN interface
+ interface-management-profile — Interface management profile
+ mtu — Maximum Transfer Unit, up to 9216 in Jumbo-Frame mode, up to 1500 otherwise
+ netflow-profile — NetFlow server profile name
> arp — ARP configuration IP address (x.x.x.x)
    + hw-address — MAC address (xx:xx:xx:xx:xx:xx)
    + interface — Interface associated with this ARP entry
> dhcp-client — Dynamic Host Configuration Protocol (DHCP) client configuration
    + create-default-route — Automatically create default route pointing to server
    + default-route-metric — Metric of the default route created (1-65535)
    + enable — Enable the DHCP client
> ip — Interface IP address and network mask (x.x.x.x/y)
> ipv6 — Interface IPv6 configuration
    + enabled — Enable IPv6 on the interface
    + interface-id — 64-bit Extended Unique Identifier (EUI-64), or user-defined 64-bit identifier (in hex)
    > address — IPv6 address or IP address and network mask (x.x.x.x/y)
        + enable-on-interface — Configure this address on interface
        > advertise — Configure router advertisement prefix option
            + auto-config-flag — Set the Auto Address Configuration Flag (A-bit) of the prefix in Router Advertisement messages
            + enable — Enable advertising this prefix in router advertisements
            + onlink-flag — Set the On-Link Flag (L-bit) of the prefix in Router Advertisement messages
            + preferred-lifetime — Preferred Lifetime of the prefix advertised in Router Advertisement messages (infinity, or between 0-4294967294 seconds)
            + valid-lifetime — Valid Lifetime of the prefix advertised in Router Advertisement messages (infinity, or between 0-4294967294 seconds)
        anycast — Anycast address
        prefix — Use this as prefix to form full address with interface id/EUI-64 (64-bit extended unique identifier)
    > neighbor-discovery — Neighbor Discovery configuration
        + dad-attempts — Number of consecutive neighbor solicitation messages sent for duplicate address detection (0-10)
        + enable-dad — Enable duplicate address detection
        + ns-interval — Interval (in seconds) between consecutive neighbor solicitation messages (1-3600)
        + reachable-time — Time (in seconds) that the Reachable status for a neighbor can be maintained (10-3600)
        > neighbor — Static entries in neighbor cache IP address and network mask (x.x.x.x/y)
        + hw-address — MAC address (xx:xx:xx:xx:xx:xx)
        > router-advertisement — Router advertisement configuration
            + enable — Enable router advertisement
            + enable-consistency-check — Check consistency of RA messages from other routers
            + hop-limit — Current Hop Limit advertised in Router Advertisement messages (unspecified, or between 1-255)
            + lifetime — Router Lifetime advertised in Router Advertisement messages, in seconds (0-9000)
            + link-mtu — Value of MTU option in Router Advertisement messages (unspecified, or between 1280-9216)
            + managed-flag — Set the Managed Configuration Flag (M-bit) in Router Advertisement messages
            + max-interval — Maximum interval between consecutive unsolicited Router Advertisement messages, in seconds (4-1800)
            + min-interval — Minimum interval between consecutive unsolicited Router Advertisement messages, in seconds (3-1350)
            + other-flag — Set the Other Stateful Configuration Flag (O-bit) in Router Advertisement messages
            + reachable-time — Reachable Time (in milliseconds) advertised in Router Advertisement messages (unspecified, or between 0-3600000)
            + retransmission-timer — Retransmission Timer (in milliseconds) advertised in Router Advertisement messages (unspecified, or between 0-0-4294967295)
> units — Logical interface alphanumeric string [ 0-9a-zA-Z./_-] (vlan.x)
```

Sample Output

The following command assigns the **ethernet1/4** interface to be a virtual wire interface.

```
[edit]
username@hostname# set network interface ethernet ethernet1/1 virtual-wire
[edit]
   username@hostname#
```

The following command sets the VLAN IP address to **1.1.1.4/32** from the network interface vlan level of the hierarchy.

```
[edit network interface vlan]
username@hostname# set ip 1.1.1.4/32

[edit network interface vlan]
username@hostname#
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network profiles

Configures network profiles on the firewall. Network profiles capture configuration information that the firewall can use to establish network connections and implement policies.

Syntax

```
set network profiles
   {
   interface-management-profile <name>
     {
     http {no | yes} |
     http-ocsp {no | yes} |
     https {no | yes} |
     ping {no | yes} |
     response-pages {no | yes} |
     snmp {no | yes} |
     ssh {no | yes} |
     telnet {no | yes} |
     userid-service {no | yes} |
     userid-syslog-listener-ssl {no | yes}
     userid-syslog-listener-udp {no | yes}
     permitted-ip {<ip address/netmask> | <address object>}
     }
   monitor-profile {default | <name>} |
     {
     action  {fail-over | wait-recover} |
     interval <value> |
     threshold <value>
     }
   zone-protection-profile <name>
     {
     asymmetric-path {bypass | drop | global} |
     description <value> |
     discard-icmp-error {no | yes} |
     discard-icmp-frag {no | yes} |
     discard-icmp-large-packet {no | yes} |
     discard-icmp-ping-zero-id {no | yes} |
     discard-ip-frag {no | yes} |
     discard-ip-spoof {no | yes} |
     discard-loose-source-routing {no | yes} |
     discard-malformed-option {no | yes} |
     discard-overlapping-tcp-segment-mismatch {no | yes} |
     discard-record-route {no | yes} |
     discard-security {no | yes} |
     discard-stream-id {no | yes} |
     discard-strict-source-routing {no | yes} |
     discard-timestamp {no | yes} |
     discard-unknown-option {no | yes} |
     remove-tcp-timestamp {no | yes} |
     suppress-icmp-needfrag {no | yes} |
     suppress-icmp-timeexceeded {no | yes} |
     tcp-reject-non-syn {global | no | yes} |
     flood |
        {
        icmp |
           {
           enable {no | yes} |
           red
              {
              activate-rate <value> |
              alarm-rate <value> |
              maximal-rate <value>
              }
           }
        icmpv6 |
           {
           enable {no | yes} |
           red
              {
              activate-rate <value> |
              alarm-rate <value> |
              maximal-rate <value>
              }
           }
        other-ip |
           {
           enable {no | yes} |
           red
              {
              activate-rate <value> |
              alarm-rate <value> |
              maximal-rate <value>
              }
           }
        tcp-syn |
           {
           enable {no | yes} |
           red
              {
              activate-rate <value> |
              alarm-rate <value> |
              maximal-rate <value>
              }
           syn-cookies
              {
              activate-rate <value> |
              alarm-rate <value> |
              maximal-rate <value>
              }
           }
        udp
           {
           enable {no | yes} |
           red
              {
              activate-rate <value> |
              alarm-rate <value> |
              maximal-rate <value>
              }
           }
        }
     ipv6 |
        {
        anycast-source {no | yes} |
        icmpv6-too-big-small-mtu-discard {no | yes} |
        ipv4-compatible-address {no | yes} |
        multicast-source {no | yes} |
        needless-fragment-hdr {no | yes} |
        options-invalid-ipv6-discard {no | yes} |
        reserved-field-set-discard {no | yes} |
        routing-header {no | yes} |
        filter-ext-hdr |
           {
           dest-option-hdr {no | yes} |
           hop-by-hop-hdr {no | yes} |
           routing-hdr {no | yes} |
           }
        ignore-inv-pkt
           {
           dest-unreach {no | yes} |
           param-problem {no | yes} |
           pkt-too-big {no | yes} |
           redirect {no | yes} |
           time-exceeded {no | yes}
           }
        }
     scan <threat_id>
        {
        interval <value> |
        threshold <value> |
        action
           {
           block-ip |
              {
              duration <value> |
              track-by {source | source-and-desintation}
              }
           alert |
           allow |
           block
           }
        }
     }
  }
```

Options

> interface-management-profile — Interface management profile configuration

   + http — Enable HTTP service on the interface

```
    + http-ocsp — Enable HTTP Online Certificate Status Protocol (OCSP) service on the interface
    + https — Enable HTTPS service on the interface
    + ping — Enable Ping service on the interface
    + response-pages — Enable response pages on the interface
    + snmp — Enable SNMP service on the interface
    + ssh — Enable SSH service on the interface
    + telnet — Enable Telnet service on the interface
    + userid-service — Enable user ID service on the interface
    + userid-syslog-listener-ssl — Enable user ID syslog listener service (no or yes)
    + userid-syslog-listener-udp — Enable user ID UDP listener service (no or yes)
    > permitted-ip — Permitted IP address and network mask (x.x.x.x/y or IPv6/netmask)
> monitor-profile — Monitor profile configuration
    + action — Configure action triggered when tunnel status change
        fail-over — When tunnel is down, make traffic fail over to backup path is configured
        wait-recover — When tunnel is down, wait for the recover
    + interval — Probing interval in seconds (2-100)
    + threshold — Number of failed probe to determine tunnel is down (2-10)
> zone-protection-profile — Zone-based protection profile configuration
    + asymmetric-path — Actions for TCP sliding window tracking errors, also control enable/disable TCP sequence number
        check for FIN/RST
        bypass — Bypass inspection for the session that has TCP sliding window tracking errors
        drop — Drop offending packets that violated TCP sliding window tracking, enable TCP sequence number check for FIN/
            RST
        global — Use global setting
    + description — Description value
    + discard-icmp-error — Discard ICMP embedded with error message
    + discard-icmp-frag — Discard ICMP fragment
    + discard-icmp-large-packet — Discard Large ICMP packet (IP length > 1024B)
    + discard-icmp-ping-zero-id — Discard ICMP Ping with zero ID
    + discard-ip-frag — Discard IP fragment
    + discard-ip-spoof — Discard spoofed IP packet
    + discard-loose-source-routing — Discard packets with loose source routing IP option
    + discard-malformed-option — Discard packets with malformed IP option
    + discard-overlapping-tcp-segment-mismatch — Discard sessions with mismatched TCP overlapping segment
    + discard-record-route — Discard packets with Record Route IP option
    + discard-security — Discard packets with Security IP option
    + discard-stream-id — Discard packets with Stream ID IP option
    + discard-strict-source-routing — Discard packets with strict source routing IP option
    + discard-timestamp — Discard packets with Timestamp IP option
    + discard-unknown-option — Discard packets with unknown IP option
    + remove-tcp-timestamp—Strip the TCP timestamp from the TCP header, if present.
    + suppress-icmp-needfrag — Do not reply ICMP NEEDFRAG (layer3 only)
    + suppress-icmp-timeexceeded — Do not reply ICMP TTL expired error (layer3 only)
    + tcp-reject-non-syn — Reject non-SYN TCP packet for session setup
        global — Use global setting
        no — Accept non-SYN TCP. Note that allowing non-SYN TCP traffic may prevent file blocking policies from working
            as expected in cases where the client and/or server connection is not set after the block occurs.
        yes — Reject non-SYN TCP
    > flood — Flood protection
        > icmp — ICMP flood protection
            + enable — Enable ICMP flood protection
            > red — Random Early Drop (RED)
                + activate-rate — Packet rate (pps) to start RED (1-2000000)
                + alarm-rate — Packet rate (pps) to generate alarm (0-2000000)
                + maximal-rate — Maximal packet rate (pps) allowed (1-2000000)
        > icmpv6 — ICMPv6 flood protection
            + enable — Enable ICMPv6 flood protection
            > red — Random Early Drop (RED)
                + activate-rate — Packet rate (pps) to start RED (1-2000000)
                + alarm-rate — Packet rate (pps) to generate alarm (0-2000000)
                + maximal-rate — Maximal packet rate (pps) allowed (1-2000000)
        > other-ip — Other IP protocols protection
            + enable — Enable other IP flood protection
            > red — Random Early Drop (RED)
                + activate-rate — Packet rate (pps) to start RED (1-2000000)
                + alarm-rate — Packet rate (pps) to generate alarm (0-2000000)
                + maximal-rate — Maximal packet rate (pps) allowed (1-2000000)
        > tcp-syn — TCP synchronies packet (SYN) flood protection
            + enable — Enable SYN flood protection
            > red — Random Early Drop (RED)
                + activate-rate — Packet rate (pps) to start RED (1-2000000)
                + alarm-rate — Packet rate (pps) to generate alarm (0-2000000)
                + maximal-rate — Maximal packet rate (pps) allowed (1-2000000)
            > syn-cookies — SYN cookies
                + activate-rate — Packet rate (pps) to activate SYN cookies proxy (0-2000000)
                + alarm-rate — Packet rate (pps) to generate alarm (0-2000000)
                + maximal-rate — Maximal packet rate (pps) allowed (1-2000000)
        > udp — UDP flood protection
            + enable — Enable UDP flood protection
            > red — Random Early Drop (RED)
                + activate-rate — Packet rate (pps) to start RED (1-2000000)
                + alarm-rate — Packet rate (pps) to generate alarm (0-2000000)
                + maximal-rate — Maximal packet rate (pps) allowed (1-2000000)
    > ipv6 — IPv6 filtering
        + anycast-source — Drop packets with anycast source address
        + icmpv6-too-big-small-mtu-discard — Drop packets with MTU in ICMPv6 (Packet Too Big) less than 1280 bytes
        + ipv4-compatible-address — Drop packets with IPv4 compatible address
        + multicast-source — Drop packets with multicast source address
        + needless-fragment-hdr — Drop packets with needless fragment header
        + options-invalid-ipv6-discard — Drop packets with invalid IPv6 options in extension header
        + reserved-field-set-discard — Drop packets with reserved field different than 0
        + routing-header — Drop packets with type 0 routing header
        > filter-ext-hdr — IPv6 extension header filtering
            + dest-option-hdr — Drop packets with Destination extension
            + hop-by-hop-hdr — Drop packets with Hop-by-Hop extension
            + routing-hdr — Drop packets with Routing extension
        > ignore-inv-pkt — Ignore invoking embedded packet session
            + dest-unreach — ICMPv6 destination unreachable - require explicit security rule match
            + param-problem — ICMPv6 parameter problem - require explicit security rule match
            + pkt-too-big — ICMPv6 packet too big - require explicit security rule match
            + redirect — ICMPv6 redirect - require explicit security rule match
            + time-exceeded — ICMPv6 time exceeded - require explicit security rule match
    > scan — Scan protection; specify threat ID
        + interval — Interval (2-65535)
        + threshold — Threshold (2-65535)
        > action — Action to take (alert, scan, block, or block IP address)
            > block-ip — Block IP address
                + duration — Duration for block IP address (1-3600)
```

+ track-by — Track by source or source and destination

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network qos

Specifies Quality of Service (QoS) settings on the firewall. The firewall supports fine grained QoS settings for clear text and tunneled traffic upon egress from the firewall. QoS profiles are attached to physical interfaces to specify how traffic classes map to bandwidth and priority. QoS classification is supported with all interface types except Aggregate Ethernet.

Syntax

```
set network qos
   {
   interface <interface_name>
     {
     enabled {no | yes} |
     interface-bandwidth {egress-max <value>} |
     regular-traffic |
        {
        bandwidth {egress-guaranteed <value> | egress-max <value>} |
        default-group {qos-profile {default | <value>}} |
        groups regular-traffic-group {members <name>}
           {
           qos-profile {default | <value>} |
           match
              {
              local-address
                 {
                 address {any | {<ip address/netmask> | <address object>}} |
                 interface <value>
                 }
              }
           }
        }
     tunnel-traffic
        {
        bandwidth {egress-guaranteed <value> | egress-max <value>} |
        default-group {per-tunnel-qos-profile {default | <value>}} |
        groups tunnel-traffic-group {members <tunnel_interface> {qos-profile {default
           | <value>}}}
        }
     }
   profile {default | <name>}
     {
     aggregate-bandwidth {egress-guaranteed <value> | egress-max <value>} |
     class <traffic_class_value>
        {
        priority {high | low | medium | real-time} |
        class-bandwidth {egress-guaranteed <value> | egress-max <value>}
        }
     }
   }
```

Options

```
> interface — Interface QoS configuration (select from the list or enter a new name)
  > interface-bandwidth — Interface bandwidth in mega-bits per second
    + egress-max — Maximum sending bandwidth in mbps (0-16000)
  > regular-traffic — QoS setting for regular traffic
    > bandwidth — Bandwidth of all regular traffic in mega-bit per second
      + egress-guaranteed — Guaranteed sending bandwidth in mbps (0-16000)
      + egress-max — Maximum sending bandwidth in mbps (0-16000)
    > default-group — QoS setting for regular traffic without specified QoS settings
      + qos-profile — Apply default or specify QoS profile for aggregated traffic
    > groups — QoS setting for regular traffic
      > members — Specify QoS setting for traffic go through given group of hosts
        + qos-profile — Apply default or specify QoS profile for traffic go through the group of hosts
        > match — Specify matching criteria for the QoS entity
          > local-address — Matching address on local side
            + address — Any or x.x.x.x/y or IPv6/netmask or a list of values enclosed in [ ]
            + interface — Local-side interface
  > tunnel-traffic — QoS setting for tunneled traffic
    > bandwidth — Bandwidth of all tunnel traffic in mega-bits per second
      + egress-guaranteed — Guaranteed sending bandwidth in mbps (0-16000)
      + egress-max — Maximum sending bandwidth in mbps (0-16000)
    > default-group — QoS setting for tunneled traffic without specified QoS settings
      + per-tunnel-qos-profile — Apply default or specify QoS profile for traffic go through each tunnel interface
    > groups — QoS setting for tunneled traffic
      > members — Specify QoS setting for traffic go through given tunnel interface
        + qos-profile — Apply default or specify QoS profile for traffic go through the tunnel interface
> profile — QoS profile; default or specify a name
  > aggregate-bandwidth — Aggregate bandwidth of all classes in mega-bits per second
    + egress-guaranteed — Guaranteed sending bandwidth in mbps (0-16000)
    + egress-max — Maximum sending bandwidth in mbps (0-16000)
  > class — QoS setting for traffic classes
    + priority — Traffic class priority (high, low, medium, or real-time = highest priority)
    > class-bandwidth — Class bandwidth in mega-bits per second
      + egress-guaranteed — Guaranteed sending bandwidth in mbps (0-16000)
      + egress-max — Maximum sending bandwidth in mbps (0-16000)
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network shared-gateway

Configures a shared gateway on the firewall. Shared gateways allow virtual systems to share a common interface for external communications. All of the virtual systems communicate with the outside world through the physical interface using a single IP address. A single virtual router is used to route the traffic for all of the virtual systems through the shared gateway.

This command is available only when virtual systems are enabled. Refer to "set system" on page 456, and "Using Configuration Commands with Virtual Systems" on page 25.

Syntax

```
set network shared-gateway <name>
   {
   display-name <name> |
   address <name> {description <value> | fqdn <value> | ip-netmask {<ip address/
     netmask> | ip-range <ip_range>} | tag <value>}
   address-group {
   {
     description <value> |
     dynamic {filter <value>} |
     static <value> |
     tag <value>
   }
   import
     {
     dns-proxy <value> |
     network interface <value>
     }
   log-settings |
     {
     email <name> |
        {
        format
           {
           config <value> |
           hip-match <value> |
           system <value> |
           threat <value> |
           traffic <value> |
           escaping {escape-character <value> | escaped-characters <value>}
           }
        server <name>
           {
           and-also-to <value> |
           display-name <name> |
           from <value> |
           gateway <value> |
           to <value>
           }
        }
     profiles <name> |
        {
        alarm {critical | high | informational | low | medium} |
           {
           send-to-panorama {no | yes} |
           send-email using-email-setting <value> |
           send-snmptrap using-snmptrap-setting <value> |
           send-syslog using-syslog-setting <value>
           }
        traffic any
           {
           send-to-panorama {no | yes} |
           send-email using-email-setting <value> |
           send-snmptrap using-snmptrap-setting <value> |
           send-syslog using-syslog-setting <value>
           }
        }
     snmptrap <name>
        {
        version v2c server <name>|
           {
           community <value> |
           manager <value>
           }
        version v3 server <name>
           {
           authpwd <value> |
           engineid <value> |
           manager <value> |
           privpwd <value> |
           user <value> |
           }
        }
     syslog <name> |
        {
        format |
           {
           config <value> |
           hip-match <value> |
           system <value> |
           threat <value> |
           traffic <value> |
           escaping {escape-character <value> | escaped-characters <value>}
           }
        server <name>
           {
           facility {LOG_LOCAL0 | LOG_LOCAL1 | LOG_LOCAL2 | LOG_LOCAL3 | LOG_LOCAL4 |
               LOG_LOCAL5 | LOG_LOCAL6 | LOG_LOCAL7 | LOG_USER} |
           port <value> |
           server <value>
           }
        }
     }
```

```
rulebase |
  {
  dos rules <name>
     {
     description <value> |
     disabled {no | yes} |
     negate-destination {no | yes} |
     negate-source {no | yes} |
     schedule <value> |
     action {allow | deny | protect} |
     destination {any | <value>} |
     from {interface <value> | zone <value>} |
     protection |
        {
        aggregate {profile <value>} |
        classified
           {
           profile <value> |
           classification-criteria
              {
              address destination-ip-only |
              address source-ip-only |
              address src-dest-ip-both
              }
           }
        }
     service {any | application-default | service-http | service-https | <value>} |
     source {any | <value>} |
     source-user {any | known-user | unknown | <value>} |
     tag <value> |
     to {interface <value> | zone <value>}
     }
  nat rules <name> |
     {
     active-active-device-binding {0 | 1 | both | primary} |
     description <value> |
     disabled {no | yes} |
     nat-type {ipv4 | nat64} |
     service {any | service-http | service-https | <value>} |
     to-interface <value> |
     destination {any | <value>} |
     destination-translation |
        {
        translated-address <value> |
        translated-port <value>
        }
     from {any | <value>} |
     source {any | <value>} |
     source-translation
        {
        dynamic-ip translated-address <value> |
        dynamic-ip-and-port |
           {
           translated-address <value> |
               interface-address
                  {
                  interface <interface_name> |
                  floating-ip <ip_address> |
                  ip <ip_address>
                  }
               }
            static-ip
               {
               bi-directional {no | yes} |
               translated-address <value>
               }
            }
         tag <value> |
         to {any | <value>} |
         }
      pbf rules <name> |
         {
         active-active-device-binding {0 | 1 | both} |
         description <value> |
         disabled {no | yes} |
         negate-destination {no | yes} |
         negate-source {no | yes} |
         schedule <value> |
         action |
            {
            forward |
               {
               egress-interface <value> |
               monitor |
                  {
                  disable-if-unreachable {no | yes} |
                  ip-addresss <ip_address> |
                  profile {default | <value>}
                  }
               nexthop <ip_address>
               }
            discard |
            no-pbf
            }
         application <value> |
         destination {any | <value>} |
         enforce-symmetric-return |
            {
            enabled {no | yes} |
            nexthop-address-list <ip_address>
            }
         from {interface <value> | zone <value>}
         service {any | application-default | service-http | service-https | <value>} |
         source {any | <value>} |
         source-user {any | known-user | unknown | <value>} |
         tag <value> |
         }
      }
```

```
    service <name> |
      {
      description <value> |
      protocol {tcp | udp} {port <value> | source-port <value>}
      }
    service-group <name> {service-http | service-https | <value>} |
    tag <value>
    {
      color <value>
      comments <value>
    zone <name>
      {
      network
         {
         log-setting <value> |
         zone-protection-profile <value>
         external <value> |
         layer3 <value> |
         }
      user-acl
         {
         + exclude-list <value> |
         + include-list <value>
         }
      }
    }
```

Options

<name> — Shared gateway name
+ display-name — Display name for shared gateway (alphanumeric string [0-9a-zA-Z._-])
> address — Address configuration
    + description — Description that identifies the address
    > fqdn — Fully Qualified Domain Name (FQDN)
    > ip-netmask — IP address and network mask (x.x.x.x/y or IPv6/netmask)
    > ip-range — IP address range (x.x.x.x-y.y.y.y or IPv6-range)
    > tag — Tag value
> address-group — Address-group name and members
    + description — Description that identifies the address
    > dynamic— Dynamic group (specify filter value)
    > static — Static group (member value or list of values enclosed in [ ])
    > tag — Tag value
> import — Import predefined configured resources
    + dns-proxy — DNS proxy object to use for resolving FQDNs
    > network — Network configuration
        + interface — Import interface (member value or list of values enclosed in [ ])
> log-settings — Log settings for shared gateway
    > email — Email log name
        > format — Custom formats for forwarded logs
            + config — Configuration log value
            + hip-match — HIP match log value
            + system — System log value
            + threat — Threat log value
            + traffic — Traffic log value

```
            > escaping
                + escape-character — Escape character
                + escaped-characters — List of characters to be escaped
        > server — Server address
            + and-also-to — email address (e.g. admin@mycompany.com)
            + display-name — Display name
            + from — email address (e.g. admin@mycompany.com)
            + gateway — IP address or FQDN of SMTP gateway to use
            + to — email address (e.g. admin@mycompany.com)
    > profiles — Profiles to configure
        > alarm — Alarm (critical, high, informational, low, or medium)
            + send-to-panorama — Send to Panorama
            > send-email — Send email (using email setting value)
            > send-snmptrap — Send SNMP trap (using SNMP trap setting value)
            > send-syslog — Send syslog (using syslog setting value)
        > traffic — Traffic profile (any)
            + send-to-panorama — Send to Panorama
            > send-email — Send email (using email setting value)
            > send-snmptrap — Send SNMP trap (using SNMP trap setting value)
            > send-syslog — Send syslog (using syslog setting value)
    > snmptrap — SNMP trap name
        > version v2c and server address
            + community — Community value
            + manager — IP address or FQDN of SNMP manager to use
        > version v3 and server address
            + authpwd — Authentication Protocol Password
            + engineid — A hex number in ASCII string
            + manager — IP address or FQDN of SNMP manager to use
            + privpwd — Privacy Protocol Password
            + user — User value
    > syslog — syslog name
        > format — Custom formats for forwarded logs
            + config — Configuration log value
            + hip-match — HIP match log value
            + system — System log value
            + threat — Threat log value
            + traffic — Traffic log value
            > escaping
                + escape-character — Escape character
                + escaped-characters — List of characters to be escaped
        > server — Server address
            + facility — Facility (LOG_LOCAL0, LOG_LOCAL1, LOG_LOCAL2, LOG_LOCAL3, LOG_LOCAL4,
                LOG_LOCAL5, LOG_LOCAL6, LOG_LOCAL7, or LOG_USER)
            + port — Port number (1-65535)
            + server — IP address or FQDN of SYSLOG server to use
> rulebase — Rule base for shared gateway
    > dos — Denial of Service (DoS) Protection Rules
        + description — Description of rule set
        + disabled — Disable the rule
        + negate-destination — Negate destination
        + negate-source — Negate source
        + schedule — Schedule value
        > action — DoS rule action
            - allow — Allow all packets
            - deny — Deny packets
            - protect — Enforce DoS protection
        > destination — Destination (any, address, address group, region code, IP address/network mask (x.x.x.x/y or IPv6/
            netmask), IP address range (x.x.x.x-y.y.y.y or IPv6-range), or list of values enclosed in [ ])
        > from — Source zone or interface
            + interface — Interface member value or list of values enclosed in [ ]
            + zone — Zone value or list of values enclosed in [ ]
        > protection — DoS protection parameters to enforce
            > aggregate — Parameters for aggregated protection
                + profile — DoS profile to use for aggregated protection
            > classified — Parameters for classified/qualified protection
                + profile — DoS profile to use for classified protection
                > classification-criteria — Parameters to control how DoS protection is applied
                    + address — Parameters for IP Address based classification
                        - destination-ip-only — Destination IP address only
                        - source-ip-only — Source IP address only
                        - src-dest-ip-both — Both source and destination IP addresses
        > service — Service (any, application default, predefined HTTP or HTTPS service, value or list of values enclosed in [ ])
        > source — Source (any, address, address group, region code, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP
            address range (x.x.x.x-y.y.y.y or IPv6-range), or list of values enclosed in [ ])
        > source-user — Source user (any, known user, unknown, user name, user group, or list of values enclosed in [ ])
        > tag — Tag (member value or list of values enclosed in [ ])
        > to — Destination zone, interface, or name
            + interface — Interface member value or list of values enclosed in [ ]
            + zone — Zone value or list of values enclosed in [ ]
                to — Source zone or interface; option to specify a name
    > nat — Network Address Translation Rules
        + active-active-device-binding — Device binding configuration in High Availability (HA) Active-Active mode
            0 — Rule is bound to device 0
            1 — Rule is bound to device 1
            both — Rule is bound to both devices
            primary — Rule is bound to Active-Primary device
        + description — Description of rule set
        + disabled — Disable the rule
        + nat-type — Rule is for NAT64
            ipv4 — IPv4 NAT
            nat64 — Translator between IPv6 and IPv4
        + service — Service (any, predefined HTTP or HTTPS service, service name, or service group)
        + to-interface — Egress interface from route lookup
        > destination — Destination (any, address, address group, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP
            address range (x.x.x.x-y.y.y.y or IPv6-range), or list of values enclosed in [ ])
        > destination-translation
            + translated-address — Address, address group, IP address and network mask (x.x.x.x/y or IPv6/netmask), or IP
                address range (x.x.x.x-y.y.y.y or IPv6-range)
            + translated-port — Port number (1-65535)
        > from — From (any, zone, or list of values enclosed in [ ])
        > source — Source (any, address, address group, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range
            (x.x.x.x-y.y.y.y or IPv6-range), or list of values enclosed in [ ])
        > source-translation
            > dynamic-ip — Dynamic IP-only translation
                + translated-address — Address, address group, IP address and network mask (x.x.x.x/y or IPv6/netmask), or IP
                    address range (x.x.x.x-y.y.y.y or IPv6-range)
            > dynamic-ip-and-port — Dynamic IP and port translation
                + translated-address — Address, address group, IP address and network mask (x.x.x.x/y or IPv6/netmask), IP
```

```
                    address range (x.x.x.x-y.y.y.y or IPv6-range), or list of values enclosed in [ ]
                > interface-address — Use interface address as translated address
                    + interface — Interface name
                    > floating-ip — Floating IP address in HA Active-Active configuration
                    > ip — specify exact IP address if interface has multiple addresses
            > static-ip — Static IP translation via IP shifting
                + bi-directional — Allow reverse translation from translated address to original address
                + translated-address — Address, address group, IP address and network mask (x.x.x.x/y or IPv6/netmask), or IP
                    address range (x.x.x.x-y.y.y.y or IPv6-range)
        > tag — Tag (member value or list of values enclosed in [ ])
        > to — To (any, zone, or list of values enclosed in [ ])
    > pbf — Policy Based Forwarding Rules
        + active-active-device-binding — Device binding configuration in High Availability (HA) Active-Active mode
            0 — Rule is bound to device 0
            1 — Rule is bound to device 1
            both — Rule is bound to both devices
        + description — Description of rule set
        + disabled — Disable the rule
        + negate-destination — Negate destination
        + negate-source — Negate source
        + schedule — Schedule value
        > action — Policy-based forwarding action
            > forward — Forward packets
                + egress-interface — Interface to route packet to
                > monitor — Parameters for monitoring
                    + disable-if-unreachable — Disable this rule if nexthop/monitor ip is unreachable
                    + ip-address — Monitor IP address (x.x.x.x or IPv6)
                    + profile — Monitoring profile associated with this rule
                > nexthop — Next hop IP address (x.x.x.x or IPv6)
            > forward-to-vsys — Virtual system/Shared gateway to route packet to
            - discard — Discard packets
            - no-pbf — Don't forward by PBF
        > application — Application (select from list of applications or enter a value)
        > destination — Destination (any, address, address-group, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP
            address range (x.x.x.x-y.y.y.y or IPv6-range), or list of values enclosed in [ ])
        > enforce-symmetric-return — Configure symmetric return
            + enabled — Enable symmetric return
            > nexthop-address-list — List of nexthop routers
        > from — Source zone or interface
            + interface — Interface member value or list of values enclosed in [ ]
            + zone — Zone value or list of values enclosed in [ ]
        > service — Service (any, application default, predefined HTTP or HTTPS service, value or list of values enclosed in [ ])
        > source — Source (any, address, address group, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range
            (x.x.x.x-y.y.y.y or IPv6-range), or list of values enclosed in [ ])
        > source-user — Source user (any, known user, unknown, user name, user group, or list of values enclosed in [ ])
        > tag — Tag (member value or list of values enclosed in [ ])
> service — Service name
    + description — Description of the service
    > protocol — Protocol (TCP or UDP)
        + port — Port value or list of values (0-65535)
        + source-port — Source port value or list of values (0-65535)
> service-group — Service group name, service HTTP, service HTTPS, or list of values enclosed in [ ]
> tag — Tag to identify the gateway
    + color — Color of the tag (color1 - color16)
    + comment — Comment on shared gateway
> zone — Zone name
    > network — Network configuration
        + log-setting — Log setting for forwarding scan logs
        + zone-protection-profile — Zone protection profile name
        > external — Virtual system or shared gateway (member value or list of values enclosed in [ ])
        > layer3 — Layer3 interfaces (member value or list of values enclosed in [ ])
    > user-acl — User Access Control List (ACL) configuration
        + exclude-list — Exclude list (address, address-group, IP/netmask, or list of values enclosed in [ ])
        + include-list — Include list (address, address-group, IP/netmask, or list of values enclosed in [ ])
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network tunnel

Specifies network tunnel settings on the firewall.

Syntax

```
set network tunnel
   {
   global-protect-gateway <name> |
     {
     max-user <value> |
     tunnel-interface <value> |
     client |
        {
        dns-suffix-inherited {no | yes} |
        dns-server |
           {
           primary {inherited | {<ip address/netmask> | <address object>}} |
           secondary {inherited | {<ip address/netmask> | <address object>}}
           }
        dns-suffix <value> |
        inheritance source <interface_name>
        ip-pool {<ip_range> | {<ip address/netmask> | <address object>}} |
        split-tunneling access-route {<ip address/netmask> | <address object>} |
        wins-server <ip_address>
           {
           primary {inherited | {<ip address/netmask> | <address object>}} |
           secondary {inherited | {<ip address/netmask> | <address object>}}
           }
        }
     ipsec |
        {
        enable {no | yes} |
        third-party-client
           {
           enable {no | yes} |
           group-name <value> |
           group-password <value> |
           rekey-noauth {no | yes}
           }
        }
     local-address
        {
        interface <value> |
        floating-ip <ip_address> |
        ip <ip_address>
        }
     }
   global-protect-site-to-site <name> |
     {
     tunnel-interface <value> |
     client |
        {
        accept-published-routes {no | yes} |
        anti-replay {no | yes} |
        config-refresh-interval <value> |
        copy-tos {no | yes} |
        dns-suffix-inherited {no | yes} |
        ipsec-crypto-profile <name> |
        dns-server |
           {
           primary {inherited | {<ip address/netmask> | <address object>}} |
           secondary {inherited | {<ip address/netmask> | <address object>}}
           }
        dns-suffix <value> |
        inheritance source <interface_name>
        ip-pool {<ip_range> | {<ip address/netmask> | <address object>} | <value>} |
        split-tunneling access-route {<ip address/netmask> | <address object>} |
        tunnel-monitor |
           {
           destination-ip <ip_address> |
           enable {no | yes} |
           tunnel-monitor-profile <name>
           }
        valid-networks <value>
        }
     local-address
        {
        interface <value> |
        floating-ip <ip_address> |
        ip <ip_address>
        }
     }
  ipsec <name> |
     {
     anti-replay {no |yes} |
     copy-tos {no |yes} |
     tunnel-interface <value> |
     auto-key |
        {
        ipsec-crypto-profile {default | <name>} |
        ike-gateway <name> |
        proxy-id <name>
           {
           local {<ip address/netmask> | <address object>} |
           remote {<ip address/netmask> | <address object>} |
           protocol
              {
              number <value> |
              tcp {local-port <port_number> | remote-port <port_number>} |
              udp {local-port <port_number> | remote-port <port_number>} |
              any
              }
           }
        }
     global-protect-satellite |
        {
        portal-address <value> |
        external-ca
           {
           certificate-profile <value> |
           local-certificate <value>
           }
        local-address
           {
           interface <value> |
           floating-ip <ip_address> |
           ip <ip_address>
           }
        publish-connected-routes enable {no | yes} |
        publish-routes <value>
        }
     manual-key |
        {
        local-spi <value> |
        remote-spi <value> |
        ah |
           {
           md5 key <key_value> |
           sha1 key <key_value> |
           sha256 key <key_value> |
           sha384 key <key_value> |
           sha512 key <key_value>
           }
        esp |
           {
           authentication |
              {
              none
              md5 key <key_value> |
              sha1 key <key_value> |
              sha256 key <key_value> |
              sha384 key <key_value> |
              sha512 key <key_value>
              }
           encryption
              {
              algorithm {3des | aes128 | aes128ccm16 | aes192 | aes256 | null} |
              key <key_value>
              }
           }
        local-address |
           {
           interface <value> |
           floating-ip  <ip_address> |
           ip <ip_address>
           }
        peer-address <ip_address>
        }
     tunnel-monitor
```

```
            {
            destination-ip <ip_address> |
            enable {no | yes} |
            tunnel-monitor-profile <value>
            }
        }
    }
```

Options

> global-protect-gateway — GlobalProtect gateway networking specific configuration
    + max-user — Max number of concurrent users logged in (1-20000)
    + tunnel-interface — Apply GlobalProtect gateway tunnels to tunnel interface
    > client — GlobalProtect client configuration
        + dns-suffix-inherited — Enable DNS suffix inheritance from a dynamic interface
        > dns-server — Primary and secondary Domain Name System (DNS) servers IP addresses (inherited or specify IP address and network mask)
        > dns-suffix — DNS suffix for client (member value or list of values enclosed in [ ])
        > inheritance — Inherit settings from specified interface
            + source — Dynamic interface name
        > ip-pool — IP subnets or ranges (x.x.x.x-y.y.y.y or IPv6-range, x.x.x.x/y or IPv6/netmask, or list of values enclosed in [ ])
        > split-tunneling — Split tunneling settings
            + access-route — Subnets need to be accessed by GlobalProtect clients (x.x.x.x/y or IPv6/netmask, or list of values enclosed in [ ])
        > wins-server — Primary and secondary Windows Internet Name Service (WINS) servers IP addresses (inherited or specify IP address and network mask)
    > ipsec — Internet Protocol Security (IPSec) traffic configuration
        + enable — Enable/disable IPSec encapsulation of client traffic
        > third-party-client — Third-party IPSec Virtual Private Network (VPN) client configuration
            + enable — Enable third-party client support
            + group-name — Group name for hybrid authentication
            + group-password — Group password for hybrid authentication
            + rekey-noauth — Skip authentication on an IKE rekey
    > local-address — Tunnel local IP configuration
        + interface — Local gateway end-point
        > floating-ip — Floating IP address in HA Active-Active configuration
        > ip — Specify exact IP address if interface has multiple addresses
> global-protect-site-to-site — GlobalProtect site to site networking specific configuration
    + tunnel-interface — Apply GlobalProtect site-to-site tunnels to specified tunnel interface
    > client — GlobalProtect site-to-site configuration
        + accept-published-routes — Whether Gateway should accept routes published by Satellite
        + anti-replay — Enable Anti-Replay check on this tunnel
        + config-refresh-interval — GlobalProtect gateway configuration refresh interval, in hours (1-48)
        + copy-tos — Copy IP TOS bits from inner packet to IPSec packet (not recommended)
        + dns-suffix-inherited — Enable DNS suffix inheritance from dynamic interface
        + ipsec-crypto-profile — IPSec crypto profile name
        > dns-server — Primary and secondary Domain Name System (DNS) servers IP addresses (inherited or specify IP address and network mask)
        > dns-suffix — DNS suffix for client (member value or list of values enclosed in [ ])
        > inheritance — Inherit settings from specified interface
            + source — Dynamic interface name
        > ip-pool — IP subnets or ranges (x.x.x.x-y.y.y.y or IPv6-range, x.x.x.x/y or IPv6/netmask, or list of values enclosed in [ ])

```
        > split-tunneling — Split tunneling settings
            + access-route — Subnets need to be accessed by GlobalProtect clients (x.x.x.x/y or IPv6/netmask, or list of values enclosed in [ ])
        > tunnel-monitor — Monitor tunnel status
            + destination-ip — Destination IP to send ICMP probe
            + enable — Enable tunnel monitoring on this tunnel
            + tunnel-monitor-profile — Name of monitoring action profile
        > valid-networks — List of valid networks allowed by the Global Protect Gateway (IP and network mask x.x.x.x/y, or list of values enclosed in [ ])
    > local-address — Tunnel local IP configuration
        + interface — Local gateway end-point
        > floating-ip — Floating IP address in HA Active-Active configuration
        > ip — Specify exact IP address if interface has multiple addresses
> ipsec — Internet Protocol Security (IPSec) tunnel configuration
    + anti-replay — Enable Anti-Replay check on this tunnel
    + copy-tos — Copy IP TOS bits from inner packet to IPSec packet (not recommended)
    + tunnel-interface — Apply IPSec VPN tunnels to tunnel interface (ex. tunnel.1)
    > auto-key — IKE VPN options
        + ipsec-crypto-profile   IPSec crypto profile (name or default)
        > ike-gateway — IKE gateway name
        > proxy-id — IKEv1 proxy identification (only needed when peer gateway requires it)
            + local — IP subnet or IP address represents local network (x.x.x.x/y or IPv6/netmask)
            + remote — IP subnet or IP address represents remote network (x.x.x.x/y or IPv6/netmask)
            > protocol — Specify protocol and port number for proxy-id
                > number — IP protocol number (1-254)
                > tcp — TCP protocol; local and remote ports (0-65535)
                > udp — UDP protocol; local and remote ports (0-65535)
                any — any IP protocol
    > global-protect-satellite — Satellite side of Global Protect Satellite tunnel
        + portal-address — GlobalProtect portal address
        > external-ca — GlobalProtect satellite external CA configuration
            + certificate-profile — Profile for authenticating GlobalProtect gateway certificates
            + local-certificate — GlobalProtect satellite certificate file name
        > local-address — Satellite outgoing interface configuration
            + interface — Interface to communicate with Portal
            > floating-ip — Floating IP address in HA Active-Active configuration
            > ip — specify exact IP address if interface has multiple addresses
        > publish-connected-routes — Knob to publish connected and static routes
            + enable — Enable publishing of connected and static routes
        > publish-routes — Specify list of routes to publish to Global Protect Gateway (IP and network mask x.x.x.x/y, or list of values enclosed in [ ])
    > manual-key — Manual key options
        + local-spi — Outbound Security Parameter Index (SPI), hex format xxxxxxxx (range 00001000 to 1FFFFFFF)
        + remote-spi — Inbound Security Parameter Index (SPI), hex format xxxxxxxx
        > ah — Authentication Header (AH) options
            > md5 — Message Digest 5 (MD5) key is 128 bit
                + key — Hex format xxxxxxxx[-xxxxxxxx]... total 4 sections
            > sha1 — Security Hash Algorithm-1 (SHA-1) key is 160 bit
                + key — Hex format xxxxxxxx[-xxxxxxxx]... total 5 sections
            > sha256 — Key is 256 bit
                + key — Hex format xxxxxxxx[-xxxxxxxx]... total 8 sections
            > sha384 — Key is 384 bit
                + key — Hex format xxxxxxxx[-xxxxxxxx]... total 12 sections
            > sha512 — Key is 512 bit
                + key — Hex format xxxxxxxx[-xxxxxxxx]... total 16 sections
        > esp — Encapsulating Security Payload (ESP) options
            > authentication — Authentication algorithm
                none — No authentication
                > md5 — Key is 128 bit
                    + key — Hex format xxxxxxxx[-xxxxxxxx]... total 4 sections
                > sha1 — Key is 160 bit
                    + key — Hex format xxxxxxxx[-xxxxxxxx]... total 5 sections
                > sha256 — Key is 256 bit
                    + key — Hex format xxxxxxxx[-xxxxxxxx]... total 8 sections
                > sha384 — Key is 384 bit
                    + key — Hex format xxxxxxxx[-xxxxxxxx]... total 12 sections
                > sha512 — Key is 512 bit
                    + key — Hex format xxxxxxxx[-xxxxxxxx]... total 16 sections
            > encryption — encryption algorithm
                + algorithm — Algorithm (press <tab> for list)
                    3des — Triple Data Encryption Standard (3DES) key is 192 bit
                    aes128 — Advanced Encryption Standard-128 (AES-128) key is 128 bit
                    aes128ccm16 — AES CCM algorithm
                    aes192 — Key is 192 bit
                    aes256 — Key is 256 bit
                    null — Null algorithm
                + key — Hex format xxxxxxxx[-xxxxxxxx]... total number of sections: 3des: 6, aes128: 4, aes192: 6, aes256: 8
        > local-address — Tunnel local IP configuration
            + interface — Interface to terminate tunnel
            > floating-ip — Floating IP address in HA Active-Active configuration
            > ip — Specify exact IP address if interface has multiple addresses
        > peer-address — Tunnel peer address (x.x.x.x or IPv6)
    > tunnel-monitor — Monitor tunnel status
        + destination-ip — Destination IP to send ICMP probe (x.x.x.x or IPv6)
        + enable — Enable tunnel monitoring on this tunnel
        + tunnel-monitor-profile — Monitoring action profile name
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network virtual-router

Configures a virtual router for the firewall. You can set up virtual routers to enable the firewall to route packets at Layer 3 by making packet forwarding decisions according to the destination address. The Ethernet interfaces, loopback interfaces, and VLAN interfaces defined on the firewall receive and forward the Layer 3 traffic.

Syntax

```
set network virtual-router <name>
    {
    admin-dists |
      {
      ebgp <value> |
      ibgp <value> |
      ospf-ext <value> |
      ospf-int <value> |
      ospfv3-ext <value> |
      ospfv3-int <value> |
      rip <value> |
      static <value> |
      static-ipv6 <value> |
      }
    interface <value> |
    multicast | [refer to separate multicast page below]
    protocol {bgp | ospf | ospfv3 | redist-profile | redist-profile-ipv6 | rip} | [refer to
      separate protocol pages below]
    routing-table {ip |ipv6} static-route <name>
      {
      admin-dist <value> |
      destination {<ip address/netmask> | <address object>}
      interface <value> |
      metric <value> |
      nexthop |
         {
         ip-address <ip_address> |
         next-vr <value> |
         discard
         }
      option no-install
      }
    }
```

Options

<name> — Configures a virtual router with the specified name

> admin-dists — Administrative distances

    + ebgp — Administrative distance used for eBGP routes (10-240)
    + ibgp — Administrative distance used for iBGP routes (10-240)
    + ospf-ext — Administrative distance used for OSPF external routes (10-240)
    + ospf-int — Administrative distance used for OSPF internal routes (10-240)
    + ospfv3-ext — Administrative distance used for OSPF external routes (10-240)
    + ospfv3-int — Administrative distance used for OSPF internal routes (10-240)

```
      + rip — Administrative distance used for RIP routes (10-240)
      + static — Administrative distance used for static routes (10-240)
      + static-ipv6 — Administrative distance used for static routes (10-240)
> interface — Interface(s) within this virtual router, ex. ethernet1/5 (member value or list of values enclosed in [ ])
> multicast — Multicast routing protocol configuration [refer to separate multicast page below]
> protocol — Routing protocol configuration [refer to separate protocol pages below]
      > bgp — Border Gateway Protocol (BGP) configuration
      > ospf — Open Shortest Path First (OSPF) configuration
      > ospfv3 — OSPFv3 (version 3) configuration
      > redist-profile — Define profiles for route redistribution rules
      > redist-profile-ipv6 — Define profiles for route redistribution rules for IPv6 routes
      > rip — Routing Information Protocol (RIP) configuration
> routing-table — Routing table configuration (IP or IPv6 routing table)
      > static-route — Static route configuration
           + admin-dist — Administrative distance (10-240)
           + destination — Destination IP address/prefix (x.x.x.x/y or IPv6/netmask)
           + interface — Interface value
           + metric — Metric value (path cost) (1-65535)
           > nexthop — Next hop to destination
                > ip-address — Next hop IP address (x.x.x.x or IPv6)
                > next-vr — Next hop virtual router
                discard — Discard packet
           > option — Route entry option
                no-install — Do not install entry to forwarding table
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network virtual-router multicast

Configures a virtual router for the firewall with the multicast routing configuration.

For additional virtual router configuration, refer to “set network virtual-router” on page 161.

Syntax

```
set network virtual-router <name> multicast
      {
      enable {no | yes} |
      interface-group <name> |
         {
         description <value> |
         group-permission |
            {
            any-source-multicast <name> |
               {
               group-address {<ip address/netmask> | <address object>} |
               included {no | yes}
               }
            source-specific-multicast <name>
               {
               group-address {<ip address/netmask> | <address object>} |
               included {no | yes} |
               source-address {<ip address/netmask> | <address object>}
               }
            }
         igmp |
            {
            enable {no | yes} |
            immediate-leave {no | yes} |
            last-member-query-interval
            max-groups {unlimited | <value>} |
            max-query-response-time <value> |
            max-sources {unlimited | <value>} |
            query-interval <value> |
            robustness {1 | 2 | 3 | 4 | 5 | 6 | 7} |
            router-alert-policing {no | yes} |
            version {1 | 2 | 3}
            {
         interface <value> |
         pim
            {
            assert-interval <value> |
            bsr-border {no | yes} |
            dr-priority <value> |
            enable {no | yes} |
            hello-interval <value> |
            join-prune-interval <value> |
            allowed-neighbors {<ip address/netmask> | <address object>}
            }
```

```
   }
rp |
   {
   external-rp <ip_address> |
      {
      override {no | yes}
      group-addresses <value> |
      }
   local-rp
      {
      candidate-rp |
         {
         address <value> |
         advertisement-interval <value> |
         interface <value> |
         priority <value>
         group-addresses <value> |
         }
      static-rp
         {
         address <value> |
         interface <value> |
         override {no | yes}
         group-addresses <value> |
         }
      }
   }
spt-threshold {<ip address/netmask> | <address object>} {threshold {0 | never |
   <value>}} |
ssm-address-space <name>
   {
   group-address {<ip address/netmask> | <address object>} |
   included {no | yes}
   }
}
```

Options

<name> — Configures a virtual router with the specified name

+ enable — Enable multicast protocol

> interface-group — Multicast interface group name

+ description — Description text

> group-permission — ASM/SSM group permission

> any-source-multicast — Array of ASM group rules

+ group-address — Group address/prefix (IP address and network mask)

+ included — Included (no or yes; default = yes)

> source-specific-multicast — Array of SSM group-source pair rules

+ group-address — Group address/prefix (IP address and network mask)

+ included — Included (no or yes; default = yes)

+ source-address — Source address/prefix (IP address and network mask)

> igmp — Internet Group Management Protocol (IGMP) configuration

+ enable — Enable IGMP; default = yes

+ immediate-leave — Leave group immediately when a leave message is received; default = no

+ last-member-query-interval — Interval between group/source specific query messages (including those sent in

```
          response of leave group messages) (0.1-3174.4; default = 1)
        + max-groups — Maximum number of groups allowed on this interface (1-65535, or no limit; default = unlimited)
        + max-query-response-time — Maximum query response time for general group membership queries, in seconds (0-3174.4; default = 10)
        + max-sources — Maximum number of source-specific memberships allowed on this interface (1-65535, or no limit; default = unlimited)
        + query-interval — Interval between group/source specific query messages (1-31744; default = 125)
        + robustness — Robustness variable (1-7; default = 2)
        + router-alert-policing — Drop IGMP packets without Router Alert option; default = no
        + version — IGMP version number (1-3)
    > interface — Interface(s) within this group (member value or list of values enclosed in [ ]) Interfaces must be from the virtual router and unique in all interface groups.
    > pim — Configure Protocol Independent Multicast (PIM) Sparse Mode
        + assert-interval — Interval between PIM Assert messages, in seconds (0-65535; default = 177)
        + bsr-border — Interface is bootstrap border; default = no
        + dr-priority — Designated Router priority (0-4294967295; default = 1)
        + enable — Enable configuration; default = yes
        + hello-interval — Interval between PIM Hello messages, in seconds (0-18000; a value of 0 represents an 'infinite' interval; default = 30)
        + join-prune-interval — Interval between PIM Join/Prune messages, in seconds (0-18000; a value of 0 represents an 'infinite' interval; default = 60)
        > allowed-neighbors — Allowed PIM neighbors (IP address and network mask); all neighbors are allowed if not configured
> rp — Rendezvous Point configuration
    > external-rp — Static RP-group mapping with non-local RPs
        + override — Override learned RP for the same group; default = no
        > group-addresses — Multicast group addresses (IP address and network mask for each, list enclosed in [ ])
    > local-rp — Local Rendezvous Point configuration
        > candidate-rp — Configure device to act as candidate RP
            + address — Candidate RP address
            + advertisement-interval — Time interval between candidate RP advertisements, in seconds (1-26214; default = 60)
            + interface — Candidate RP interface
            + priority — Priority for this candidate (0-255; default = 192)
            > group-addresses — Multicast group addresses (IP address and network mask for each, list enclosed in [ ])
        > static-rp — Configure device to act as a static RP
            + address — Local RP address
            + interface — Local RP interface
            + override — Override learned RP for the same group; default = no
            > group-addresses — Multicast group addresses (IP address and network mask for each, list enclosed in [ ])
> spt-threshold — Shortest-Path Tree (SPT) switch rules (IP address and network mask) If not configured, default behavior will be to switch to SPT when the first data packet is received.
    + threshold — Threshold options:
        0 — Switch on first data packet (default)
        never — Do not switch to SPT
        <value> — Data rate at which a SPT switch is triggered, in kbps (1-4294967295)
> ssm-address-space — Source-Specific Multicast address group space as defined in RFC 4604
    + group-address — Group address/prefix (IP address and network mask)
    + included — Included (no or yes; default = yes)
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network virtual-router protocol bgp

Configures a virtual router for the firewall with the Border Gateway Protocol (BGP).

For additional virtual router configuration, refer to “set network virtual-router” on page 161.

Syntax

```
set network virtual-router <name> protocol bgp
         {
         allow-redist-default-route {no | yes} |
         enable {no | yes} |
         install-route {no | yes} |
         local-as <value> |
         reject-default-route {no | yes} |
         router-id <ip_address> |
         auth-profile <name> {secret <value>} |
         dampening-profile <name> |
            {
            cutoff <value> |
            decay-half-life-reachable <value> |
            decay-half-life-unreachable <value> |
            enable {no | yes} |
            max-hold-time <value> |
            reuse <value>
            }
         peer-group <name> |
            {
            aggregated-confed-as-path {no |yes} |
            enable {no |yes} |
            soft-reset-with-stored-info {no |yes} |
            peer <name> |
               {
               enable {no |yes} |
               max-prefixes {unlimited | <value>} |
               peer-as <value> |
               peering-type {bilateral | unspecified} |
               reflector-client {client | meshed-client | non-client} |
               connection-options
                  {
                  authentication <name> |
                  hold-time <value> |
                  idle-hold-time <value> |
                  keep-alive-interval <value> |
                  multihop <value> |
                  open-delay-time <value> |
                  incoming-bgp-connection |
                     {
                     allow {no | yes} |
                     remote-port <port_number>
                     }
                  outgoing-bgp-connection
```

```
                     {
                     allow {no | yes} |
                     local-port <port_number>
                     }
                  }
               local-address {interface <value> | ip <ip_address>} |
               peer-address ip <ip_address>
               }
            type
               {
               ebgp |
                  {
                  export-nexthop {resolve | use-self} |
                  import-nexthop {original | use-peer} |
                  remove-private-as {no | yes}
                  }
               ebgp-confed {export-nexthop {original | use-self}} |
               ibgp {export-nexthop {original | use-self}} |
               ibgp-confed {export-nexthop {original | use-self}}
               }
            }
         policy |
            {
            aggregation {address <aggregating_address>} |
               {
               as-set {no | yes} |
               enable {no | yes} |
               prefix {<ip address/netmask> | <address object>} |
               summary {no | yes} |
               advertise-filters <name> |
                  {
                  enable {no | yes} |
                  match med <value> |
                  match address-prefix {<ip address/netmask> | <address object>}
                     {exact {no | yes}} |
                  match as-path {regex <value>} |
                  match community {regex <value>} |
                  match extended-community {regex <value>}
                  match from-peer <name> |
                  match nexthop {<ip address/netmask> | <address object>} |
                  }
               aggregate-route-attributes |
                  {
                  as-path-limit <value> |
                  local-preference <value> |
                  med <value> |
                  nexthop <ip_address> |
                  origin {egp | igp | incomplete} |
                  weight <value> |
                  as-path {prepend <value> | none} |
                  community |
                     {
                     append {local-as | no-advertise | no-export | nopeer | <value>} |
                     overwrite {local-as | no-advertise | no-export | nopeer |
                        <value>} |
                     remove-regex <value> |
                     none |
                     remove-all
                     }
                  extended-community
                     {
                     append <values> |
                     overwrite <value> |
                     remove-regex <value> |
                     none |
                     remove-all
                     }
                  }
               suppress-filters <name>
                  {
                  enable {no | yes} |
                  match med <value> |
                  match address-prefix {<ip address/netmask> | <address object>}
                     {exact {no | yes}} |
                  match as-path {regex <value>} |
                  match community {regex <value>} |
                  match extended-community {regex <value>}
                  match from-peer <name> |
                  match nexthop {<ip address/netmask> | <address object>} |
                  }
               }
            conditional-advertisement {policy <name>} |
               {
               enable {no | yes} |
               advertise-filters <name> |
                  {
                  enable {no | yes} |
                  match med <value> |
                  match address-prefix {<ip address/netmask> | <address object>} |
                  match as-path {regex <value>} |
                  match community {regex <value>} |
                  match extended-community {regex <value>}
                  match from-peer <name> |
                  match nexthop {<ip address/netmask> | <address object>} |
                  }
               non-exist-filters <name>
                  {
                  enable {no | yes} |
                  match med <value> |
                  match address-prefix {<ip address/netmask> | <address object>} |
                  match as-path {regex <value>} |
                  match community {regex <value>} |
                  match extended-community {regex <value>}
                  match from-peer <name> |
                  match nexthop {<ip address/netmask> | <address object>} |
                  }
               used-by <member_value> |
               }
```

```
export {rules <name>} |
   {
   enable {no | yes} |
   action |
      {
      allow {update as-path-limit <value>} |
      allow {update local-preference <value>} |
      allow {update med <value>} |
      allow {update nexthop <ip_address>} |
      allow {update origin {egp | igp | incomplete}} |
      allow {update as-path} |
         {
         prepend <value> |
         remove-and-prepend <value> |
         none |
         remove
         }
      allow {update community} |
         {
         append {local-as | no-advertise | no-export | nopeer | <value>} |
         overwrite {local-as | no-advertise | no-export | nopeer |
            <value>} |
         remove-regex <value> |
         none |
         remove-all
         }
      allow {update extended-community} |
         {
         append <value> |
         overwrite <value> |
         remove-regex <value> |
         none |
         remove-all
         }
      deny
      }
   match
      {
      med <value> |
      address-prefix {<ip address/netmask> | <address object>} {exact {no
         | yes}} |
      as-path {regex <value>} |
      community {regex <value>} |
      extended-community {regex <value>}
      from-peer <name> |
      nexthop {<ip address/netmask> | <address object>} |
      }
   used-by <member_value> |
   }
import |
   {
   enable {no | yes} |
   action |
      {
         allow |
            {
            dampening <value> |
            update as-path-limit <value>} |
            update local-preference <value>} |
            update med <value>} |
            update nexthop <ip_address>} |
            update origin {egp | igp | incomplete}} |
            update weight <value> |
            update as-path |
               {
               prepend <value> |
               remove-and-prepend <value> |
               none |
               remove
               }
            update community |
               {
               append {local-as | no-advertise | no-export | nopeer |
                  <value>} |
               overwrite {local-as | no-advertise | no-export | nopeer |
                  <value>} |
               remove-regex <value> |
               none |
               remove-all
               }
            update extended-community |
               {
               append <value> |
               overwrite <value> |
               remove-regex <value> |
               none |
               remove-all
               }
            }
         deny
         }
      match
         {
         med <value> |
         address-prefix {<ip address/netmask> | <address object>} {exact {no
            | yes}} |
         as-path {regex <value>} |
         community {regex <value>} |
         extended-community {regex <value>}
         from-peer <name> |
         nexthop {<ip address/netmask> | <address object>} |
         }
      used-by <member_value> |
      }
   }
redist-rules {{<ip address/netmask> | <address object>} | <value>} |
   {
   enable {no | yes} |
   metric <value> |
   set-as-path-limit <value> |
   set-local-preference <value> |
   set-med <value> |
   set-origin {egp | igp | incomplete}
   set-community {local-as | no-advertise | no-export | nopeer | <value>} |
   set-extended-community <value> |
   }
routing-options
   {
   as-format {2-byte | 4-byte} |
   confederation-member-as <value> |
   default-local-preference <value> |
   reflector-cluster-id <ip_address> |
   aggregate {aggregate-med {no | yes}} |
   graceful-restart |
      {
      enable {no | yes} |
      local-restart-time <value> |
      max-peer-restart-time <value> |
      stale-route-time <value>
      }
   med
      {
      always-compare-med {no | yes} |
      deterministic-med-comparison {no | yes}
      }
   }
}
```

Options

<name> — Configures a virtual router with the specified name
+ allow-redist-default-route — Allow redistribute default route to BGP
+ enable — Enable (no or yes)
+ install-route — Populate BGP learned route to global route table
+ local-as — Local Autonomous system (AS) number (1-4294967295)
+ reject-default-route — Do not learn default route from BGP
+ router-id — Router id of this BGP instance (x.x.x.x)
> auth-profile — BGP authentication profiles
+ secret — Shared secret for the TCP MD5 authentication
> dampening-profile — Route flap dampening profiles
+ cutoff — Cutoff threshold value (0-1000)
+ decay-half-life-reachable — Decay half-life while reachable, in seconds (1-3600)
+ decay-half-life-unreachable — Decay half-life while unreachable, in seconds (1-3600)
+ enable — Enable (no or yes)
+ max-hold-time — maximum of hold-down time, in seconds (1-3600)
+ reuse — reuse threshold value (0-1000)
> peer-group — Peer group configuration
+ aggregated-confed-as-path — Peers understand aggregated confederation AS path
+ enable — Enable (no or yes)
+ soft-reset-with-stored-info — Soft reset with stored info
> peer — Peer configuration
+ enable — Enable (no or yes)

```
        + max-prefixes — Maximum of prefixes to receive from peer (unlimited or 1-100000)
        + peer-as — Peer AS number (1-4294967295)
        + peering-type — Peering type that affects NOPEER community value handling
          bilateral — Block sending and receiving routes with NOPEER community value
          unspecified — Disregard NOPEER community value with this peer
        + reflector-client    Peer is reflector client
          client — Reflector client
          meshed-client — Fully meshed reflector client
          non-client — Not a reflector client
        > connection-options — Peer connection options
          + authentication — Authentication options
          + hold-time — Hold time, in seconds (3-3600)
          + idle-hold-time — Idle hold time, in seconds (1-3600)
          + keep-alive-interval — Keep-alive interval, in seconds (1-1200)
          + multihop — IP TTL value used for sending BGP packet (set to 0 means eBGP use 2, iBGP use 255)
          + open-delay-time — Open delay time, in seconds (0-240)
          > incoming-bgp-connection — Incoming TCP connection for BGP
            + allow — Allow (no or yes)
            + remote-port — Restrict remote port for incoming BGP connections (0-65535)
          > outgoing-bgp-connection — Outgoing TCP connection for BGP
            + allow — Allow (no or yes)
            + local-port — Use specific local port for outgoing BGP connections (0-65535)
        > local-address — Local address configuration
          + interface — Interface to accept BGP session
          + ip — Specify exact IP address if interface has multiple addresses
        > peer-address — Peer address configuration (x.x.x.x or IPv6)
      > type — Peer group type and options
        > ebgp — External BGP
          + export-nexthop — Export next hop
            resolve — Export locally resolved next hop
            use-self — Export self address as next hop
          + import-nexthop — Import next hop
            original — Keep original next hop
            use-peer — Override next hop with peer address
          + remove-private-as — Remove private AS when exporting route
        > ebgp-confed — External BGP confederation
          + export-nexthop — Export next hop
            original — Keep original next hop
            use-self — Override next hop with self address
        > ibgp — Internal BGP
          + export-nexthop — Export next hop
            original — Keep original next hop
            use-self — Override next hop with self address
        > ibgp-confed — Internal BGP confederation
          + export-nexthop — Export next hop
            original — Keep original next hop
            use-self — Override next hop with self address
    > policy — BGP routing policy configuration
      > aggregation — Address aggregation policy
        + as-set — Generate AS-set attribute
        + enable — Enable aggregation for this prefix
        + prefix — Aggregating address prefix (x.x.x.x/y or IPv6/netmask)
        + summary — Summarize route
        > advertise-filters — Filter(s) to always advertise route if matched
          + med — Multi-exit Discriminator (MED) (0-4294967295)
          > address-prefix — Address prefix IP address (x.x.x.x/y) or IPv6/netmask to match
            + exact — Match exact prefix length
          > as-path — Autonomous system (AS) path to match
            > regex — AS-path regular expression
          > community — Community to match
            > regex — AS-path regular expression
          > extended-community — Extended community to match
            > regex — AS-path regular expression
          > from-peer — Peer that advertised the route entry (name or list enclosed in [ ])
          > nexthop — Next hop attributes (x.x.x.x/y or IPv6/netmask)
        > aggregate-route-attributes — Aggregate route attributes
          + as-path-limit — Add AS path limit attribute if it does not exist (1-255)
          + local-preference — New local preference value (0-4294967295)
          + med — New MED value (0-4294967295)
          + nexthop — Next hop address {x.x.x.x or IPv6)
          + origin — New route origin
            egp — Route originated from EGP
            igp — Route originated from IGP
            incomplete — Incomplete route
          + weight — New weight value (0-65535)
          > as-path — AS path update options
            > prepend — Prepend local AS for specified number of times (1-255)
             none — No change on AS path
          > community — Community update options
            + append — Append community
                [ — Start a list of values
                local-as — Well known community value: NO_EXPORT_SUBCONFED
                no-advertise — Well known community value: NO_ADVERTISE
                no-export — Well known community value: NO_EXPORT
                nopeer — Well known community value: NOPEER
                <value> — 32-bit value in hex, or in AS:VAL format, AS and VAL each in 0-65535 range
            + overwrite — Remove all communities and replace with specified value
                [ — Start a list of values
                local-as — Well known community value: NO_EXPORT_SUBCONFED
                no-advertise — Well known community value: NO_ADVERTISE
                no-export — Well known community value: NO_EXPORT
                nopeer — Well known community value: NOPEER
                <value> — 32-bit value in hex, or in AS:VAL format, AS and VAL each in 0-65535 range
            > remove-regex — Remove specified community match regular expression
            none — No change on communities
            remove-all — Remove all communities
          > extended-community — Extended community update options
            + append — Append community (64-bit value in hex, or one of TYPE:AS:VAL, TYPE:IP:VAL,
                TYPE:A.B:VAL format, TYPE is 'target', 'origin' or decimal number (0-65535) or list enclosed in
                [ ])
            + overwrite — Remove all communities and replace with specified value (64-bit value in hex, or one
                of TYPE:AS:VAL, TYPE:IP:VAL, TYPE:A.B:VAL format, TYPE is 'target', 'origin' or decimal
                number (0-65535) or list enclosed in [ ])
            > remove-regex — Remove specified community match regular expression
            none — No change on communities
            remove-all — Remove all communities
        > suppress-filters — Filter(s) to suppress route advertisement if matched
          + med — Multi-exit Discriminator (MED) (0-4294967295)
```

```
          > address-prefix — Address prefix IP address (x.x.x.x/y) or IPv6/netmask to match
              + exact — Match exact prefix length
          > as-path — Autonomous system (AS) path to match
              > regex — AS-path regular expression
          > community — Community to match
              > regex — AS-path regular expression
          > extended-community — Extended community to match
              > regex — AS-path regular expression
          > from-peer — Peer that advertised the route entry (name or list enclosed in [ ])
          > nexthop — Next hop attributes (x.x.x.x/y or IPv6/netmask or list enclosed in [ ])
  > conditional-advertisement — Conditional-advertisement policy configuration
      + enable — Enable this policy
      > advertise-filters — Filter(s) to match route to be advertised
          + enable — Enable this filter
          + med — Multi-exit Discriminator (MED) (0-4294967295)
          > address-prefix — Address prefix IP address (x.x.x.x/y) or IPv6/netmask to match
          > as-path — Autonomous system (AS) path to match
              > regex — AS-path regular expression
          > community — Community to match
              > regex — AS-path regular expression
          > extended-community — Extended community to match
              > regex — AS-path regular expression
          > from-peer — Peer that advertised the route entry (name or list enclosed in [ ])
          > nexthop — Next hop attributes (x.x.x.x/y or IPv6/netmask or list enclosed in [ ])
      > non-exist-filters — Filter(s) to match non-exist routes
          + enable — Enable this filter
          + med — Multi-exit Discriminator (MED) (0-4294967295)
          > address-prefix — Address prefix IP address (x.x.x.x/y) or IPv6/netmask to match
          > as-path — Autonomous system (AS) path to match
              > regex — AS-path regular expression
          > community — Community to match
              > regex — AS-path regular expression
          > extended-community — Extended community to match
              > regex — AS-path regular expression
          > from-peer — Peer that advertised the route entry (name or list enclosed in [ ])
          > nexthop — Next hop attributes (x.x.x.x/y or IPv6/netmask or list enclosed in [ ])
      > used-by — Peer/peer-groups that use this rule
  > export — Export policy rule
      + enable — Enable this rule
      > action — Rule action (allow update or deny)
          + as-path-limit — Add AS path limit attribute if it does not exist (1-255)
          + local-preference — New local preference value (0-4294967295)
          + med — New MED value (0-4294967295)
          + nexthop — Next hop address {x.x.x.x or IPv6)
          + origin — New route origin
              egp — Route originated from EGP
              igp — Route originated from IGP
              incomplete — Incomplete route
          > as-path — AS path update options
              > prepend — Prepend local AS for specified number of times (1-255)
              > remove-and-prepend — remove matched AS path(s), and prepend local AS for specified number of
                  times (1-255)
              none — No change on AS path
              remove — Remove matched AS path(s)
```

```
            > community — Community update options
                + append — Append community
                    [ — Start a list of values
                    local-as — Well known community value: NO_EXPORT_SUBCONFED
                    no-advertise — Well known community value: NO_ADVERTISE
                    no-export — Well known community value: NO_EXPORT
                    nopeer — Well known community value: NOPEER
                    <value> — 32-bit value in hex, or in AS:VAL format, AS and VAL each in 0-65535 range
                + overwrite — Remove all communities and replace with specified value
                    [ — Start a list of values
                    local-as — Well known community value: NO_EXPORT_SUBCONFED
                    no-advertise — Well known community value: NO_ADVERTISE
                    no-export — Well known community value: NO_EXPORT
                    nopeer — Well known community value: NOPEER
                    <value> — 32-bit value in hex, or in AS:VAL format, AS and VAL each in 0-65535 range
                > remove-regex — Remove specified community match regular expression
                none — No change on communities
                remove-all — Remove all communities
            > extended-community — Extended community update options
                + append — Append community (64-bit value in hex, or one of TYPE:AS:VAL, TYPE:IP:VAL,
                    TYPE:A.B:VAL format, TYPE is 'target', 'origin' or decimal number (0-65535) or list enclosed in
                    [ ])
                + overwrite — Remove all communities and replace with specified value (64-bit value in hex, or one
                    of TYPE:AS:VAL, TYPE:IP:VAL, TYPE:A.B:VAL format, TYPE is 'target', 'origin' or decimal
                    number (0-65535) or list enclosed in [ ])
                > remove-regex — Remove specified community match regular expression
                none — No change on communities
                remove-all — Remove all communities
        > match — Export match
            + med — Multi-exit Discriminator (MED) (0-4294967295)
            > address-prefix — Address prefix IP address (x.x.x.x/y) or IPv6/netmask to match
                + exact — match exact prefix length
            > as-path — Autonomous system (AS) path to match
                > regex — AS-path regular expression
            > community — Community to match
                > regex — AS-path regular expression
            > extended-community — Extended community to match
                > regex — AS-path regular expression
            > from-peer — Peer that advertised the route entry (name or list enclosed in [ ])
            > nexthop — Next hop attributes (x.x.x.x/y or IPv6/netmask or list enclosed in [ ])
        > used-by — Peer-groups that use this rule
    > import — Import policy rule
        + enable — Enable this rule
        > action — Rule action (allow or deny)
            + dampening — Route flap dampening profile
            > update
                + as-path-limit — Add AS path limit attribute if it does not exist (1-255)
                + local-preference — New local preference value (0-4294967295)
                + med — New MED value (0-4294967295)
                + nexthop — Next hop address {x.x.x.x or IPv6)
                + origin — New route origin
                    egp — Route originated from EGP
                    igp — Route originated from IGP
                    incomplete — Incomplete route
                + weight — New weight value (0-65535)
                > as-path — AS path update options
                    > prepend — Prepend local AS for specified number of times (1-255)
                    > remove-and-prepend — remove matched AS path(s), and prepend local AS for specified
                        number of times (1-255)
                    none — No change on AS path
                    remove — Remove matched AS path(s)
                > community — Community update options
                    + append — Append community
                        [ — Start a list of values
                        local-as — Well known community value: NO_EXPORT_SUBCONFED
                        no-advertise — Well known community value: NO_ADVERTISE
                        no-export — Well known community value: NO_EXPORT
                        nopeer — Well known community value: NOPEER
                        <value> — 32-bit value in hex, or in AS:VAL format, AS and VAL each in 0-65535 range
                    + overwrite — Remove all communities and replace with specified value
                        [ — Start a list of values
                        local-as — Well known community value: NO_EXPORT_SUBCONFED
                        no-advertise — Well known community value: NO_ADVERTISE
                        no-export — Well known community value: NO_EXPORT
                        nopeer — Well known community value: NOPEER
                        <value> — 32-bit value in hex, or in AS:VAL format, AS and VAL each in 0-65535 range
                    > remove-regex — Remove specified community match regular expression
                    none — No change on communities
                    remove-all — Remove all communities
                > extended-community — Extended community update options
                    + append — Append community (64-bit value in hex, or one of TYPE:AS:VAL, TYPE:IP:VAL,
                        TYPE:A.B:VAL format, TYPE is 'target', 'origin' or decimal number (0-65535) or list
                        enclosed in [ ])
                    + overwrite — Remove all communities and replace with specified value (64-bit value in hex, or
                        one of TYPE:AS:VAL, TYPE:IP:VAL, TYPE:A.B:VAL format, TYPE is 'target', 'origin' or
                        decimal number (0-65535) or list enclosed in [ ])
                    > remove-regex — Remove specified community match regular expression
                    none — No change on communities
                    remove-all — Remove all communities
        > match — Export match
            + med — Multi-exit Discriminator (MED) (0-4294967295)
            > address-prefix — Address prefix IP address (x.x.x.x/y) or IPv6/netmask to match
                + exact — match exact prefix length
            > as-path — Autonomous system (AS) path to match
                > regex — AS-path regular expression
            > community — Community to match
                > regex — AS-path regular expression
            > extended-community — Extended community to match
                > regex — AS-path regular expression
            > from-peer — Peer that advertised the route entry (name or list enclosed in [ ])
            > nexthop — Next hop attributes (x.x.x.x/y or IPv6/netmask or list enclosed in [ ])
        > used-by — Peer-groups that use this rule
    > redist-rules — Redistribution rules for export through BGP
        <ip address/netmask> | <address object> — IP address and netmask (x.x.x.x/y) or ipv6/netmask or address
            object
        <value> — Redistribute routes using redist-profile
        + enable — Enable rule
        + metric — Specify metric value
        + set-as-path-limit — Add the AS_PATHLIMIT path attribute (1-255)
        + set-local-preference — Add the LOCAL_PREF path attribute (0-4294967295)
        + set-med — Add the MULTI_EXIT_DISC path attribute (0-4294967295)
        + set-origin — Add the ORIGIN path attribute
            egp — Path learned via EGP protocol
            igp — Path interior to originating AS
            incomplete — Path was learned by some other means
        > set-community — Add the COMMUNITY path attribute
            [ — Start a list of values
            local-as — Well known community value: NO_EXPORT_SUBCONFED
            no-advertise — Well known community value: NO_ADVERTISE
            no-export — Well known community value: NO_EXPORT
            nopeer — Well known community value: NOPEER
            <value> — 32-bit value in hex, or in AS:VAL format, AS and VAL each in 0-65535 range
        > set-extended-community — Add the EXTENDED COMMUNITY path attribute
            [ — Start a list of values
            <value> — 64-bit value in hex, or one of TYPE:AS:VAL, TYPE:IP:VAL, TYPE:A.B:VAL format, TYPE
                is 'target', 'origin' or decimal number (0-65535)
    > routing-options — Routing instance options
        + as-format — AS format
            2-byte   2-byte AS format
            4-byte   4-byte AS format specified in RFC-4893
        + confederation-member-as — Confederation requires member-AS number (1-4294967295)
        + default-local-preference — Default local preference (0-4294967295)
        + reflector-cluster-id — Route reflector cluster ID (x.x.x.x or IPv6)
        > aggregate — Aggregate options
            + aggregate-med — Aggregate route only if they have same MED attributes
        > graceful-restart — Graceful restart options
            + enable — Enable graceful restart
            + local-restart-time — Local restart time to advertise to peer, in seconds (1-3600)
            + max-peer-restart-time — Maximum of peer restart time accepted, in seconds (1-3600)
            + stale-route-time — Time to remove stale routes after peer restart, in seconds (1-3600)
        > med — Path selection based on Multiple Exit Discriminator (MED) Metric
            + always-compare-med — Always compare MEDs
            + deterministic-med-comparison — Deterministic MEDs comparison
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network virtual-router protocol ospf

Configures a virtual router for the firewall with the Open Shortest Path First (OSPF) protocol.

For additional virtual router configuration, refer to “set network virtual-router” on page 161.

Syntax

```
set network virtual-router <name> protocol ospf
   {
   allow-redist-default-route {no | yes} |
   enable {no | yes} |
   reject-default-route {no | yes} |
   rfc1583 {no | yes} |
   router-id <ip_address> |
   area <ip_address> |
     {
     interface <interface_name> |
        {
        authentication <name> |
        dead-counts <value> |
        enable {no | yes} |
        hello-interval <value> |
        metric <value> |
        passive {no | yes} |
        priority <value> |
        retransmit-interval <value> |
        transit-delay <value> |
        link-type {broadcast | p2mp | p2p} |
        neighbor <ip_address>
        }
     range {<ip address/netmask> | <address object>} {advertise | suppress} |
     type |
        {
        nssa |
           {
           accept-summary {no | yes} |
           default-route |
              {
              advertise |
                 {
                 metric <value> |
                 type {ext-1 | ext-2}
                 }
              disable
              }
           nssa-ext-range {<ip address/netmask> | <address object>} {advertise |
              suppress}
           }
        stub
           {
           accept-summary {no | yes} |
           default-route
              {
              advertise {metric <value>} |
              disable
              }
           }
        normal
        }
     virtual-link <name>
        {
        authentication <name> |
        dead-counts <value> |
        enable {no | yes} |
        hello-interval <value> |
        neighbor-id <ip_address>
        retransmit-interval <value> |
        transit-area-id <value> |
        transit-delay <value>
        }
     }
   auth-profile <name> |
     {
     md5 <value> {key <value> | preferred {no | yes}} |
     password <value>
     }
   export-rules {{<ip address/netmask> | <address object>} | <value>} |
     {
     new-path-type {ext-1 | ext-2} |
     new-tag {{<ip address/netmask> | <address object>} | <value>} |
     metric <value>
     {
   graceful-restart{
     enable {yes | no}
     grace-period [5-1800]
     max-neighbor-restart-time [5-1800]
     helper-enable {yes | no}
     strict-LSA-checking-enable {yes | no}
     }
   timers {spf-calculation <value> | lsa-interval <value>}
   }
```

Options

<name> — Configures a virtual router with the specified name
   + allow-redist-default-route — Allow redistribute default route to OSPF
   + enable — Enable configuration
   + reject-default-route — Do not learn default route from OSPF
   + rfc1583 — RFC-1583 compatibility
   + router-id — Router ID of this OSPF instance (x.x.x.x)
   > area — Area configuration (x.x.x.x or IPv6)
      > interface — Protocol configuration for interface(s)
         + authentication — Authentication options
         + dead-counts — Number of lost hello packets to declare router down (3-20)
         + enable — Enable OSPF in this interface

```
    + hello-interval — Interval to send Hello packets, in seconds (0-3600)
    + metric — Cost of OSPF interface (1-65535)
    + passive — Suppress the sending of hello packets in this interface
    + priority — Priority for OSPF designated router selection (0-255)
    + retransmit-interval — Interval to retransmit LSAs, in seconds (1-3600)
    + transit-delay — Estimated delay to transmit LSAs, in seconds (1-3600)
    > link-type — Link type (broadcast, p2mp, or p2p)
    > neighbor — Neighbor configuration (x.x.x.x or IPv6)
  > range — Area range for summarization (x.x.x.x/y or IPv6/netmask)
    advertise — Do summarization and advertise
    suppress — Suppress summarization to be sent, make this subnet hidden
  > type — Area type
    > nssa — Not-So-Stubby Area (NSSA) configuration
      + accept-summary — Accept summary
      > default-route — Configure default route behavior via this interface/subnet
        > advertise — Advertise default route link-state advertisement (LSA) to this area
          + metric — Metric to be used when advertising default route within stub area (1-255)
          + type — Metric type to be used when advertising default route
            ext-1 — Metric comparable with OSPF metric
            ext-2 — External route is always less preferred than OSPF routes
        disable — Do not advertise default route LSA to this area
      > nssa-ext-range — Address range for summary external routes learned within this NSSA area (x.x.x.x/y or
        IPv6/netmask)
        advertise — Do summarization and advertise
        suppress — Suppress summarization to be sent, make this subnet hidden from other areas
    > stub — Stub area configuration
      + accept-summary — Accept-summary
      > default-route — Config default route LSA advertise behavior for this area
        > advertise — Advertise default route LSA to this area
          + metric — Metric to be used when advertising default route within stub area (1-255)
        disable — Do not advertise default route LSA to this area
    normal — Normal area configuration
  > virtual-link — Virtual link configuration
    + authentication — Authentication options
    + dead-counts — Number of lost hello packets to declare router down (3-20)
    + enable — Enable this virtual link
    + hello-interval — Interval to send Hello packets, in seconds (0-3600)
    + neighbor-id — Neighbor router id for virtual link (x.x.x.x or IPv6)
    + retransmit-interval — Interval to retransmit LSAs, in seconds (1-3600)
    + transit-area-id — ID of transit area, cannot be backbone, stub or NSSA
    + transit-delay — Estimated delay to transmit LSAs, in seconds (1-3600)
> auth-profile — OSPF authentication profiles
  > md5 — Use OSPF MD5 authentication method (0-255 index of MD5 key)
    + key — Key for the authentication
    + preferred — Use this key when sending packet
  > password — Simple password authentication
> export-rules — Redistribution rules for export through OSPF
  <ip address/netmask> | <address object>— IP address and netmask (x.x.x.x/y) or IPv6/netmask or address object
  <value> — Redistribute routes using redist-profile
  + new-path-type — Path type to be used for imported external routes
    ext-1 — Metric comparable with OSPF metric
    ext-2 — External route is always less preferred than OSPF routes
  + metric — Metric value
  + new-tag — New tag value (x.x.x.x/y or IPv6/netmask or 1-4294967295)
```

```
> graceful-restart — Graceful restart options
    + enable — Enable graceful restart
    + grace-period — Specify maximum local restarting time (in seconds)
    + helper-enable — Enable/disable helping neighboring routers to graceful restart
    + max-neighbor-restart-time — Specify maximum of neighbor restart time accepted (in seconds)
    + strict-LSA-checking      enable/disable strict LSA checking. Abort GR if lsa change is detected
> timers — OSPF timer options
    > spf-calculation — Sets the delay time between receiving new topology information and performing an SPF calculation,
        in seconds (0.05-10, default = 5)
    > lsa-interval — Specifies the minimum time between transmissions of two instances of the same LSA (equivalent to
        MinLSInterval in RFC 2328), in seconds (1-10, default = 5)
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network virtual-router protocol ospfv3

Configures a virtual router for the firewall with the Open Shortest Path First (OSPF) version 3 protocol.

For additional virtual router configuration, refer to “set network virtual-router” on page 161.

Syntax

```
set network virtual-router <name> protocol ospfv3
    {
    allow-redist-default-route {no | yes} |
    disable-transit-traffic {no | yes} |
    enable {no | yes} |
    reject-default-route {no | yes} |
    router-id <ip_address> |
    area <ip_address> |
      {
      interface <interface_name> |
         {
         authentication <name> |
         dead-counts <value> |
         enable {no | yes} |
         hello-interval <value> |
         metric <value> |
         passive {no | yes} |
         priority <value> |
         retransmit-interval <value> |
         transit-delay <value> |
         link-type {broadcast | p2mp | p2p} |
         neighbor <ip_address>
         }
      range {<ip address/netmask> | <address object>} {advertise | suppress} |
      type |
         {
         nssa |
            {
            accept-summary {no | yes} |
            default-route |
               {
               advertise |
                  {
                  metric <value> |
                  type {ext-1 | ext-2}
                  }
               disable
               }
            nssa-ext-range {<ip address/netmask> | <address object>} {advertise |
               suppress}
            }
         stub
            {
            accept-summary {no | yes} |
            default-route
               {
               advertise {metric <value>} |
               disable
               }
            }
         normal
         }
      virtual-link <name>
         {
         authentication <name> |
         dead-counts <value> |
         enable {no | yes} |
         hello-interval <value> |
         neighbor-id <ip_address>
         retransmit-interval <value> |
         transit-area-id <value> |
         transit-delay <value>
         }
      }
      auth-profile <name> |
      {
         spi <value> |
         ah |
         {
            md5 key <key_value> |
            sha1 key <key_value> |
            sha256 key <key_value> |
            sha384 key <key_value> |
            sha512 key <key_value>
         }
         esp |
         {
            authentication |
            {
               none
               md5 key <key_value> |
               sha1 key <key_value> |
               sha256 key <key_value> |
               sha384 key <key_value> |
               sha512 key <key_value>
            }
            encryption
            {
               algorithm {3des | aes128 | aes128ccm16 | aes192 | aes256 |
               null} |
               key <key_value>
            }
         }
      }
    export-rules {{<ip address/netmask> | <address object>} | <value>} |
      {
      new-path-type {ext-1 | ext-2} |
      new-tag {{<ip address/netmask> | <address object>} | <value>} |
      metric <value>
      {
   graceful-restart{
      enable {yes | no}
      grace-period [5-1800]
      max-neighbor-restart-time [5-1800]
      helper-enable {yes | no}
      strict-LSA-checking-enable {yes | no}
      }
   timers {spf-calculation <value> | lsa-interval <value>}
   }
```

Options

<name> — Configures a virtual router with the specified name

- + allow-redist-default-route — Allow redistribute default route to OSPF
- + disable-transit-traffic — Specify whether OSPFv3 should set the R- and V6-bits in its Router-LSAs
- + enable — Enable configuration
- + reject-default-route — Do not learn default route from OSPF
- + router-id — Router ID of this OSPF instance (x.x.x.x)
- > area — Area configuration (x.x.x.x or IPv6)
  - + authentication — Options for authentication
  - > interface — Protocol configuration for interface(s)
    - + authentication — Authentication options
    - + dead-counts — Number of lost hello packets to declare router down (3-20)
    - + enable — Enable OSPF in this interface
    - + hello-interval — Interval to send Hello packets, in seconds (0-3600)
    - + instance-id — OSPFv3 instance ID
    - + metric — Cost of OSPF interface (1-65535)
    - + passive — Suppress the sending of hello packets in this interface
    - + priority — Priority for OSPF designated router selection (0-255)
    - + retransmit-interval — Interval to retransmit LSAs, in seconds (1-3600)
    - + transit-delay — Estimated delay to transmit LSAs, in seconds (1-3600)
    - > link-type — Link type (broadcast, p2mp, or p2p)
    - > neighbor — Neighbor configuration (x.x.x.x or IPv6)
- > auth-profile — OSPFvw authentication profiles
  - + spi — SPI for both inbound and outbound SA, hex format xxxxxxxx.
  - > ah — AH options
    - > md5 — Use OSPF MD5 authentication method (0-255 index of MD5 key)
    - > sha1 — NIST rating 128-bit strength
    - > sha256 — NIST rating 256-bit strength
    - > sha384 — NIST rating over 256-bit strength
    - > sha512 — NIST rating over 256-bit strength
  - > esp — ESP options
    - > authentication — Authentication algorithm
      - > md5 — Use OSPF MD5 authentication method (0-255 index of MD5 key)
      - > sha1 — NIST rating 128-bit strength
      - > sha256 — NIST rating 256-bit strength
      - > sha384 — NIST rating over 256-bit strength
      - > sha512 — NIST rating over 256-bit strength
      - > none — No authentication
    - > encryption — Encryption algorithm
      - + algorithm (specify 3des | aes128 | aes128ccm16 | aes192 | aes256 | null)
      - + key (specify key value)

> export-rules — Redistribution rules for export through OSPF
    <ip address/netmask> | <address object> — IP address and netmask (x.x.x.x/y) or IPv6/netmask or address object
    <value> — Redistribute routes using redist-profile
    + metric — metric value
    + new-path-type — Path type to be used for imported external routes
        ext-1 — Metric comparable with OSPF metric
        ext-2 — External route is always less preferred than OSPF routes
    + new-tag — New tag value (x.x.x.x/y or IPv6/netmask or 1-4294967295)
> graceful-restart — Graceful restart options
    + enable — Enable graceful restart
    + grace-period — Specify maximum local restarting time (in seconds)
    + helper-enable — Enable/disable helping neighboring routers to graceful restart
    + max-neighbor-restart-time — Specify maximum of neighbor restart time accepted (in seconds)
    + strict-LSA-checking — Enable/disable strict LSA checking. Abort GR if LSA change is detected
> timers — OSPF timer options
    > spf-calculation — Sets the delay time between receiving new topology information and performing an SPF calculation, in seconds (0.05-10, default = 5)
    > lsa-interval — Specifies the minimum time between transmissions of two instances of the same LSA (equivalent to MinLSInterval in RFC 2328), in seconds (1-10, default = 5)

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network virtual-router protocol redist-profile

Defines profiles for route redistribution rules.

For additional virtual router configuration, refer to “set network virtual-router” on page 161.

Syntax

```
set network virtual-router <name> protocol redist-profile <name>
   {
   priority <value> |
   action {redist {new-metric <value>} | no-redist} |
   filter
     {
     bgp |
        {
        community {local-as | no-advertise | no-export | nopeer | <value>} |
        extended-community <value>
        }
     destination {<ip address/netmask> | <address object>} |
     interface <value> |
     nexthop {<ip address/netmask> | <address object>} |
     ospf
        {
        area <ip_address> |
        path-type {ext-1 | ext-2 | inter-area | intra-area | <list>} |
        tag {{<ip address/netmask> | <address object>} | <value>}
        }
     type <bgp | connect | ospf | rip | static | <type> |
     }
   }
```

Options

<name> — Configures a virtual router with the specified name
    redist-profile — Route redistribution profile name
        + priority — Priority (1-255)
        > action — Action taken when filter is matched
            > redist — Redistribute when this rule matched
                + new-metric — New metric value (1-255)
            no-redist — Do not redistribute when this rule matched
        > filter — Define filter criteria for redistribution rules
            > bgp — Specify candidate BGP routes' attributes
                > community — BGP community
                    [— Start a list of values
                    local-as — Well known community value: NO_EXPORT_SUBCONFED
                    no-advertise — Well known community value: NO_ADVERTISE
                    no-export — Well known community value: NO_EXPORT
                    nopeer — Well known community value: NOPEER
                    <value> — 32-bit value in hex, or in AS:VAL format, AS and VAL each in 0-65535 range
                > extended-community — BGP extended-community
                    [— Start a list of values

<value> — 64-bit value in hex, or one of TYPE:AS:VAL, TYPE:IP:VAL, TYPE:A.B:VAL format, TYPE is 'target', 'origin' or decimal number (0-65535)
> destination — Specify candidate routes' destination networks (subnet match) (x.x.x.x/y or IPv6/netmask or list enclosed in [ ])
> interface — Specify candidate routes' interfaces (member value or list enclosed in [ ])
> nexthop — Specify candidate routes' next-hop addresses (subnet match) (x.x.x.x/y or IPv6/netmask or list enclosed in [ ])
> ospf — Specify candidate OSPF routes' attributes
+ area — Area (x.x.x.x or IPv6 or list enclosed in [ ])
+ path-type — Path-type (ext-1, ext-2, inter-area, intra-area, or list enclosed in [ ])
+ tag — Tag (x.x.x.x/y, IPv6/netmask, value between 1-4294967295, or list enclosed in [ ])
> type — Specify candidate routes' types (BGP, connect, OSPF, RIP, static, or list enclosed in [ ])

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network virtual-router protocol redist-profile-ipv6

Defines profiles for IPv6 route redistribution rules.

For additional virtual router configuration, refer to “set network virtual-router” on page 161.

Syntax

```
set network virtual-router <name> protocol redist-profile <name>
    {
    priority <value> |
    action {redist {new-metric <value>} | no-redist} |
    filter
       {
       destination {<ip address/netmask> | <address object>} |
       interface <value> |
       nexthop {<ip address/netmask> | <address object>} |
       type <bgp | connect | ospf | rip | static | <type> |
       }
    }
```

Options

<name> — Configures a virtual router with the specified name
    redist-profile — Route redistribution profile name
        + priority — Priority (1-255)
        > action — Action taken when filter is matched
            > redist — Redistribute when this rule matched
                + new-metric — New metric value (1-255)
            no-redist — Do not redistribute when this rule matched
        > filter — Define filter criteria for redistribution rules
            > destination — Specify candidate routes' destination networks (subnet match) (x.x.x.x/y or IPv6/netmask or list enclosed in [ ])
            > interface — Specify candidate routes' interfaces (member value or list enclosed in [ ])
            > nexthop — Specify candidate routes' next-hop addresses (subnet match) (x.x.x.x/y or IPv6/netmask or list enclosed in [ ])
            > type — Specify candidate routes' types (connect, static, or list enclosed in [ ])

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network virtual-router protocol rip

Configures a virtual router for the firewall with the Routing Information Protocol (RIP).

For additional virtual router configuration, refer to “set network virtual-router” on page 161.

Syntax

```
set network virtual-router <name> protocol rip
   {
   allow-redist-default-route {no | yes} |
   enable {no | yes} |
   reject-default-route {no | yes} |
   auth-profile <name>
     {
     md5 <value> {key <value> | preferred {no | yes}} |
     password <value>
     }
   export-rules metric <value> |
   interface <interface_name>
     {
     authentication <name> |
     enable {no | yes} |
     mode {normal | passive | send-only} |
     default-route {advertise {metric <value>} | disable}
     }
   timers
     {
     delete-intervals <value> |
     expire-intervals <value> |
     interval-seconds <value> |
     update-intervals <value>
     }
   }
```

Options

<name> — Configures a virtual router with the specified name

+ allow-redist-default-route — Allow redistribute default route to RIP

+ enable — Enable configuration

+ reject-default-route — do not learn default route from RIP

> auth-profile — RIP authentication profiles

> md5 — Use RIP MD5 authentication method (0-255 index of MD5 key)

+ key — Key for the authentication

+ preferred — Use this key when sending packet

> password — Simple password authentication

> export-rules — Redistribution rules for export through RIP (metric value 1-16)

> interface — Protocol Configuration for Interface(s)

+ authentication — Authentication options

+ enable — Enable interface

+ mode — Mode selection

normal — Send and receive

```
        passive — Receive only
        send-only — Send only, do not receive RIP updates
    > default-route — Configure default route advertise behavior via this interface/subnet
        > advertise — Advertise default route via this interface/subnet
            + metric — Metric to be used when advertise default route via RIP (1-15)
        disable — Do not advertise default route via this interface/subnet
> timers — Configure RIP timers
    + delete-intervals — Number of intervals take between route expiration to its deletion (1-255)
    + expire-intervals — Number of intervals take between route last updated to its expiration (1-255)
    + interval-seconds — Timer interval value, in seconds (1-60)
    + update-intervals — Number of intervals take between route advertisement (RIP response packet) (1-255)
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network virtual-wire

Specifies virtual wire settings for the firewall. In a virtual wire deployment, the firewall is installed transparently on a network segment by binding two ports together. Virtual wire can be used to install the firewall in any network environment with no configuration of adjacent network devices required.

Syntax

```
set network virtual-wire {default-vwire | <name>}
   {
   interface1 <value> |
   interface2 <value> |
   tag-allowed <value> |
   link-state-pass-through enable {no | yes} |
   multicast-firewalling enable {no | yes}
   }
```

Options

default-vwire — Configures a default virtual wire
<name> — Configures a virtual wire with the specified name
+ interface1 — Interface 1 name
+ interface2 — Interface 2 name
+ tag-allowed — Allowed 802.1q VLAN tags (0-4094)
> link-state-pass-through — Pass link state change from one interface to another
> multicast-firewalling — Firewalling for non-unicast traffic

Required Privilege Level

superuser, vsysadmin, deviceadmin

set network vlan

Configures a Virtual Local Area Network (VLAN) interface on the firewall.

Syntax

```
set network vlan <name>
   {
   interface <value> |
   mac <mac_address> interface <name> |
   virtual-interface
     {
     interface <value> |
     l3-forwarding {no | yes}
     }
   }
```

Options

<name> — VLAN identifier
+ interface — Interface(s) within this VLAN, ex. ethernet1/5 (member value or list of values enclosed in [ ])
> mac — Static MAC configuration (MAC address format xx:xx:xx:xx:xx:xx)
   + interface — Interface name
> virtual-interface   Virtual interface for this VLAN
   + interface — Virtual interface identifier, ex. vlan 1
   + l3-forwarding — Enable Layer3 forwarding on this virtual interface

Required Privilege Level

superuser, vsysadmin, deviceadmin

set ocsp-responder

Configures the Online Certificate Status Protocol (OCSP) responder, which defines a server that will be used to verify the revocation status of certificates issues by PAN-OS devices.

Syntax

```
set ocsp-responder <name> {host-name <name>}
```

Options

<name> — OCSP responder identifier
+ host-name — Host name value

Required Privilege Level

superuser, vsysadmin, deviceadmin

set panorama

(Panorama only) Configures Panorama firewall management.

For information about the syntax and options for each configuration available for Panorama, refer to its command page in this chapter.

Syntax

```
set panorama
   {
   authentication-profile |
   authentication-sequence |
   certificate |
   certificate-profile |
   log-settings |
   server-profile
   }
```

Options

> authentication-profile — [*refer to "set shared authentication-profile" on page 249*]
> authentication-sequence — [*refer to "set shared authentication-sequence" on page 251*]
> certificate — [*refer to "set shared certificate" on page 254*]
> certificate-profile — [*refer to "set shared certificate-profile" on page 255*]
> log-settings — [*refer to "set shared log-settings" on page 258*]
> server-profile — [*refer to "set shared server-profile" on page 274*]

Required Privilege Level

superuser, vsysadmin, deviceadmin

set pdf-summary-report

Specifies format settings for PDF summary reports.

Syntax

```
set pdf-summary-report <name>
    {
    custom-widget <name> |
       {
       chart-type {bar | line | pie | table} |
       column <value> |
       row <value>
       }
    footer {note <value>} |
    header {caption <value>}|
    }
```

Options

<name> — PDF report to configure
> custom-widget — Report widget layout information
    + chart-type — Chart type (bar, line, pie, or table)
    + column — Column number (1-3)
    + row — Row number (1-6)
> footer — Footer information for PDF summary layout
    + note — Static string to be printed as a note
> header — Header information for PDF summary layout
    + caption — Caption for the layout

Required Privilege Level

superuser, vsysadmin, deviceadmin

set profile-group

Specifies settings for sets of security profiles that are treated as a unit and added to security policies. For example, you can create a “threats” security profile group that includes profiles for antivirus, anti-spyware, and vulnerability and then create a security policy that includes the “threats” profile.

Syntax

```
set profile-group <name>
   {
   data-filtering <value> |
   file-blocking <value> |
   spyware <value> |
   url-filtering <value> |
   virus <value> |
   vulnerability <value>
   }
```

Options

<name> — Profile group to configure
+ data-filtering — Data filtering profile to include in the group, or list of profiles enclosed in [ ]
+ file-blocking — File blocking profile to include in the group, or list of profiles enclosed in [ ]
+ spyware — Spyware default profile or profile name to include in the group, or list of profiles enclosed in [ ]
+ url-filtering — URL filtering default profile or profile name to include in the group, or list of profiles enclosed in [ ]
+ virus — AV default profile or profile name to include in the group, or list of profiles enclosed in [ ]
+ vulnerability — Vulnerability default profile or profile name to include in the group, or list of profiles enclosed in [ ]

Required Privilege Level

superuser, vsysadmin, deviceadmin

set profiles

Specifies settings for security profiles that can be applied to security policies.

Syntax

```
set profiles
   {
   custom-url-category <name> |
     {
     description <value> |
     list <value>
     }
   data-filtering <name> |
     {
     data-capture {no | yes} |
     description <value> |
     rules <name>
        {
        alert-threshold <value> |
        block-threshold <value> |
        data-object <value> |
        direction {both | download | upload} |
        application {any | <value>} |
        file-type {any | <value>}
        }
     }
   data-objects <name> |
     {
     description <value> |
     credit-card-numbers {weight <value>} |
     pattern <name> {regex <value> | weight <value>} |
     social-security-numbers {weight <value>} |
     social-security-numbers-without-dash {weight <value>}
     } |
   decryption <name> |
     {
     interface <name> |
     ssh-proxy |
        {
        block-if-no-resource {no | yes} |
        block-ssh-errors {no | yes} |
        block-unsupported-alg {no | yes} |
        block-unsupported-version {no | yes}
        }
     ssl-forward-proxy |
        {
        block-client-cert {no | yes} |
        block-expired-certificate {no | yes} |
        block-if-no-resource {no | yes} |
        block-unsupported-cipher {no | yes} |
        block-unsupported-version {no | yes} |
        block-untrusted-issuer {no | yes} |
        restrict-cert-exts {no | yes}
        }
     ssl-inbound-proxy
        {
        block-if-no-resource {no | yes} |
        block-unsupported-cipher {no | yes} |
        block-unsupported-version {no | yes}
        forwarded-only {no | yes}
     }}
  dos-protection <name> |
     {
     description <value> |
     type {aggregate | classified} |
     flood |
        {
        icmp |
           {
           enable {no | yes} |
           red
              {
              activate-rate <value> |
              alarm-rate <value> |
              maximal-rate <value>
              block {duration <value>}
              }
           }
        icmpv6 |
           {
           enable {no | yes} |
           red
              {
              activate-rate <value> |
              alarm-rate <value> |
              maximal-rate <value>
              block {duration <value>}
              }
           }
        other-ip |
           {
           enable {no | yes} |
           red
              {
              activate-rate <value> |
              alarm-rate <value> |
              maximal-rate <value>
              block {duration <value>}
              }
           }
        tcp-syn |
           {
           enable {no | yes} |
           red
              {
```

```
                activate-rate <value> |
                alarm-rate <value> |
                maximal-rate <value>
                block {duration <value>}
                }
             syn-cookies
                {
                activate-rate <value> |
                alarm-rate <value> |
                maximal-rate <value>
                block {duration <value>}
                }
             }
          udp
             {
             enable {no | yes} |
             red
                {
                activate-rate <value> |
                alarm-rate <value> |
                maximal-rate <value>
                block {duration <value>}
                }
             }
          }
       resource
          {
          sessions
             {
             enabled {no | yes} |
             max-concurrent-limit <value>
             }
          }
       }
    file-blocking <name> |
       {
       description <value> |
       rules <name>
          {
          action {alert | block | continue} |
          direction {both | download | upload} |
          application {any | <value>} |
          file-type {any | <value>}
          }
       }
    hip-objects <name> |
       {
       description <value> |
       anti-spyware |
          {
          exclude-vendor {no | yes} |
          criteria |
             {
             is-installed {no | yes} |
            real-time-protection {no | not-available | yes} |
            last-scan-time |
               {
               not-available |
               not-within {days <value> | hours <value>} |
               within {days <value> | hours <value>}
               }
            product-version |
               {
               contains <value> |
               greater-equal <value> |
               greater-than <value> |
               is <value> |
               is-not <value> |
               less-equal <value> |
               less-than <value> |
               not-within versions <value> |
               within versions <value>
               }
            virdef-version
               {
               not-within {days <value> | versions <value>} |
               within {days <value> | versions <value>}
               }
            }
         vendor <name> {product <name>}
         }
      antivirus |
         {
         exclude-vendor {no | yes} |
         criteria |
            {
            is-installed {no | yes} |
            real-time-protection {no | not-available | yes} |
            last-scan-time |
               {
               not-available |
               not-within {days <value> | hours <value>} |
               within {days <value> | hours <value>}
               }
            product-version |
               {
               contains <value> |
               greater-equal <value> |
               greater-than <value> |
               is <value> |
               is-not <value> |
               less-equal <value> |
               less-than <value> |
               not-within versions <value> |
               within versions <value>
               }
            virdef-version
               {
```

```
         not-within {days <value> | versions <value>} |
         within {days <value> | versions <value>}
         }
      }
   vendor <name> {product <name>}
   }
custom-checks criteria |
   {
   plist <name> |
      {
      negate {no | yes} |
      key <key_name>
         {
         negate {no | yes} |
         value <key_value>
         }
      }
   process-list <name> {running {no | yes}} |
   registry-key <value>
      {
      default-value-data  <value> |
      negate {no | yes} |
      registry-value <name>
         {
         negate {no | yes} |
         value-data <value>
         }
      }
   }
data-loss-prevention |
   {
   exclude-vendor {no | yes} |
   criteria |
      {
      is-installed {no | yes} |
      is-enabled|
         {
         not-available |
         no |
         yes
         }
      }
   vendor <name> {product <name>}
   }

disk-backup |
   {
   exclude-vendor {no | yes} |
   criteria |
      {
      is-installed {no | yes} |
      last-backup-time |
         {
         not-available |
         not-within {days <value> | hours <value>} |
         within {days <value> | hours <value>}
         }
      }
   vendor <name> {product <name>}
   }
disk-encryption |
   {
   exclude-vendor {no | yes} |
   criteria |
      {
      is-installed {no | yes} |
      encrypted-locations <value> |
         {
         encryption-state is {full | none | not-available | partial} |
         encryption-state is-not {full | none | not-available | partial} |
         }
      }
   vendor <name> {product <name>}
   }
firewall |
   {
   exclude-vendor {no | yes} |
   criteria |
      {
      is-enabled {no | not-available | yes} |
      is-installed {no | yes}
      }
   vendor <name> {product <name>}
   }
host-info criteria |
   {
   client-version {contains | is | is-not} <value> |
   domain {contains | is | is-not} <value> |
   host-name {contains | is | is-not} <value> |
   os contains {Apple | Microsoft} <value>
   }
mobile-device criteria {
   {
   disk-encrypted {no | yes} |
   jailbroken {no | yes} |
   managed-by-mdm {no | yes} |
   passcode-set {no | yes} |
   applications
   {
      has-malware {no | yes} |
      includes <value> {hash <value>} {package <name>} |
   }
   imei {is <value> | is-not <value> | contains <value>} |
   last-checkin-time {not-within <value> | within <value>} |
   model {is <value> | is-not <value> | contains <value>} |
   phone-number {is <value> | is-not <value> | contains <value>} |
   serial-number {is <value> | is-not <value> | contains <value>} |
   tag {is <value> | is-not <value> | contains <value>} |
          }
       }
    network-info criteria {is <value> | is-not <value>}
    patch-management
       {
       exclude-vendor {no | yes} |
       criteria |
          {
          is-enabled {no | not-available | yes} |
          is-installed {no | yes}|
          missing-patches
             {
             check {has-all | has-any | has-none} |
             patches <value> |
             severity
                {
                greater-equal <value> |
                greater-than <value> |
                is <value> |
                is-not <value> |
                less-equal <value> |
                less-than <value>
                }
             }
          }
       vendor <name> {product <name>}
       }
    }
 hip-profiles <name> |
    {
    description <value> |
    match <value>
    }
 spyware <name> |
    {
    description <value> |
    botnet-domains
       {
       packet-capture {no | yes} |
       passive-dns {no | yes} |
       action {alert | allow | block} |
       threat-exception <threat_id>
       }
    rules <value>
       {
       category {any | <value>} |
       packet-capture {no | yes} |
       threat-name {any | <value>} |
       action
          {alert |
          allow |
          block |
          default |
          sinkhole
```

```
            {ipv4-address <address> | ipv6-address <address>} |
         }
      severity {any | critical | high | informational | low | medium | <value>} |
      }
   threat-exception <threat_id>
      {
      packet-capture {no | yes} |
      action |
         {
         block-ip |
            {
            duration <value> |
            track-by {source | source-and-destination}
            }
         alert |
         allow |
         default |
         drop |
         drop-all-packets |
         reset-both |
         reset-client |
         reset-server
         }
      exempt-ip <ip_address>
      }
   }
url-filtering <name> |
   {
   action {alert | block | continue | override} |
   description <value> |
   dynamic-url {no | yes} |
   enable-container-page {no | yes} |
   license-expired {allow | block} |
   log-container-page-only {no | yes} |
   log-http-hdr-referer {no | yes} |
   log-http-hdr-user-agent {no | yes} |
   log-http-hdr-xff {no | yes} |
   safe-search-enforcement {no | yes} |
   alert <value> |
   allow <value> |
   allow-list <value> |
   block <value> |
   block-list <value> |
   continue <value> |
   override <value>
   }
virus <name>
   {
   description <value> |
   packet-capture {no | yes} |
   application <name> {action {alert | allow | block | default}} |
   decoder <name> |
      {
      action {alert | allow | block | default} |
      wildfire-action {alert | allow | block | default}
      }
   threat-exception <threat_id>
   }
vulnerability <name>
   {
   description <value> |
   rules <value> |
      {
      category {any | <value>} |
      host {any | client | server} |
      packet-capture {no | yes} |
      threat-name {any | <value>} |
      action |
         {
         alert |
         block-ip |
            {
            duration <value> |
            track-by {source | source-and-destination}
            }
         default |
         drop |
         drop-all-packets |
         reset-both |
         reset-client |
         reset-server
         }
      cve {any | <value>} |
      severity {any | <value>} |
      vendor-id {any | <value>}
      }
   threat-exception <threat_id> |
      {
      packet-capture {no | yes} |
      action |
         {
         alert |
         allow |
         block-ip |
            {
            duration <value> |
            track-by {source | source-and-destination}
            }
         default |
         drop |
         drop-all-packets |
         reset-both |
         reset-client |
         reset-server
         }
      exempt-ip <ip_address> |
      time-attribute
         {
             interval <value> |
             threshold <value> |
             track-by {destination | source | source-and-destination}
             }
         }
     }
 }
```

Options

> custom-url-category — Custom URL category profiles
 + description — Profile description
 + list — List; specify member value or list of values enclosed in [ ]
> data-filtering — Data filtering profiles
 + data-capture — Data capture option
 + description — Profile description
 > rules — Data filtering rules for the profile
  + alert-threshold — Alert threshold value (0-65535)
  + block-threshold — Block threshold value (0-65535)
  + data-object — Data object value
  + direction — Direction for data filtering (both, download, or upload)
  > application — Application name or list of values enclosed in [ ]; press <tab> for list of applications; option to include all applications (any)
  > file-type — File type or list of values enclosed in [ ]; press <tab> for list of file types; option to include all types (any)
> data-objects — Data objects profiles
 + description — Description of the profile
 > credit-card-numbers — Credit card numbers; option to specify weight (0-255)
 > pattern — Pattern; option to specify a regular expression value and weight (0-255)
 > social-security-numbers — Social security numbers; option to specify weight (0-255)
 > social-security-numbers-without-dash — Social security numbers without dash; option to specify weight (0-255)
> decryption — Decryption profiles
 > interface <name>
 > ssh-proxy — Secure Shell (SSH) proxy profile settings
  + block-if-no-resource — Whether to block sessions if device has not enough resources
  + block-ssh-errors — Whether to block sessions if SSH errors are encountered
  + block-unsupported-alg — Whether to block sessions if SSH algorithm is not supported
  + block-unsupported-version — Whether to block sessions if ssh version is not supported
 > ssl-forward-proxy — Secure Socket Layer (SSL) forwarding proxy
  + block-client-cert — Whether to block sessions if client certificate authentication is used
  + block-expired-certificate — Whether to block sessions if server's certificate is expired
  + block-if-no-resource — Whether to block sessions if device has not enough resources
  + block-unsupported-cipher — Whether to block sessions if SSL cipher suite is not supported
  + block-unsupported-version — Whether to block sessions if SSL version is not supported
  + block-untrusted-issuer — Whether to block sessions if server's certificate is issued by untrusted CA
  + restrict-cert-exts — Whether to restrict certificates' extensions
 > ssl-inbound-proxy — SSL inbound proxy
  + block-if-no-resource — Whether to block sessions if device has not enough resources
  + block-unsupported-cipher — Whether to block sessions if SSL cipher suite is not supported
  + block-unsupported-version — Whether to block sessions if SSL version is not supported
  + forwarded-only — Mirror after security policy allow
> dos-protection — Denial of Service (DoS) protection profiles
 + description — Description of the profile
 + type — Type (aggregate or classified)
 > flood — Flood protection

```
        > icmp — ICMP flood protection
            + enable — Enable ICMP flood protection
            > red — Random Early Drop (RED)
                + activate-rate — Packet rate (pps) to start RED (1-2000000)
                + alarm-rate — Packet rate (pps) to generate alarm (0-2000000)
                + maximal-rate — Maximal packet rate (pps) allowed (1-2000000)
                > block — Parameters for blocking
                    + duration — Duration (1-21600)
        > icmpv6 — ICMPv6 flood protection
            + enable — Enable ICMPv6 flood protection
            > red — Random Early Drop (RED)
                + activate-rate — Packet rate (pps) to start RED (1-2000000)
                + alarm-rate — Packet rate (pps) to generate alarm (0-2000000)
                + maximal-rate — Maximal packet rate (pps) allowed (1-2000000)
                > block — Parameters for blocking
                    + duration — Duration (1-21600)
        > other-ip — Other IP protocols protection
            + enable — Enable other IP flood protection
            > red — Random Early Drop (RED)
                + activate-rate — Packet rate (pps) to start RED (1-2000000)
                + alarm-rate — Packet rate (pps) to generate alarm (0-2000000)
                + maximal-rate — Maximal packet rate (pps) allowed (1-2000000)
                > block — Parameters for blocking
                    + duration — Duration (1-21600)
        > tcp-syn — TCP synchronies packet (SYN) flood protection
            + enable — Enable SYN flood protection
            > red — Random Early Drop (RED)
                + activate-rate — Packet rate (pps) to start RED (1-2000000)
                + alarm-rate — Packet rate (pps) to generate alarm (0-2000000)
                + maximal-rate — Maximal packet rate (pps) allowed (1-2000000)
                > block — Parameters for blocking
                    + duration — Duration (1-21600)
            > syn-cookies — SYN cookies
                + activate-rate — Packet rate (pps) to activate SYN cookies proxy (0-2000000)
                + alarm-rate — Packet rate (pps) to generate alarm (0-2000000)
                + maximal-rate — Maximal packet rate (pps) allowed (1-2000000)
                > block — Parameters for blocking
                    + duration — Duration (1-21600)
        > udp — UDP flood protection
            + enable — Enable UDP flood protection
            > red — Random Early Drop (RED)
                + activate-rate — Packet rate (pps) to start RED (1-2000000)
                + alarm-rate — Packet rate (pps) to generate alarm (0-2000000)
                + maximal-rate — Maximal packet rate (pps) allowed (1-2000000)
                > block — Parameters for blocking
                    + duration — Duration (1-21600)
    > resource — Parameters to protect resources
        > sessions — Parameters to protect excessive sessions
            + enabled — Enable session protections
            + max-concurrent-limit — Maximum concurrent limit (1-2097152)
> file-blocking — File blocking profiles
    + description — Description of the profile
    > rules — File blocking rules for the profile
        + action — Action (alert, block, or continue)
        + direction — Direction for file blocking (both, download, or upload)
        > application — Application name or list of values enclosed in [ ]; press <tab> for list of applications; option to include
            all applications (any)
        > file-type — File type or list of values enclosed in [ ]; press <tab> for list of file types; option to include all types (any)
> hip-objects — Host Identity Protocol (HIP) objects profiles
    + description — Description of the profile
    > anti-spyware — Anti-spyware HIP objects
        + exclude-vendor — Exclude vendor (no or yes)
        > criteria — Matching criteria
            + is-installed — Is installed (no or yes)
            + real-time-protection — Real time protection (no, not available, or yes)
            > last-scan-time — Last full scan time
                > not-within — Not-within; specify time in days or hours (1-65535)
                > within — Within; specify time in days or hours (1-65535)
                - not-available — Last scan time not available
            > product-version — Specify product versions
                > contains — Contains specified value
                > greater-equal — Greater than or equal to specified value
                > greater-than — Greater than specified value
                > is — Is specified value
                > is-not — Is not specified value
                > less-equal — Less than or equal to specified value
                > less-than — Less than specified value
                > not-within — Not within versions range (1-65535)
                > within — Within versions range (1-65535)
            > virdef-version — Virus definition version
                > not-within — Not within; specify time in days or versions range (1-65535)
                > within — Within; specify time in days or versions range (1-65535)
        > vendor — Vendor name
            > product — Product name (value or list of values enclosed in [ ])
    > antivirus — Antivirus HIP objects
        + exclude-vendor — Exclude vendor (no or yes)
        > criteria — Matching criteria
            + is-installed — Is installed (no or yes)
            + real-time-protection — Real time protection (no, not available, or yes)
            > last-scan-time — Last full scan time
                > not-within — Not-within; specify time in days or hours (1-65535)
                > within — Within; specify time in days or hours (1-65535)
                - not-available — Last scan time not available
            > product-version — Specify product versions
                > contains — Contains specified value
                > greater-equal — Greater than or equal to specified value
                > greater-than — Greater than specified value
                > is — Is specified value
                > is-not — Is not specified value
                > less-equal — Less than or equal to specified value
                > less-than — Less than specified value
                > not-within — Not within versions range (1-65535)
                > within — Within versions range (1-65535)
            > virdef-version — Virus definition version
                > not-within — Not within; specify time in days or versions range (1-65535)
                > within — Within; specify time in days or versions range (1-65535)
        > vendor — Vendor name
            > product — Product name (value or list of values enclosed in [ ])
    > custom-checks — Custom checks HIP objects
        > criteria — Matching criteria
            > plist — Preference list name
                + negate — Plist does not exist
                > key — Key name
                    + negate — Value does not exist or match specified value data
                    + value — Key value
            > process-list — Process list name; option to specify running
            > registry-key — Registry key value
                + default-value-data — Registry key default value data
                + negate — Key does not exist or match specified value data
                > registry-value — Registry value
                    + negate — Value does not exist or match specified value data
                    + value-data — Registry value data
    > data-loss-prevention — Settings for data loss prevention
        + exclude-vendor — Exclude vendor (no or yes)
        > criteria — Matching criteria
            + is-installed — Is installed (no or yes)
            > last-backup-time — Last full backup time
                > not-within — Not-within; specify time in days or hours (1-65535)
                > within — Within; specify time in days or hours (1-65535)
                - not-available — Last scan time not available
        > vendor — Vendor name
            > product — Product name (value or list of values enclosed in [ ])

    > disk-backup — Disk backup HIP objects
        + exclude-vendor — Exclude vendor (no or yes)
        > criteria — Matching criteria
            + is-installed — Is installed (no or yes)
            > is-enabled — Is enabled (no or yes)
        > vendor — Vendor name
            > product — Product name (value or list of values enclosed in [ ])
    > disk-encryption — Disk encryption HIP objects
        + exclude-vendor — Exclude vendor (no or yes)
        > criteria — Matching criteria
            + is-installed — Is installed (no or yes)
            > encrypted-locations — Specify encryption location
                > encryption-state is — Encryption state is full, none, not-available, or partial
                > encryption-state is-not — Encryption state is not full, none, not-available, or partial
        > vendor — Vendor name
            > product — Product name (value or list of values enclosed in [ ])
    > firewall — Firewall HIP objects
        + exclude-vendor — Exclude vendor (no or yes)
        > criteria — Matching criteria
            + is-enabled — Is enabled (no, not available, or yes)
            + is-installed — Is installed (no or yes)
        > vendor — Vendor name
            > product — Product name (value or list of values enclosed in [ ])
    > host-info — Host information HIP objects
        > criteria — Matching criteria
            > client-version — Client version contains, is, or is not value
            > domain — Domain contains, is, or is not value
            > host-name — Host name contains, is, or is not value
            > os — OS contains Apple vendor or Windows vendor value
    > mobile-device— Mobile device objects
        > criteria — Matching criteria
            + disk-encrypted — If disk encrypted (no or yes)
            + jailbroken — If disk encrypted (no or yes)
            + managed-by-mdm — If managed by Mobile Security Manager (no or yes)
            + passcode-set — If a password is set (no or yes)
            > applications — Specify if has malware and any hash value or package name
            > imei — Is, is not, or contains specified International Mobile Equipment Identity (IMEI)
            > last-checkin-time — Within or not within value
            > model — Is, is not, or contains value
            > phone-number — Is, is not, or contains value
            > serial-number — Is, is not, or contains value
            > tag — Is, is not, or contains value
    > os — OS contains Apple vendor or Windows vendor value
    > patch-management — Patch management HIP objects
        + exclude-vendor — Exclude vendor (no or yes)
        > criteria — Matching criteria
            + is-enabled — Is enabled (no, not available, or yes)
            + is-installed — Is installed (no or yes)
            > missing-patches — Missing patches criteria
                + check — Check has all, has any, or has none
                + patches — Patch security bulletin ID or KB article ID (specify value or list of values enclosed in [ ])
                > severity   Severity
                    > greater-equal — Greater than or equal to specified value (0-100000)
                    > greater-than — Greater than specified value (0-100000)
                    > is — Is specified value (0-100000)
                    > is-not — Is not specified value (0-100000)
                    > less-equal — Less than or equal to specified value (0-100000)
                    > less-than — Less than specified value (0-100000)
        > vendor — Vendor name
            > product — Product name (value or list of values enclosed in [ ])
> hip-profiles — Host Identity Protocol (HIP) profiles
    + description — Profile description
    + match — Match value
> spyware — Spyware profiles
    + description — Profile description
    > botnet-domains - Spyware profile settings for botnets
        + packet-capture — Packet capture (no or yes)
        > action — Action for botnet domains (alert, allow, block, or sinkhole)
            > sinkhole — IP address of sinkhole for botnets
                + ipv4-address (address)
                + ipv6-address (address)
        > threat-exception — Threat ID for exception
    > rules — Spyware profile rules (rule name is alphanumeric string [  0-9a-zA-Z._-])
        + category — Category (any or specify a category)
        + packet-capture — Packet capture (no or yes)
        + passive-dns— Passive DNS (no or yes)
        + threat-name — Threat name (any or specify a name)
        > action — Rule action (alert, allow, block, default)
        > severity — Severity (all severities or specify value or list of values enclosed in [ ])
    > threat- exception — Specify a threat ID
        + packet-capture — Packet capture (no or yes)
        > action — Exception action (alert, allow, default, drop, drop all packets, reset client, reset server, or reset both)
        > exempt-ip — IP address where exempt
> url-filtering — URL filtering profiles
    + action — Action for block list items (alert, block, continue, override)
    + description — Profile description
    + dynamic-url — Dynamic URL filtering (for BrightCloud only)
    + enable-container-page — Track container page
    + license-expired — Action when URL filtering license expires (allow or block) (for BrightCloud only)
    + log-container-page-only   Log container page only
    + log-http-hdr-referer      Log HTTP Header Referer field
    + log-http-hdr-user-agent   Log HTTP Header User-Agent field
    + log-http-hdr-xff          Log HTTP Header X-Forwarded-For field
    + log-container-page-only — Log container page only
    +safe-search-enforcement — Enable the safe search option (yes or no)
    > alert — Categories to alert on (value or list of values enclosed in [ ])
    > allow — Categories to allow (value or list of values enclosed in [ ])
    > allow-list — Host or IP address to pass (e.g. www.hotmail.com or www.cnn.com/news) (value or list of values enclosed in [ ])
    > block — Categories to block (value or list of values enclosed in [ ])
    > block-list — Host or IP address to block (e.g. www.hotmail.com or www.cnn.com/news) (value or list of values enclosed in [ ])
    > continue — Categories to block/continue (value or list of values enclosed in [ ])
    > override — Categories to administratively override (value or list of values enclosed in [ ])
> virus — Virus profiles
    + description — Profile description
    + packet-capture — Packet capture (no or yes)
    > application — Application name
        + action — Action to take (alert, allow, block, or default)
    > decoder — Decoder name
        + action — Action to take (alert, allow, block, or default)
        + wildfire-action — Action for Wildfire to take (alert, allow, block, or default)
    > threat-exception — Specify a threat ID
> vulnerability — Vulnerability profiles
    + description — Profile description
    > rules — Spyware profile rules (rule name is alphanumeric string [  0-9a-zA-Z._-])
        + category — Category (any or specify a category)
        + host — Host (any, client, server)
        + packet-capture — Packet capture (no or yes)
        + threat-name — Threat name (any or specify a name)
        > action — Rule action (alert, allow, block, default)
        > cve — Common Vulnerabilities and Exposures (CVE) (all or specify a CVE identifier or list of identifiers enclosed in [ ])
        > severity — Severity (all severities or specify value or list of values enclosed in [ ])
        > vendor-id — Vendor ID (all or specify a vendor or list of vendors enclosed in [ ])
    > threat-exception — Specify a threat ID
        + packet-capture — Packet capture (no or yes)
        > action — Exception action (alert, allow, default, drop, drop all packets, reset client, reset server, reset both, or block IP address)
            > block-ip — Block IP address
                + duration — Duration for blocking the IP address (1-3600)
                + track-by — Track by source or source and destination
        > exempt-ip — IP address to exempt
        > time-attribute — Exception time attribute
            + interval — Interval value (1-3600)
            + threshold — Threshold value (1-255)
            + track-by — Track by destination, source, or source and destination
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set region

Defines a custom region on the firewall. The firewall supports creation of policy rules that apply to specified countries or other regions. The region is available as an option when specifying source and destination for security policies, SSL decryption policies, and DoS policies. A standard list of countries is available by default. This command allows you to define custom regions to include as options for security policy rules.

Syntax

```
set region <code>
   {
   address {<value> | {<ip address/netmask> | <address object>} | <ip_range>} |
   geo-location |
     {
     latitude <coordinate> |
     longitude <coordinate>
     }
   }
```

Options

<code> — Region to configure (two-character code; press <tab> for list)
+ address — IP address and network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or IPv6-range), or list of values enclosed in [ ]
> geo-location — Device geographic location
   + latitude — Latitude coordinate
   + longitude — Longitude coordinate

Required Privilege Level

superuser, vsysadmin, deviceadmin

set report-group

Specifies settings for report groups. Report groups allow you to create sets of reports that the system can compile and send as a single aggregate PDF report with an optional title page and all the constituent reports included.

Syntax

```
set report-group <name> |
   {
   title-page {no | yes} |
   custom-widget <value> |
     {
     custom-report <value> |
     log-view <value> |
     pdf-summary-report <value>
     }
   predefined user-activity-report |
   variable <name> {value <value>}
   }
```

Options

<name> — Report group to configure
+ title-page — Include title page
> custom-widget — Custom-widget value
    > custom-report — Custom report value
    > log-view — Log view value
    > pdf-summary-report — PDF summary report value
> predefined — Predefined user activity report
> variable — Variable name; option to include a value

Required Privilege Level

superuser, vsysadmin, deviceadmin

set reports

Specifies settings for generating reports.

Syntax

```
set reports <name>
   {
   caption <value> |
   disabled {no | yes} |
   end-time <value> |
   frequency daily |
   period {last-12-hrs | last-15-minutes | last-24-hrs | last-30-days | last-60-seconds
     | last-7-calendar-days | last-7-days | last-calendar-day | last-calendar-month |
     last-calendar-week | last-hour} |
   query <value> |
   start-time <value> |
   topm <value> |
   topn <value> |
   type
     {
     appstat |
        {
        group-by {category-of-name | container-of-name | day-of-receive_time | hour-
           of-receive_time | name | quarter-hour-of-receive_time | risk | risk-of-name
           | subcategory-of-name | technology-of-name | vsys} |
        sortby {nbytes | npkts | nsess | nthreats} |
        aggregate-by {category-of-name | container-of-name | day-of-receive_time |
           hour-of-receive_time | name | quarter-hour-of-receive_time | risk | risk-
           of-name | subcategory-of-name | technology-of-name | vsys | <value>} |
        labels <value> |
        values {nbytes | npkts | nsess | nthreats | <value>}
        }
     data |
        {
        group-by {action | app | category-of-app | container-of-app | day-of-
           receive_time | direction | dport | dst | dstloc | dstuser | from | hour-of-
           receive_time | inbound_if | misc | natdport | natdst | natsport | natsrc |
           outbound_if | proto | quarter-hour-of-receive_time | risk-of-app | rule |
           severity | sport | src | srcloc | srcuser | subcategory-of-app | subtype |
           technology-of-app | threatid | to | vsys} |
        sortby repeatcnt |
        aggregate-by {action | app | category-of-app | container-of-app | day-of-
           receive_time | direction | dport | dst | dstloc | dstuser | from | hour-of-
           receive_time | inbound_if | misc | natdport | natdst | natsport | natsrc |
           outbound_if | proto | quarter-hour-of-receive_time | risk-of-app | rule |
           severity | sport | src | srcloc | srcuser | subcategory-of-app | subtype |
           technology-of-app | threatid | to | vsys | <value>} |
        labels <value> |
        values {repeatcnt | <value>}
        }
     hipmatch |
        {
        group-by {day-of-receive_time | hour-of-receive_time | machinename | matchname
           | matchtype | quarter-hour-of-receive_time | src | srcuser | vsys} |
        last-match-by time_generated |
        aggregate-by {day-of-receive_time | hour-of-receive_time | machinename |
           matchname | matchtype | quarter-hour-of-receive_time | src | srcuser | vsys
           | <value>} |
        labels <value> |
        values {repeatcnt | <value>}
        }
     threat |
        {
        group-by {action | app | category-of-app | container-of-app | day-of-
           receive_time | direction | dport | dst | dstloc | dstuser | from | hour-of-
           receive_time | inbound_if | misc | natdport | natdst | natsport | natsrc |
           outbound_if | proto | quarter-hour-of-receive_time | risk-of-app | rule |
           severity | sport | src | srcloc | srcuser | subcategory-of-app | subtype |
           technology-of-app | threatid | to | vsys} |
        sortby repeatcnt |
        aggregate-by {action | app | category-of-app | container-of-app | day-of-
           receive_time | direction | dport | dst | dstloc | dstuser | from | hour-of-
           receive_time | inbound_if | misc | natdport | natdst | natsport | natsrc |
           outbound_if | proto | quarter-hour-of-receive_time | risk-of-app | rule |
           severity | sport | src | srcloc | srcuser | subcategory-of-app | subtype |
           technology-of-app | threatid | to | vsys | <value>} |
        labels <value> |
        values {repeatcnt | <value>}
        }
     thsum |
        {
        group-by {app | category-of-app | container-of-app | day-of-receive_time | dst
           | dstloc | dstuser | from | hour-of-receive_time | quarter-hour-of-
           receive_time | risk-of-app | rule | severity-of-threatid | src | srcloc |
           srcuser | subcategory-of-app | subtype | technology-of-app | threatid | to
           | vsys} |
        sortby count |
        aggregate-by {app | category-of-app | container-of-app | day-of-receive_time |
           dst | dstloc | dstuser | from | hour-of-receive_time | quarter-hour-of-
           receive_time | risk-of-app | rule | severity-of-threatid | src | srcloc |
           srcuser | subcategory-of-app | subtype | technology-of-app | threatid | to
           | vsys | <value>} |
        labels <value> |
        values {count | <value>}
        }
     traffic |
        {
        group-by {action | app | category | category-of-app | container-of-app | day-
           of-receive_time | dport | dst | dstloc | dstuser | from | hour-of-
           receive_time | inbound_if | natdport | natdst | natsport | natsrc |
           outbound_if | proto | quarter-hour-of-receive_time | risk-of-app | rule |
           sessionid | sport | src | srcloc | srcuser | subcategory-of-app |
           technology-of-app | to | vsys} |
        sortby {bytes | bytes_received | bytes_sent | elapsed | packets |
           ptks_received | pkts_sent | repeatcnt} |
        aggregate-by {action | app | category | category-of-app | container-of-app |
           day-of-receive_time | dport | dst | dstloc | dstuser | from | hour-of-
           receive_time | inbound_if | natdport | natdst | natsport | natsrc |
           outbound_if | proto | quarter-hour-of-receive_time | risk-of-app | rule |
           sessionid | sport | src | srcloc | srcuser | subcategory-of-app |
           technology-of-app | to | vsys | <value>} |
        labels <value> |
        values {bytes | bytes_received | bytes_sent | elapsed | packets |
           ptks_received | pkts_sent | repeatcnt | <value>}
        }
     trsum |
        {
        group-by {app | category | category-of-app | container-of-app | day-of-
           receive_time | dst | dstuser | from | hour-of-receive_time | quarter-hour-
           of-receive_time | risk-of-app | rule | src | srcuser | subcategory-of-app |
           technology-of-app | to | vsys} |
        sortby {bytes | sessions} |
        aggregate-by {app | category | category-of-app | container-of-app | day-of-
           receive_time | dst | dstuser | from | hour-of-receive_time | quarter-hour-
           of-receive_time | risk-of-app | rule | src | srcuser | subcategory-of-app |
           technology-of-app | to | vsys | <value>} |
        labels <value> |
        values {bytes | sessions | <value>}
        }
     url
        {
        group-by {action | app | category | category-of-app | container-of-app |
           contenttype | day-of-receive_time | direction | dport | dst | dstloc |
           dstuser | from | hour-of-receive_time | inbound_if | misc | natdport |
           natdst | natsport | natsrc | outbound_if | proto | quarter-hour-of-
           receive_time | risk-of-app | rule | severity | sport | src | srcloc |
           srcuser | subcategory-of-app | technology-of-app | to | vsys} |
        sortby repeatcnt |
        aggregate-by {action | app | category | category-of-app | container-of-app |
           contenttype | day-of-receive_time | direction | dport | dst | dstloc |
           dstuser | from | hour-of-receive_time | inbound_if | misc | natdport |
           natdst | natsport | natsrc | outbound_if | proto | quarter-hour-of-
           receive_time | risk-of-app | rule | severity | sport | src | srcloc |
           srcuser | subcategory-of-app | technology-of-app | to | vsys | <value>} |
        labels <value> |
        values {repeatcnt | <value>}
        }
     }
  }
```

Options

<name> — Report to configure
+ caption — Caption value
+ disabled — Disabled (no or yes)
+ end-time — End time (e.g. 2008/12/31 11:59:59)
+ frequency — Configure the report to automatically run daily.
+ period — Time period to include in report (last 12 hrs, last 15 minutes, last 24 hrs, last 30 days, last 60 seconds, last 7 calendar days, last 7 days, last calendar day, last calendar month, last calendar week, or last hour)

```
+ query — Query value
+ start-time — Start time (e.g. 2008/01/01 09:00:00)
+ topm — TopM value (1-50)
+ topn — TopN value (1-500)
> type — Report type
    > appstat — Appstat report
        + group-by — Group by category of name, container of name, day of receive time, hour of receive time, name, quarter hour of receive time, risk, risk of name, subcategory of name, technology of name, or virtual system
        + sortby — Sort by nbytes, npkts, nsess, or nthreats
        > aggregate-by — Aggregate by category of name, container of name, day of receive time, hour of receive time, name, quarter hour of receive time, risk, risk of name, subcategory of name, technology of name, virtual system, or list of values enclosed in [ ]
        > labels — Label value or list of values enclosed in [ ]
        > values — Values (nbytes, npkts, nsess, nthreats, or list of values enclosed in [ ])
    > data — Data report
        + group-by — Select from the list provided
        + sortby — Sort by repeat count
        > aggregate-by — Select from the list provided or specify a list of values enclosed in [ ]
        > labels — Label value or list of values enclosed in [ ]
        > values — Values (repeat count, or list of values enclosed in [ ])
    > hipmatch — HIP match report
        + group-by — Select from the list provided
        + last-match-by — Last match by time generated
        > aggregate-by — Select from the list provided or specify a list of values enclosed in [ ]
        > labels — Label value or list of values enclosed in [ ]
        > values — Values (repeat count, or list of values enclosed in [ ])
    > threat — Threat report
        + group-by — Select from the list provided
        + sortby — Sort by repeat count
        > aggregate-by — Select from the list provided or specify a list of values enclosed in [ ]
        > labels — Label value or list of values enclosed in [ ]
        > values — Values (repeat count, or list of values enclosed in [ ])
    > thsum — thsum report
        + group-by — Select from the list provided
        + sortby — Sort by count
        > aggregate-by — Select from the list provided or specify a list of values enclosed in [ ]
        > labels — Label value or list of values enclosed in [ ]
        > values — Values (count, or list of values enclosed in [ ])
    > traffic — Traffic report
        + group-by — Select from the list provided
        + sortby — Sort by bytes, bytes received, bytes sent, elapsed, packets, packets received, packets sent, or repeatcnt
        > labels — Label value or list of values enclosed in [ ]
        > aggregate-by — Select from the list provided or specify a list of values enclosed in [ ]
        > values — Values (bytes, bytes received, bytes sent, elapsed, packets, packets received, packets sent, repeatcnt, or list of values enclosed in [ ])
    > trsum — trsum report
        + group-by — Select from the list provided
        + sortby — Sort by bytes or sessions
        > aggregate-by — Select from the list provided or specify a list of values enclosed in [ ]
        > labels — Label value or list of values enclosed in [ ]
        > values — Values (bytes, sessions, or list of values enclosed in [ ])
    > url — URL report
        + group-by — Select from the list provided
        + sortby — Sort by repeat count
```

> aggregate-by — Select from the list provided or specify a list of values enclosed in [ ]
> labels — Label value or list of values enclosed in [ ]
> values — Values (repeat count, or list of values enclosed in [ ])

Required Privilege Level

superuser, vsysadmin, deviceadmin

set rulebase or set vsys rulebase

Configures sets of rules for the following policy types: application override, captive portal, SSL decryption, Denial of Service (DoS), Network Address Translation (NAT), Policy-based Forwarding (PBF), Quality of Service (QoS), and security. You also use this command to modify the default security rules.

Syntax

```
set rulebase or set vsys <name> rulebase
   {
   application-override rules <name> |
     {
     application <value> |
     description <value> |
     disabled {no | yes} |
     negate-destination {no | yes} |
     negate-source {no | yes} |
     port <port_number> |
     protocol {tcp | udp} |
     destination {any | <value>} |
     from {any | <value>} |
     source {any | <value>} |
     source-user {any | known-user | pre-logon | unknown | <value>} |
     tag <value> |
     to {any | multicast | <value>}
     }
   captive-portal rules <name> |
     {
     action {browser-challenge | no-captive-portal | web-form} |
     description <value> |
     disabled {no | yes} |
     negate-destination {no | yes} |
     negate-source {no | yes} |
     category {any | <value>} |
     destination {any | <value>} |
     from {any | <value>} |
     service {any | default | service-http | service-https | <value>} |
     source {any | <value>} |
     tag <value> |
     to {any | <value>}
     }
   decryption rules <name> |
     {
     action {decrypt | no-decrypt} |
     description <value> |
     disabled {no | yes} |
     negate-destination {no | yes} |
     negate-source {no | yes} |
     profile <name>
     category {any | <value>} |
     destination {any | <value>} |
     from {any | <value>} |
     source {any | <value>} |
     source-user {any | known-user | pre-logon | unknown | <value>} |
     tag <value> |
     to {any | <value>} |
     type {ssh-proxy | ssl-forward-proxy | ssl-inbound-inspection <value>}
     }
  default-security-rules rules {interzone-default | intrazone-default}
     {
     action {allow | deny} |
     log-end {no | yes} |
     log-setting <value> |
     log-start {no | yes} |
     profile-setting |
        {
        group <value> |
        profiles
           {
           data-filtering <value> |
           file-blocking <value> |
           spyware <value> |
           url-filtering <value> |
           virus <value> |
           vulnerability <value>
           }
     tag |
        }

  dos rules <name> |
     {
     description <value> |
     disabled {no | yes} |
     log-setting <value> |
     negate-destination {no | yes} |
     negate-source {no | yes} |
     schedule <value> |
     action {allow | deny | protect} |
     destination {any | <value>} |
     from {interface <value> | zone <value>} |
     protection |
        {
        aggregate {profile <value>} |
        classified
           {
           profile <value> |
           classification-criteria
              {
              address destination-ip-only |
              address source-ip-only |
              address src-dest-ip-both
              }
           }
        }
     service {any | application-default | service-http | service-https | <value>} |
     source {any | <value>} |
     source-user {any | known-user | pre-logon | unknown | <value>} |
     tag <value> |
     to {interface <value> | zone <value>}
     }
  nat rules <name> |
     {
     active-active-device-binding {0 | 1 | both | primary} |
     description <value> |
     disabled {no | yes} |
     nat-type {ipv4 | nat64} |
     service {any | service-http | service-https | <value>} |
     to-interface {any | <value>} |
     destination {any | <value>} |
     destination-translation |
        {
        translated-address <value> |
        translated-port <value>
        }
     from {any | <value>} |
     source {any | <value>} |
     source-translation |
        {
        dynamic-ip |
           {
           fallback |
              {
              interface-address |
                 {
                 interface <name> |
                 floating-ip <ip_address> |
                 ip <ip_address>
                 }
              translated-address <value>
              }
           translated-address <value>
           }
        dynamic-ip-and-port |
           {
           interface-address |
              {
              interface <interface_name> |
              floating-ip <ip_address> |
              ip <ip_address>
              }
           translated-address <value>
           }
        static-ip
           {
           bi-directional {no | yes} |
           translated-address <value>
           }
        }
     tag <value> |
     to <value>
     }
  pbf rules <name> |
     {
     active-active-device-binding {0 | 1 | both} |
     description <value> |
     disabled {no | yes} |
     negate-destination {no | yes} |
     negate-source {no | yes} |
     schedule <value> |
     action |
        {
        forward |
           {
           egress-interface <value> |
           monitor |
              {
              disable-if-unreachable {no | yes} |
              ip-addresss <ip_address> |
              profile {default | <value>}
              }
           nexthop <ip_address>
           }
        forward-to-vsys <value> |
        discard |
        no-pbf
        }
     application {any | <value>} |
     destination {any | <value>} |
     enforce-symmetric-return |
        {
        enabled {no | yes} |
        nexthop-address-list <value>
        }
     from {interface <value> | zone <value>} |
     service {any | application-default | service-http | service-https | <value>} |
     source {any | <value>} |
     source-user {any | known-user | pre-logon | unknown | <value>} |
     tag <value>
     }
  qos rules <name> |
     {
     description <value> |
     disabled {no | yes} |
     negate-destination {no | yes} |
     negate-source {no | yes} |
     schedule <value> |
     action {class {1 | 2 | 3 | 4 | 5 | 6 | 7 | 8}}
     application <value> |
     category {any | <value>} |
     destination {any | <value>} |
     from {any | <value>} |
     service {any | application-default | service-http | service-https | <value>} |
     source {any | <value>} |
     source-user {any | known-user | pre-logon | unknown | <value>} |
     tag <value> |
     to {any | <value>}
     }
   security rules <name>
     {
     action {allow | deny} |
     description <value> |
     disabled {no | yes} |
     log-end {no | yes} |
     log-setting <value> |
     log-start {no | yes} |
     rule-type {interzone | intrazone | universal}
     negate-destination {no | yes} |
     negate-source {no | yes} |
     rule-type {interzone | intrazone | universal} |
     schedule <value> |
     application <value> |
     category {any | <value>} |
     destination {any | <value>} |
     from {any | <value>} |
     hip-profiles {any | no-hip | <value>} |
     option disable-server-response-inspection {no | yes} |
     profile-setting |
        {
        group <value> |
        profiles
           {
           data-filtering <value> |
           file-blocking <value> |
           spyware <value> |
           url-filtering <value> |
           virus <value> |
           vulnerability <value>
           }
        }
     qos |
        {
        marking ip-dscp <value> |
        marking ip-precedence <value>
        }
     service {any | application-default | service-http | service-https | <value>} |
     source {any | <value>} |
     source-user {any | known-user | pre-logon | unknown | <value>} |
     tag <value> |
     to {any | multicast | <value>}
     }
   }
```

Options

> application-override — Application override rules

+ application — Application (select from list of applications or enter a value)

+ description — Description of rule set

```
    + disabled — Disables the rule
    + negate-destination — Negates destination
    + negate-source — Negates source
    + port — Port number value or list of values enclosed in [ ] (1-65535)
    + protocol — Protocol (TCP or UDP)
    > destination — Destination (any, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or IPv6-range), value or list of values enclosed in [ ])
    > from — From (any zone, value or list of values enclosed in [ ])
    > source — Source (any, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or IPv6-range), value or list of values enclosed in [ ])
    > source-user — Source user (any, known user, pre-logon, unknown, value or list of values enclosed in [ ])
    > tag — Tag (member value or list of values enclosed in [ ])
    > to — To (any zone, value or list of values enclosed in [ ])
> captive-portal — Captive portal rules
    + action — Action (browser challenge, no captive portal, or web form)
    + description — Description of rule set
    + disabled — Disables the rule
    + negate-destination — Negates destination
    + negate-source — Negates source
    > category — URL category (any, specified category, or list of categories enclosed in [ ])
    > destination — Destination (any, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or IPv6-range), value or list of values enclosed in [ ])
    > from — From (any zone, value or list of values enclosed in [ ])
    > service — Service (any, default, predefined HTTP or HTTPS service, value or list of values enclosed in [ ])
    > source — Source (any, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or IPv6-range), value or list of values enclosed in [ ])
    > tag — Tag (member value or list of values enclosed in [ ])
    > to — To (any zone, value or list of values enclosed in [ ])
> decryption — SSL/SSH decryption rules
    + action — Action (decrypt or not decrypt)
    + description — Description of rule set
    + disabled — Disables the rule
    + negate-destination — Negates destination
    + negate-source — Negates source
    + profile — Use this command to add a decryption profile to the decryption rule. Decryption profiles are configured in set profiles decryption.
    > category — URL category (any, specify a URL category, or list of categories enclosed in [ ])
    > destination — Destination (any, region code, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or IPv6-range), value or list of values enclosed in [ ])
    > from — From (any zone, value or list of values enclosed in [ ])
    > source — Source (any, region code, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or IPv6-range), value or list of values enclosed in [ ])
    > source-user — Source user (any, known user, pre-logon, unknown, value or list of values enclosed in [ ])
    > tag — Tag (member value or list of values enclosed in [ ])
    > to — To (any zone, value or list of values enclosed in [ ])
    > type — Decryption type
        > ssl-inbound-inspection — SSL Inbound Inspection value
        - ssh-proxy — SSH Proxy
        - ssl-forward-proxy — SSL Forward Proxy
> default-security-rules— Allow you to modify the default rules for interzone and intrazone traffic that does not match any other rule.
    + action — Whether the rule allows traffic matching the rule or denies it.
    + log-end — Log at session end (required for certain ACC tables)
    + log-setting — Log setting
    + log-start — Log at session start
    > profile-setting — Profile setting for group or profile rules
        + group — Group member value or list of values enclosed in [ ]
        > profiles — Profiles for security rules
            > data-filtering — Data filtering profiles member value or list of values enclosed in [ ]
            > file-blocking — File blocking profiles member value or list of values enclosed in [ ]
            > spyware — Spyware profiles member value or list of values enclosed in [ ]
            > url-filtering — URL filtering profiles member value or list of values enclosed in [ ]
            > virus — Anti-virus profiles member value or list of values enclosed in [ ]
            > vulnerability — Vulnerability profiles member value or list of values enclosed in [ ]
        > tag — Tag (member value or list of values enclosed in [ ])
> dos — Denial of Service (DoS) protection rules
    + description — Description of rule set
    + disabled — Disables the rule
    + log-setting — Specifies the log setting
    + negate-destination — Negates destination
    + negate-source — Negates source
    + schedule — Schedule value
    > action — DoS rule action
        - allow — Allow all packets
        - deny — Deny packets
        - protect — Enforce DoS protection
    > destination — Destination (any, region code, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range
        (x.x.x.x-y.y.y.y or IPv6-range), value or list of values enclosed in [ ])
    > from — Source zone or interface
        + interface — Interface member value or list of values enclosed in [ ]
        + zone — Zone value or list of values enclosed in [ ]
    > protection — DoS protection parameters to enforce
        > aggregate — Parameters for aggregated protection
            + profile — DoS profile to use for aggregated protection
        > classified — Parameters for classified/qualified protection
            + profile — DoS profile to use for classified protection
            > classification-criteria — Parameters to control how DoS protection is applied
                + address — Parameters for IP Address based classification
                    - destination-ip-only — Destination IP address only
                    - source-ip-only — Source IP address only
                    - src-dest-ip-both — Both source and destination IP addresses
    > service — Service (any, application default, predefined HTTP or HTTPS service, value or list of values enclosed in [ ])
    > source — Source (any, region code, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y
        or IPv6-range), value or list of values enclosed in [ ])
    > source-user — Source user (any, known user, pre-logon, unknown, value or list of values enclosed in [ ])
    > tag — Tag (member value or list of values enclosed in [ ])
    > to — Destination zone, interface, or name
        + interface — Interface member value or list of values enclosed in [ ]
        + zone — Zone value or list of values enclosed in [ ]
> nat — Network Address Translation (NAT) rules
    + active-active-device-binding — Device binding configuration in High Availability (HA) Active-Active mode
        0 — Rule is bound to device 0
        1 — Rule is bound to device 1
        both — Rule is bound to both devices
        primary — Rule is bound to Active-Primary device
    + description — Description of rule set
    + disabled — Disables the rule
    +nat-type — Sets Internet Protocol version for NAT - IPv4 or NAT64 (translator between IPv6 and IPv4)
    + service — Service (any, predefined HTTP or HTTPS service, service name, or service group)
    + to-interface — Egress interface from route lookup (any or interface name)
    > destination — Destination (any, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or IPv6-range), value or list of values enclosed in [ ])
    > destination-translation
        + translated-address — IP address and network mask (x.x.x.x/y or IPv6/netmask), or IP address range (x.x.x.x-y.y.y.y or IPv6-range)
        + translated-port — Port number (1-65535)
    > from — From (any zone, value or list of values enclosed in [ ])
    > source — Source (any, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or IPv6-range), value or list of values enclosed in [ ])
    > source-translation
        > dynamic-ip — Dynamic IP-only translation
            > fallback — Fallback Dynamic IP and port translation
                > interface-address — Use interface address as translated address
                    + interface — Interface name
                    > floating-ip — Floating IP address in HA Active-Active configuration
                    > ip — Specify exact IP address if interface has multiple addresses
                > translated-address — IP address and network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or IPv6-range), value or list of values enclosed in [ ]
            > translated-address — IP address and network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or IPv6-range), value or list of values enclosed in [ ]
        > dynamic-ip-and-port — Dynamic IP and port translation
            > interface-address — Use interface address as translated address
                + interface — Interface name
                > floating-ip — Floating IP address in HA Active-Active configuration
                > ip — Specify exact IP address if interface has multiple addresses
            > translated-address — IP address and network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or IPv6-range), value or list of values enclosed in [ ]
        > static-ip — Static IP translation via IP shifting
            + bi-directional — Allow reverse translation from translated address to original address
            + translated-address — IP address and network mask (x.x.x.x/y or IPv6/netmask), or IP address range (x.x.x.x-y.y.y.y or IPv6-range)
    > tag — Tag (member value or list of values enclosed in [ ])
    > to — To (any zone, value or list of values enclosed in [ ])
> pbf — Policy-based Forwarding (PBF) rules
    + active-active-device-binding — Device binding configuration in High Availability (HA) Active-Active mode
        0 — Rule is bound to device 0
        1 — Rule is bound to device 1
        both — Rule is bound to both devices
    + description — Description of rule set
    + disabled — Disables the rule
    + negate-destination — Negates destination
    + negate-source — Negates source
    + schedule — Schedule value
    > action — Policy-based forwarding action
        > forward — Forward packets
            + egress-interface — Interface to route packet to
            > monitor — Parameters for monitoring
                + disable-if-unreachable — Disable this rule if nexthop/monitor ip is unreachable
                + ip-address — Monitor IP address (x.x.x.x or IPv6)
                + profile — Monitoring profile associated with this rule
            > nexthop — Next hop IP address (x.x.x.x or IPv6)
        > forward-to-vsys — Virtual system/Shared gateway to route packets to
        - discard — Discard packets
        - no-pbf — Don't forward by PBF
    > application — Application (any, value or list of values enclosed in [ ])
    > destination — Destination (any, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or
        IPv6-range), value or list of values enclosed in [ ])
    > enforce-symmetric-return — Configure symmetric return
        + enabled — Enable symmetric return
        > nexthop-address-list — List of nexthop routers (IP addresses)
    > from — Source zone or interface
        + interface — Interface member value or list of values enclosed in [ ]
        + zone — Zone value or list of values enclosed in [ ]
    > service — Service (any, application default, predefined HTTP or HTTPS service, value or list of values enclosed in [ ])
    > source — Source (any, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or IPv6-
        range), value or list of values enclosed in [ ])
    > source-user — Source user (any, known user, pre-logon, unknown, value or list of values enclosed in [ ])
    > tag — Tag (member value or list of values enclosed in [ ])
> qos — Quality of Service (QoS) rules
    + description — Description of rule set
    + disabled — Disables the rule
    + negate-destination — Negates destination
    + negate-source — Negates source
    + schedule — Schedule value
    > action — Classification action
        + class — Assigned class (1-8)
    > application — Application (select from list of applications or enter a value)
    > category — URL category (any, specified category, or list of categories enclosed in [ ])
    > destination — Destination (any, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or
        IPv6-range), value or list of values enclosed in [ ])
    > from — From (any zone, value or list of values enclosed in [ ])
    > service — Service (any, application default, predefined HTTP or HTTPS service, value or list of values enclosed in [ ])
    > source — Source (any, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y or IPv6-
        range), value or list of values enclosed in [ ])
    > source-user — Source user (any, known user, pre-logon, unknown, value or list of values enclosed in [ ])
    > tag — Tag (member value or list of values enclosed in [ ])
    > to — To (any zone, multicast, value or list of values enclosed in [ ])
> security — Security rules
    + action — Action (allow or deny)
    + description — Description of rule set
    + disabled — Disables the rule
    + log-end — Log at session end (required for certain ACC tables)
    + log-setting — Log setting
    + log-start — Log at session start
    + rule-type — Specifies whether the rule applies to traffic within a zone, between zones, or both (called universal, which is
        the default). Note that rules migrated from a PAN-OS version prior to 6.1.0 do not show a rule type.
    + negate-destination — Negates destination
    + negate-source — Negates source
    + schedule — Schedule value
    > application — Application (select from list of applications or enter a value)
    > category — URL category (any, specified category, or list of categories enclosed in [ ])
    > destination — Destination (any, region code, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range
        (x.x.x.x-y.y.y.y or IPv6-range), value or list of values enclosed in [ ])
    > from — From (any zone, value or list of values enclosed in [ ])
    > hip-profiles — Host IP profiles (any, no HIP profile, value or list of values enclosed in [ ])
    > option — Security option
```

```
        + disable-server-response-inspection — Disable inspection of server side traffic
    > profile-setting — Profile setting for group or profile rules
        + group — Group member value or list of values enclosed in [ ]
        > profiles — Profiles for security rules
            > data-filtering — Data filtering profiles member value or list of values enclosed in [ ]
            > file-blocking — File blocking profiles member value or list of values enclosed in [ ]
            > spyware — Spyware profiles member value or list of values enclosed in [ ]
            > url-filtering — URL filtering profiles member value or list of values enclosed in [ ]
            > virus — Anti-virus profiles member value or list of values enclosed in [ ]
            > vulnerability — Vulnerability profiles member value or list of values enclosed in [ ]
        > tag — Tag (member value or list of values enclosed in [ ])
    > qos — QoS security
        > marking — Marking rules
            > ip-dscp — IP dscp; specify codepoint in format of 'xxxxxx' where x is {0|1}
                af11    codepoint 001010
                af12    codepoint 001100
                af13    codepoint 001110
                af21    codepoint 010010
                af22    codepoint 010100
                af23    codepoint 010110
                af31    codepoint 011010
                af32    codepoint 011100
                af33    codepoint 011110
                af41    codepoint 100010
                af42    codepoint 100100
                af43    codepoint 100110
                cs0     codepoint 000000
                cs1     codepoint 001000
                cs2     codepoint 010000
                cs3     codepoint 011000
                cs4     codepoint 100000
                cs5     codepoint 101000
                cs6     codepoint 110000
                cs7     codepoint 111000
                ef      codepoint 101110, expedited forwarding
            > ip-precedence — IP precedence; specify codepoint in format of 'xxx'
                cs0     codepoint 000
                cs1     codepoint 001
                cs2     codepoint 010
                cs3     codepoint 011
                cs4     codepoint 100
                cs5     codepoint 101
                cs6     codepoint 110
                cs7     codepoint 111
    > service — Service (any, application default, predefined HTTP or HTTPS service, value or list of values enclosed in [ ])
    > source — Source (any, region code, IP address/network mask (x.x.x.x/y or IPv6/netmask), IP address range (x.x.x.x-y.y.y.y
        or IPv6-range), value or list of values enclosed in [ ])
    > source-user — Source user (any, known user, pre-logon, unknown, value or list of values enclosed in [ ])
    > tag — Tag (member value or list of values enclosed in [ ])
    > to — To (any zone, multicast zone, value or list of values enclosed in [ ])
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set schedule

Specifies schedules for use in security policies. By default, each security policy applies to all dates and times. To limit a security policy to specific dates and times, define a schedule and then apply it to the policy.

Syntax

```
set schedule <name>
   {
   non-recurring <value> |
   recurring
     {
     daily <value> |
     weekly {friday | monday | saturday | sunday | thursday | tuesday | wednesday}
        <value>
     }
   }
```

Options

<name> — Schedule to configure
+ non-recurring — Non-recurring date-time range specification (YYYY/MM/DD@hh:mm-YYYY/MM/DD@hh:mm; e.g. 2006/08/01@10:00-2007/12/31@23:59), or list of values enclosed in [ ]
> recurring — Recurring period
   + daily — Daily time range specification (hh:mm-hh:mm; e.g. 10:00-23:59), or list of values enclosed in [ ]
   > weekly — Week day and time range specification (hh:mm-hh:mm; e.g. 10:00-23:59), or list of values enclosed in [ ]

Required Privilege Level

superuser, vsysadmin, deviceadmin

set service

Configures protocol settings for services. When you define security policies for specific applications, you can specify services to limit the port numbers the applications can use. Services requiring the same security settings can be combined into service groups that you can refer to as a unit.

For information on configuring service groups using the CLI, refer to “set service-group” on page 233.

Syntax

```
set service <name>
   {
   description <value> |
   protocol
     {
     tcp {port <port_number> | source-port <port_number>} |
     udp {port <port_number> | source-port <port_number>}
     }
   tag <value>
   }
```

Options

<name> — Service to configure (up to 63 characters)
+ description — Service description
> protocol — Protocol service
   > tcp — Transmission Control Protocol (TCP)
      + port — Port number or list of values enclosed in [ ] (1-65535)
      + source-port — Source port number or list of values enclosed in [ ] (1-65535)
   > udp — User Datagram Protocol (UDP)
      + port — Port number or list of values enclosed in [ ] (1-65535)
      + source-port — Source port number or list of values enclosed in [ ] (1-65535)
> tag — Tag name

Required Privilege Level

superuser, vsysadmin, deviceadmin

set service-group

Configures sets of services that will be assigned the same security settings, to simplify the creation of security policies. When you define security policies for specific applications, you can specify one or more services or service groups to limit the port numbers the applications can use.

For information on configuring services using the CLI, refer to “set service” on page 232.

Syntax

```
set service-group <name> {service-http | service-https | <value>} {tag <value>}
```

Options

<name> — Service group name to configure (up to 63 characters)
<value> — HTTP, HTTPS, member value or list of values enclosed in [ ]
tag — Tag name

Required Privilege Level

superuser, vsysadmin, deviceadmin

set setting

Configures Network Address Translation (NAT) and SSL decryption settings for interaction with other services on the firewall.

Syntax

```
set setting
    {
    nat |
       {
       reserve-ip {no | yes} |
       reserve-time <value>
       }
    ssl-decrypt
       {
       allow-forward-decrypted-content {no | yes} |
       answer-timeout <value> |
       notify-user {no | yes} |
       url-proxy {no | yes}
       }
    }
```

Options

> nat — Network Address Translation (NAT)
    + reserve-ip — Reserve translated IP for specified time
    + reserve-time — Reserve time value in seconds (1-604800)
> ssl-decrypt — Secure Socket Layer (SSL) decryption
    + allow-forward-decrypted-content — Allow forwarding of decrypted content. For example, this setting will determine whether files from decrypted sessions can be sent to WildFire for analysis.
    + answer-timeout — Set user reply timeout value in seconds (1-86400)
    + notify-user — Set if user notification should be enabled
    + url-proxy — Set proxy for SSL sessions if IP's URL category is blocked

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared admin-role

Specifies the access and responsibilities that are assigned to administrative users.

Syntax

```
set shared admin-role <name>
   {
   description <value> |
   role
     {
     device
        {
        cli {deviceadmin | devicereader | superreader | superuser} |
        webui
           {
           acc {disable | enable} |
           commit {disable | enable} |
           dashboard {disable | enable} |
           device |
              {
              access-domain {disable | enable | read-only} |
              admin-roles {disable | enable | read-only} |
              administrators {disable | enable | read-only} |
              authentication-profile {disable | enable | read-only} |
              authentication-sequence {disable | enable | read-only} |
              block-pages {disable | enable | read-only} |
              config-audit {disable | enable} |
              dynamic-updates {disable | enable | read-only} |
              global-protect-client {disable | enable | read-only} |
              high-availability {disable | enable | read-only} |
              licenses {disable | enable | read-only} |
              master-key {disable | enable | read-only} |
              password-profiles {disable | enable | read-only} |
              scheduled-log-export {disable | enable} |
              setup {disable | enable | read-only} |
              shared-gateways {disable | enable | read-only} |
              software {disable | enable | read-only} |
              support {disable | enable | read-only} |
              user-identification {disable | enable | read-only} |
              virtual-systems {disable | enable | read-only} |
              certificate-management |
                 certificate-profile {disable | enable | read-only} |
                 certificates {disable | enable | read-only} |
                 ocsp-responder {disable | enable | read-only}
                 }
              local-user-database |
                 {
                 user-groups {disable | enable | read-only} |
                 users {disable | enable | read-only} |
                 }
              log-settings |
                 {
                 cc-alarm {disable | enable | read-only} |
                 config {disable | enable | read-only} |
                 hipmatch {disable | enable | read-only} |
                 manage-log {disable | enable | read-only} |
                 system {disable | enable | read-only}
                 }
              server-profile
                 {
                 email {disable | enable | read-only} |
                 kerberos {disable | enable | read-only} |
                 ldap {disable | enable | read-only} |
                 netflow {disable | enable | read-only} |
                 radius {disable | enable | read-only} |
                 snmp-trap {disable | enable | read-only} |
                 syslog {disable | enable | read-only}
                 }
              }
           global system-alarms {disable | enable} |
           monitor |
              {
              app-scope {disable | enable} |
              application-reports {disable | enable} |
              botnet {disable | enable | read-only} |
              packet-capture {disable | enable | read-only} |
              session-browser {disable | enable} |
              threat-reports {disable | enable} |
              traffic-reports {disable | enable} |
              url-filtering-reports {disable | enable} |
              view-custom-reports {disable | enable} |
              custom-reports |
                 {
                 application-statistics {disable | enable} |
                 data-filtering-log {disable | enable} |
                 hipmatch {disable | enable} |
                 threat-log {disable | enable} |
                 threat-summary {disable | enable} |
                 traffic-log {disable | enable} |
                 traffic-summary {disable | enable} |
                 url-log {disable | enable}
                 }
              logs |
                 {
                 alarm {disable | enable} |
                 configuration {disable | enable} |
                 data-filtering {disable | enable} |
                 hipmatch {disable | enable} |
                 system {disable | enable} |
                 threat {disable | enable} |
                 traffic {disable | enable} |
                 url {disable | enable} |
                 wildfire {disable | enable}
                 }
              pdf-reports
                 {
                 email-scheduler {disable | enable | read-only} |
                 manage-pdf-summary {disable | enable | read-only} |
                 pdf-summary-reports {disable | enable} |
                 report-groups {disable | enable | read-only} |
                 user-activity-report {disable | enable | read-only} |
                 }
              }
           network |
              dhcp {disable | enable | read-only} |
              dns-proxy {disable | enable | read-only} |
              interfaces {disable | enable | read-only} |
              ipsec-tunnels {disable | enable | read-only} |
              qos {disable | enable | read-only} |
              virtual-routers {disable | enable | read-only} |
              virtual-wires {disable | enable | read-only} |
              vlans {disable | enable | read-only} |
              zones {disable | enable | read-only} |
              global-protect |
                 {
                 gateways {disable | enable | read-only} |
                 portals {disable | enable | read-only}
                 }
              network-profiles
                 {
                 ike-crypto {disable | enable | read-only} |
                 ike-gateways {disable | enable | read-only} |
                 interface-mgmt {disable | enable | read-only} |
                 ipsec-crypto {disable | enable | read-only} |
                 qos-profile {disable | enable | read-only} |
                 tunnel-monitor {disable | enable | read-only} |
                 zone-protection {disable | enable | read-only}
                 }
              }
           objects |
              {
              address-groups {disable | enable | read-only} |
              addresses {disable | enable | read-only} |
              application-filters {disable | enable | read-only} |
              application-groups {disable | enable | read-only} |
              applications {disable | enable | read-only} |
              custom-url-category {disable | enable | read-only} |
              decryption-profile {disable | enable | read-only} |
              dynamic-block-lists {disable | enable | read-only} |
              log-forwarding {disable | enable | read-only} |
              regions {disable | enable | read-only} |
              schedules {disable | enable | read-only} |
              security-profile-groups {disable | enable | read-only} |
              service-groups {disable | enable | read-only} |
              services {disable | enable | read-only} |
              custom-signatures |
                 {
                 data-patterns {disable | enable | read-only} |
                 spyware {disable | enable | read-only} |
                 vulnerability {disable | enable | read-only} |
                 }
              global-protect |
                 {
                 hip-objects {disable | enable | read-only} |
                 hip-profiles {disable | enable | read-only} |
                 }
              security-profiles
                 {
                 anti-spyware {disable | enable | read-only} |
                 antivirus {disable | enable | read-only} |
                 data-filtering {disable | enable | read-only} |
                 dos-protection {disable | enable | read-only} |
                 file-blocking {disable | enable | read-only} |
                 url-filtering {disable | enable | read-only} |
                 vulnerability-protection {disable | enable | read-only} |
                 }
              }
           policies |
              {
              application-override-rulebase {disable | enable | read-only}|
              captive-portal-rulebase {disable | enable | read-only} |
              dos-rulebase {disable | enable | read-only} |
              nat-rulebase {disable | enable | read-only} |
              pbf-rulebase {disable | enable | read-only} |
              qos-rulebase {disable | enable | read-only} |
              security-rulebase {disable | enable | read-only} |
              ssl-decryption-rulebase {disable | enable | read-only}
              }
           privacy
              {
              show-full-ip-addresses {disable | enable} |
              show-user-names-in-logs-and-reports {disable | enable} |
              view-pcap-files {disable | enable}
              }
           }
        xmlapi
           {
           commit {disable | enable} |
           config {disable | enable} |
           export {disable | enable} |
           import {disable | enable} |
           log {disable | enable} |
           op {disable | enable} |
           report {disable | enable} |
           user-id {disable | enable}
           }
        }
     vsys
        {
        cli {vsysadmin | vsysreader} |
        webui
           {
           acc {disable | enable} |
           commit {disable | enable} |
           dashboard {disable | enable} |
           device |
              {
              access-domain {disable | enable | read-only} |
              administrators {disable | enable | read-only} |
              authentication-profile {disable | enable | read-only} |
              authentication-sequence {disable | enable | read-only} |
              block-pages {disable | enable | read-only} |
              setup {disable | enable | read-only} |
              user-identification {disable | enable | read-only} |
              local-user-database |
                 {
                 user-groups {disable | enable | read-only} |
                 users {disable | enable | read-only} |
                 }
              log-settings |
                 {
                 config {disable | enable | read-only} |
                 hipmatch {disable | enable | read-only} |
                 system {disable | enable | read-only}
                 }
              server-profile
                 {
                 email {disable | enable | read-only} |
                 kerberos {disable | enable | read-only} |
                 ldap {disable | enable | read-only} |
                 netflow {disable | enable | read-only} |
                 radius {disable | enable | read-only} |
                 snmp-trap {disable | enable | read-only} |
                 syslog {disable | enable | read-only}
                 }
              }
           global system-alarms {disable | enable} |
           monitor |
              {
              app-scope {disable | enable} |
              session-browser {disable | enable} |
              view-custom-reports {disable | enable} |
              custom-reports |
                 {
                 application-statistics {disable | enable} |
                 data-filtering-log {disable | enable} |
                 hipmatch {disable | enable} |
                 threat-log {disable | enable} |
                 threat-summary {disable | enable} |
                 traffic-log {disable | enable} |
                 traffic-summary {disable | enable} |
                 url-log {disable | enable}
                 }
              logs |
                 {
                 alarm {disable | enable} |
                 data-filtering {disable | enable} |
                 hipmatch {disable | enable} |
                 threat {disable | enable} |
                 traffic {disable | enable} |
                 url {disable | enable} |
                 wildfire {disable | enable}
                 }
              pdf-reports
                 {
                 email-scheduler {disable | enable | read-only} |
                 manage-pdf-summary {disable | enable | read-only} |
                 pdf-summary-reports {disable | enable} |
                 report-groups {disable | enable | read-only} |
                 user-activity-report {disable | enable | read-only}
                 }
              }
           network |
              zones {disable | enable | read-only} |
              global-protect
                 {
                 gateways {disable | enable | read-only} |
                 portals {disable | enable | read-only}
                 }
              }
           objects |
              {
              address-groups {disable | enable | read-only} |
              addresses {disable | enable | read-only} |
              application-filters {disable | enable | read-only} |
              application-groups {disable | enable | read-only} |
              applications {disable | enable | read-only} |
              custom-url-category {disable | enable | read-only} |
              decryption-profile {disable | enable | read-only} |
              dynamic-block-lists {disable | enable | read-only} |
              log-forwarding {disable | enable | read-only} |
              regions {disable | enable | read-only} |
              schedules {disable | enable | read-only} |
              security-profile-groups {disable | enable | read-only} |
              service-groups {disable | enable | read-only} |
              services {disable | enable | read-only} |
              custom-signatures |
                 {
                 data-patterns {disable | enable | read-only} |
                 spyware {disable | enable | read-only} |
                 vulnerability {disable | enable | read-only} |
                 }
              global-protect |
                 {
                 hip-objects {disable | enable | read-only} |
                 hip-profiles {disable | enable | read-only} |
                 }
              security-profiles
                 {
                 anti-spyware {disable | enable | read-only} |
                 antivirus {disable | enable | read-only} |
                 data-filtering {disable | enable | read-only} |
                 dos-protection {disable | enable | read-only} |
                 file-blocking {disable | enable | read-only} |
                 url-filtering {disable | enable | read-only} |
                 vulnerability-protection {disable | enable | read-only} |
                 }
              }
          policies |
              {
              application-override-rulebase {disable | enable | read-only}|
              captive-portal-rulebase {disable | enable | read-only} |
              dos-rulebase {disable | enable | read-only} |
              nat-rulebase {disable | enable | read-only} |
              pbf-rulebase {disable | enable | read-only} |
              qos-rulebase {disable | enable | read-only} |
              security-rulebase {disable | enable | read-only} |
              ssl-decryption-rulebase {disable | enable | read-only}
              }
          privacy
              {
              show-full-ip-addresses {disable | enable} |
              show-user-names-in-logs-and-reports {disable | enable} |
              view-pcap-files {disable | enable}
              }
          }
       xmlapi
          {
          commit {disable | enable} |
          config {disable | enable} |
          export {disable | enable} |
          import {disable | enable} |
          log {disable | enable} |
          op {disable | enable} |
          report {disable | enable} |
          user-id {disable | enable}
          }
       }
    }
  }
```

Options

<name> — Shared administrative role name
+ description — Description text
> role — Sets access and responsibilities for the role
    > device — Device settings
        + cli — Command Line Interface access
            - deviceadmin — Device Administrator
            - devicereader — Device Reader
            - superreader — Super Reader
            - superuser — Super User
        > webui — Sets enable, disable, or read-only access to the web user interface
            + acc — Access
            + commit — Commit

```
+ dashboard — Dashboard
> device — Device settings
    + access-domain — Access domain
    + admin-roles — Admin roles
    + administrators — Administrators
    + authentication-profile — Authentication profile
    + authentication-sequence — Authentication sequence
    + block-pages — Block pages
    + config-audit — Configuration audit
    + dynamic-updates — Dynamic updates
    + global-protect-client — GlobalProtect Client
    + high-availability — High Availability
    + licenses — Licenses
    + master-key — Disable, enable, or read-only device master key
    + password-profiles — Password profiles
    + scheduled-log-export — Scheduled log export
    + setup — Setup
    + shared-gateways — Shared gateways
    + software — Software
    + support — Support
    + user-identification — User identification
    + virtual-systems — Virtual systems
    > certificate-management — Certificate management
        + certificate-profile — Certificate profile
        + certificates — Certificates
        + ocsp-responder — OCSP responder
    > local-user-database — Local user database
        + user-groups — User groups
        + users — Users
    > log-settings — Log settings
        + cc-alarm — Disable, enable, or read-only the CC alarm log
        + config — Disable, enable, or read-only the configuration log
        + hipmatch — Disable, enable, or read-only the hipmatch log
        + manage-log — Disable, enable, or read-only management log
        + system — Disable, enable, or read-only the system log
    > server-profile — Server profile
        + email — Email profile
        + kerberos — Kerberos profile
        + ldap — LDAP profile
        + netflow — NetFlow profile
        + radius — RADIUS profile
        + snmp-trap — SNMP trap profile
        + syslog — syslog profile
> global — Global settings
    + system-alarms — Global system alarm settings
> monitor — Monitor settings
    + app-scope — Application scope
    + application-reports — Application reports
    + botnet — Botnet
    + packet-capture — Packet capture
    + session-browser — Session browser
    + threat-reports — Threat reports
    + traffic-reports — Traffic reports
    + url-filtering-reports — URL filtering reports
    + view-custom-reports — View custom reports
    > custom-reports — Custom report settings
        + application-statistics — Application statistics
        + data-filtering-log — Data filtering log
        + hipmatch — hipmatch report
        + threat-log — Threat log
        + threat-summary — Threat summary
        + traffic-log — Traffic log
        + traffic-summary — Traffic summary
        + url-log — URL log
    > logs — Logs settings
        + alarm — Disable or enable monitor alarm logs
        + configuration — Configuration logs
        + data-filtering — Data filtering logs
        + hipmatch — HIPmatch logs
        + system — System logs
        + threat — Threat logs
        + traffic — Traffic logs
        + url — URL logs
        + wildfire — Wildfire logs
    > pdf-reports — PDF reports
        + email-scheduler — Email scheduler
        + manage-pdf-summary — manage PDF summary
        + pdf-summary-reports — PDF summary reports
        + report-groups — Report groups
        + user-activity-report — User activity report
> network — Network settings
    + dhcp — DHCP
    + dns-proxy — DNS proxy
    + interfaces — Interfaces
    + ipsec-tunnels — IPSec tunnels
    + qos — QOS
    + virtual-routers — Virtual routers
    + virtual-wires — Virtual wires
    + vlans — VLANs
    + zones — Zones
    > global-protect — GlobalProtect settings
        + gateways — Gateways
        + portals — Portals
    > network-profiles — Network profile settings
        + ike-crypto — IKE crypto
        + ike-gateways — IKE gateways
        + interface-mgmt — Interface management
        + ipsec-crypto — IPSec crypto
        + qos-profile — QOS profile
        + tunnel-monitor — Tunnel monitor
        + zone-protection — Zone protection
> objects — Objects settings
    + address-groups — Address groups
    + addresses — Addresses
    + application-filters — Application filters
    + application-groups — Application groups
    + applications — Applications
    + custom-url-category — Custom URL category
```

```
            + decryption-profile — Decryption profile
            + dynamic-block-lists — Dynamic block lists
            + log-forwarding — Log forwarding
            + regions — Regions
            + schedules — Schedules
            + security-profile-groups — Security profile groups
            + service-groups — Service groups
            + services — Services
            > custom-signatures — Custom signatures
                + data-patterns — Data patterns
                + spyware — Spyware
                + vulnerability — Vulnerability
            > global-protect — GlobalProtect settings
                + hip-objects — HIP objects
                + hip-profiles — HIP profiles
            > security-profiles — Security profile settings
                + anti-spyware — Anti-spyware
                + antivirus — Antivirus
                + data-filtering — Data filtering
                + dos-protection — DOS protection
                + file-blocking — File blocking
                + url-filtering — URL filtering
                + vulnerability-protection — Vulnerability protection
        > policies — Policy settings
            + application-override-rulebase — Application override rulebase
            + captive-portal-rulebase — Captive portal rulebase
            + dos-rulebase — DOS rulebase
            + nat-rulebase — NAT rulebase
            + pbf-rulebase — PBF rulebase
            + qos-rulebase — QOS rulebase
            + security-rulebase — Security rulebase
            + ssl-decryption-rulebase — SSL decryption rulebase
        > privacy — Privacy settings
            + show-full-ip-addresses — Show full IP addresses
            + show-user-names-in-logs-and-reports — Show user names in logs and reports
            + view-pcap-files — View packet capture files
    > xmlapi — Sets enable or disable access to the XML API user interface
        + commit — Commit
        + config — Configuration
        + export — Export
        + import — Import
        + log — Log
        + op — Operation
        + report — Report
        + user-id — User ID
> vsys — Virtual system settings
    + cli — Command Line Interface access
        - vsysadmin — Virtual System Administrator
        - vsysreader — Virtual System Reader
    > webui — Sets enable, disable, or read-only access to the web user interface
        + acc — acc
        + commit — commit
        + dashboard — dashboard
        > device — Device settings
            + access-domain — Access domain
            + administrators — Administrators
            + authentication-profile — Authentication profile
            + authentication-sequence — Authentication sequence
            + block-pages — Block pages
            + setup — Setup
            + user-identification — User identification
            > local-user-database — Local user database
                + user-groups — User groups
                + users — Users
            > log-settings — Disable, enable, or read-only log settings
                + config — Configuration log
                + hipmatch — Host IP match log
                + system — System log
            > server-profile — Server profile settings
                + email — Email
                + kerberos — Kerberos
                + ldap — LDAP
                + netflow — NetFlow
                + radius — RADIUS
                + snmp-trap — SNMP trap
                + syslog — syslog
        > global — Global settings
            + system-alarms — Global system alarm settings
        > monitor — Monitor settings
            + app-scope — Application scope
            + session-browser — Session browser
            + view-custom-reports — View custom reports
            > custom-reports — Custom report settings
                + application-statistics — Application statistics
                + data-filtering-log — Data filtering log
                + hipmatch — Host IP match
                + threat-log — Threat log
                + threat-summary — Threat summary
                + traffic-log — Traffic log
                + traffic-summary — Traffic summary
                + url-log — URL log
            > logs — Log settings
                + alarm — Disable or enable monitor alarm logs
                + configuration — configuration
                + data-filtering — data-filtering
                + hipmatch — hipmatch
                + system — system
                + threat — threat
                + traffic — traffic
                + url — url
                + wildfire
            > pdf-reports — PDF report settings
                + email-scheduler — Email scheduler
                + manage-pdf-summary — Manage PDF summary
                + pdf-summary-reports — PDF summary reports
                + report-groups — Report groups
                + user-activity-report — User activity report
        > network — Network settings
```

```
        + zones — Zones
        > global-protect — GlobalProtect settings
            + gateways — Gateways
            + portals — Portals
    > objects — Objects settings
        + address-groups — Address groups
        + addresses — Addresses
        + application-filters — Application filters
        + application-groups — Application groups
        + applications — Applications
        + custom-url-category — Custom URL category
        + decryption-profile — Decryption profile
        + dynamic-block-lists — Dynamic block lists
        + log-forwarding — Log forwarding
        + regions — Regions
        + schedules — Schedules
        + security-profile-groups — Security profile groups
        + service-groups — Service groups
        + services — Services
        > custom-signatures — Custom signatures
            + data-patterns — Data patterns
            + spyware — Spyware
            + vulnerability — Vulnerability
        > global-protect — GlobalProtect settings
            + hip-objects — Host IP objects
            + hip-profiles — Host IP profiles
        > security-profiles — Security profile settings
            + anti-spyware — Anti-spyware
            + antivirus — Antivirus
            + data-filtering — Data filtering
            + dos-protection — DOS protection
            + file-blocking — file blocking
            + url-filtering — URL filtering
            + vulnerability-protection — Vulnerability protection
    > policies — Policy settings
        + application-override-rulebase — Application override rulebase
        + captive-portal-rulebase — Captive portal rulebase
        + dos-rulebase — DOS rulebase
        + nat-rulebase — NAT rulebase
        + pbf-rulebase — PBF rulebase
        + qos-rulebase — QOS rulebase
        + security-rulebase — Security rulebase
        + ssl-decryption-rulebase — SSL decryption rulebase
    > privacy — Privacy settings
        + show-full-ip-addresses — Show full IP addresses
        + show-user-names-in-logs-and-reports — Show user names in logs and reports
        + view-pcap-files — View packet capture files
> xmlapi — Sets enable or disable access to the XML API user interface
    + commit — Commit
    + config — Configuration
    + export — Export
    + import — Import
    + log — Log
    + op — Operation
```

+ report — Report
+ user-id — User ID

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared alg-override

Enables or disables SIP application level gateway (ALG).

Syntax

```
set shared alg-override application <name>
   {
   alg-disabled {no | yes}
   }
```

Options

> application — Specify application name
   + alg-disabled — Specify whether SIP ALG is disabled (yes) or disabled (no)

Sample Output

The following command disables SIP ALG.

```
username@hostname# set shared alg-override application sip alg-disabled yes
no
[edit]
username@hostname#
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared authentication-profile

Specifies local database, RADIUS, or LDAP settings for assignment to administrator accounts, SSL VPN access, and captive portal. When an administrator attempts to log in to the firewall directly or through an SSL VPN or captive portal, the firewall checks the authentication profile that is assigned to the account and authenticates the user based on the authentication settings.

Syntax

```
set shared authentication-profile <group_name> |
   {
   allow-list {all | <value>} |
   lockout |
     {
     failed-attempts <value> |
     lockout-time <minutes>
     }
   method
     {
     kerberos {server-profile <object_name>} |
     ldap |
        {
        login-attribute <value> |
        passwd-exp-days <value> |
        server-profile <name>
        }
     radius {server-profile <object_name>}
     local-database |
     none
     }
   }
```

Options

<group_name> — Specify group to share the profile
+ allow-list — List of allowed users and groups enclosed in [ ]; option to specify all
> lockout — Network user login lockout settings
    + failed-attempts — Number of failed login attempts to trigger lock-out
    + lockout-time — Number of minutes to lock-out
> method — method
    > kerberos — Kerberos authentication
        + server-profile — Kerberos server profile object
    > ldap — Lightweight Directory Access Protocol (LDAP) authentication
        + login-attribute — Login attribute in LDAP server to authenticate against; default = uid
        + passwd-exp-days — Days until the password expires
        + server-profile — LDAP server profile object
    > radius — Remote Authentication Dial In User Service (RADIUS) authentication
        + server-profile — RADIUS server profile object
    - local-database — Local database authentication
    - none — No authentication

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared authentication-sequence

Specifies a set of authentication profiles that are applied in order when a user attempts to log in to the firewall. Useful in environments where user accounts (including guest and other accounts) reside in multiple directories. The firewall tries each profile in sequence until the user is identified. Access to the firewall is denied only if authentication fails for any of the profiles in the authentication sequence.

For information on configuring authentication profiles using the CLI, refer to "set shared authentication-profile" on page 249.

Syntax

```
set shared authentication-sequence <name>
   {
   authentication-profiles <value> |
   lockout
     {
     failed-attempts <value> |
     lockout-time <value>
     }
   }
```

Options

<name> — Authentication sequence name
+ authentication-profiles — Authentication profiles to apply in the sequence (name or list of names enclosed in [ ])
> lockout — Network user login lockout settings
    + failed-attempts— Number of failed login attempts to trigger lock-out (0-10)
    + lockout-time— Number of minutes to lock-out (0-60)

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared botnet

Specifies types of suspicious traffic (traffic that may indicate botnet activity). The firewall provides support to help identify possible botnet infected clients by analyzing potentially suspicious traffic, such as unknown TCP and UDP traffic, traffic destined for unknown URL or malware categories, and increased Domain Name Service (DNS) traffic.

Syntax

```
set shared botnet
   {
   configuration |
     {
     http |
        {
        dynamic-dns {enabled {no | yes} | threshold <value>} |
        executables-from-unknown-sites {enabled {no | yes} | threshold <value>} |
        ip-domains {enabled {no | yes} | threshold <value>} |
        malware-sites {enabled {no | yes} | threshold <value>} |
        recent-domains {enabled {no | yes} | threshold <value>}
        }
     other-applications irc {no | yes} |
     unknown-application {unknown-tcp | unknown-udp}
        {
        destinations-per-hour <value> |
        sessions-per-hour <value> |
        session-length {maximum-bytes <value> | minimum-bytes <value>}
        }
     }
   report
     {
     query <value> |
     scheduled {no | yes} |
     topn <value>
     }
   }
```

Options

> configuration — Botnet configuration
   > http — HTTP configuration
      > dynamic-dns — Dynamic DNS
         + enabled — Enabled (no or yes)
         + threshold — Repeat dynamic DNS sites visit threshold (2-1000)
      > executables-from-unknown-sites   executables-from-unknown-sites
         + enabled — Enabled (no or yes)
         + threshold — Repeat executables download from unknown sites visit threshold (2-1000)
      > ip-domains — IP domains
         + enabled — Enabled (no or yes)
         + threshold — Repeat IP domains visit threshold (2-1000)
      > malware-sites — Malware sites
         + enabled — Enabled (no or yes)
         + threshold — Repeat malware sites visit threshold (2-1000)

```
      > recent-domains — Recent domains
         + enabled — Enabled (no or yes)
         + threshold — Repeat recent domains visit threshold (2-1000)
   > other-applications — Other applications
      + irc — Internet Relay Chat (IRC)
   > unknown-application — Unknown application (TCP or UDP)
      + destinations-per-hour — Destinations per hour (1-3600)
      + sessions-per-hour — Sessions per hour (1-3600)
      > session-length — Session length
         + maximum-bytes — Maximum bytes of the session length (1-3600)
         + minimum-bytes — Minimum bytes of the session length (1-3600)
> report — Botnet report
   + query — Query value
   + scheduled — Scheduled (no or yes)
   + topn — TopN value (1-500)
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared certificate

Specifies settings for security certificates.

Syntax

```
set shared certificate <name> |
   {
   common-name <value> |
   expiry-epoch <value> |
   issuer <value> |
   issuer-hash <value> |
   not-valid-after <value> |
   not-valid-before <value> |
   private-key <value> |
   revoke-date-epoch <value> |
   status {revoked | valid} |
   subject <value> |
   subject-hash <value> |
   csr <value> |
   public-key <value>
   }
```

Options

<name> — Shared certificate name
+ common-name — Common name value
+ expiry-epoch — Expiry epoch value
+ issuer — Issuer value
+ issuer-hash — Issuer-hash value
+ not-valid-after — Not-valid-after value
+ not-valid-before — Not-valid-before value
+ private-key — Private key value
+ revoke-date-epoch — Revoke date epoch value
+ status — Status (revoked or valid)
+ subject — Subject value
+ subject-hash — Subject-hash value
> csr — Certificate Signing Request (CSR) value
> public-key — Public key value

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared certificate-profile

Specifies settings for client security certificates. You can create client certificate profiles and then attach a profile to an administrator login on the Setup page or to a Secure Socket Layer (SSL) virtual private network (VPN) login for authentication purposes.

Syntax

```
set shared certificate-profile <name> |
   {
   block-timeout-cert {no | yes} |
   block-unknown-cert {no | yes} |
   cert-status-timeout <value> |
   crl-receive-timeout <value> |
   domain <name> |
   ocsp-receive-timeout <value> |
   use-crl {no | yes} |
   use-ocsp {no | yes} |
   CA <name> |
      {
      default-ocsp-url <value> |
      ocsp-verify-ca <value>
      }
   username-field
      {
      subject common-name |
      subject-alt {email | principal-name}
      }
   }
```

Options

<name> — Profile name
+ block-timeout-cert — Whether to block a session if certificate status can't be retrieved within timeout
+ block-unknown-cert — Whether to block a session if certificate status is unknown
+ cert-status-timeout — Set certificate status query timeout value in seconds (0-60)
+ crl-receive-timeout — Set CRL receive timeout value in seconds (0-60)
+ domain — Domain name (alphanumeric string [0-9a-zA-Z._-])
+ ocsp-receive-timeout — Set OCSP receive timeout value in seconds (0-60)
+ use-crl — Use Certificate Revocation List (CRL)
+ use-ocsp — Use Online Certificate Status Protocol (OCSP)
> CA — Certificate Authority (CA) name
    + default-ocsp-url — Default URL for OCSP verification
    + ocsp-verify-ca — CA file for OCSP response verify
> username-field — User name field population
    > subject — Get user name from subject
    > subject-alt — Get user name from subject alternative name (email or principal name)

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared email-scheduler

Specifies shared settings for email delivery of PDF summary reports.

Syntax

```
set shared email-scheduler <name>
    {
    email-profile <value> |
    recipient-emails <value> |
    report-group <value> |
    recurring
      {
      weekly {friday | monday | saturday | sunday | thursday | tuesday | wednesday} |
      daily |
      disabled
      }
    }
```

Options

<name> — Specifies the name for the email scheduler
+ email-profile — Email profile value
+ recipient-emails — Recipient emails value
+ report-group — Report group value
> recurring — Recurring frequency
    > weekly — Once a week; specify the day
    - daily — Every day
    - disabled — No scheduling

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared local-user-database

Configures a local database on the firewall to store authentication information for administrator access, captive portal, and Secure Socket Layer (SSL) virtual private network (VPN) remote users.

Syntax

```
set shared local-user-database
   {
   user <name> |
     {
     disabled {no | yes} |
     phash <value>
     }
   user-group <name> {user <value>}
   }
```

Options

> user — User name
    + disabled — Disabled (no or yes)
    + phash — phash value
> user-group — User group name
    > user — User name or list of names enclosed in [ ]

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared log-settings

Configures log settings on the firewall.

Syntax

```
set shared log-settings
   {
   config |
     {
     any
        {
        send-to-panorama {no | yes} |
        send-email using-email-setting <value> |
        send-snmptrap using-snmptrap-setting <value> |
        send-syslog using-syslog-setting <value>
        }
     }
   email <name> |
     {
     format |
        {
        config <value> |
        hip-match <value> |
        system <value> |
        threat <value> |
        traffic <value> |
        escaping {escape-character <value> | escaped-characters <value>}
        }
     server <name>
        {
        and-also-to <value> |
        display-name <name> |
        from <value> |
        gateway <value> |
        to <value>
        }
     }
   hipmatch |
     {
     any
        {
        send-to-panorama {no | yes} |
        send-email using-email-setting <value> |
        send-snmptrap using-snmptrap-setting <value> |
        send-syslog using-syslog-setting <value>
        }
     }
   profiles <name> |
     {
     alarm {critical | high | informational | low | medium} |
        {
        send-to-panorama {no | yes} |
        send-email using-email-setting <value> |
        send-snmptrap using-snmptrap-setting <value> |
        send-syslog using-syslog-setting <value>
        }
     traffic
        {
        any
           {
           send-to-panorama {no | yes} |
           send-email using-email-setting <value> |
           send-snmptrap using-snmptrap-setting <value> |
           send-syslog using-syslog-setting <value>
           }
     wiidfire {benign | malicious}
        {
        send-to-panorama {no | yes} |
        send-email using-email-setting <value> |
        send-snmptrap using-snmptrap-setting <value> |
        send-syslog using-syslog-setting <value>
        }
     }
  snmptrap <name> |
     {
     version
        {
        v2c server <name> |
           {
           community <value> |
           manager <value> |
           }
        v3 server <name>
           {
           authpwd <value> |
           engineid <value> |
           manager <value> |
           privpwd <value> |
           user <value>
           }
        }
     }
  syslog <name>
     {
     format |
        {
        config <value> |
        hip-match <value> |
        system <value> |
        threat <value> |
        traffic <value> |
        escaping {escape-character <value> | escaped-characters <value>}
        }
     server <name>
        {
```

```
        facility {LOG_LOCAL0 | LOG_LOCAL1 | LOG_LOCAL2 | LOG_LOCAL3 | LOG_LOCAL4 |
           LOG_LOCAL5 | LOG_LOCAL6 | LOG_LOCAL7 | LOG_USER} |
        port <value> |
        server <value>
        }
     }
  system {critical | high | informational | low | medium}
     {
     send-email using-email-setting <value> |
     send-snmptrap using-snmptrap-setting <value> |
     send-syslog using-syslog-setting <value>
     }
  threat {critical | high | informational | low | medium}
     {
     send-email using-email-setting <value> |
     send-snmptrap using-snmptrap-setting <value> |
     send-syslog using-syslog-setting <value>
  }
  traffic {any}
     {
     send-email using-email-setting <value> |
     send-snmptrap using-snmptrap-setting <value> |
     send-syslog using-syslog-setting <value>
  }
  wildfire {benign | malicious}
     {
     send-email using-email-setting <value> |
     send-snmptrap using-snmptrap-setting <value> |
     send-syslog using-syslog-setting <value>
  }
```

Options

> config — Configuration log settings (any)
    + send-to-panorama — Send to Panorama (no or yes)
    > send-email — Send email using email setting value
    > send-snmptrap — Send SNMP trap using SNMP trap setting value
    > send-syslog — Send syslog using syslog setting value
> email — Email log settings name
    > format — Custom formats for forwarded logs
        + config — Config value
        + hip-match — HIP match value
        + system — System value
        + threat — Threat value
        + traffic — Traffic value
        > escaping — Escaping values
            + escape-character — Escape character
            + escaped-characters — List of characters to be escaped
    > server — Server address
        + and-also-to — Email address (e.g. admin@mycompany.com)
        + display-name — Display name of server
        + from — Email address (e.g. admin@mycompany.com)
        + gateway — IP address or FQDN of SMTP gateway to use
        + to — Email address (e.g. admin@mycompany.com)

```
> hipmatch — HIP match log settings
    + send-to-panorama — Send to Panorama (no or yes)
    > send-email — Send email using email setting value
    > send-snmptrap — Send SNMP trap using SNMP trap setting value
    > send-syslog — Send syslog using syslog setting value
> profiles — Profile log settings
    > alarm — Alarm settings (critical, high, informational, low, or medium)
        + send-to-panorama — Send to Panorama (no or yes)
        > send-email — Send email using email setting value
        > send-snmptrap — Send SNMP trap using SNMP trap setting value
        > send-syslog — Send syslog using syslog setting value
    > traffic — Traffic settings any
        + send-to-panorama — Send to Panorama (no or yes)
        > send-email — Send email using email setting value
        > send-snmptrap — Send SNMP trap using SNMP trap setting value
        > send-syslog — Send syslog using syslog setting value
    > wildfire — Type of wildfire events (benign or malicious)
        + send-to-panorama — Send to Panorama (no or yes)
        > send-email — Send email using email setting value
        > send-snmptrap — Send SNMP trap using SNMP trap setting value
        > send-syslog — Send syslog using syslog setting value
> snmptrap — SNMP trap log settings
    > version v2c server — Server address
        + community — Community value
        + manager — IP address or FQDN of SNMP manager to use
    > version v3 server — Server address
        + authpwd — Authentication Protocol Password
        + engineid — A hex number in ASCII string
        + manager — IP address or FQDN of SNMP manager to use
        + privpwd — Privacy Protocol Password
        + user — User value
> syslog — syslog settings
    > format — Custom formats for forwarded logs (escaping)
        + config — Config value
        + hip-match — HIP match value
        + system — System value
        + threat — Threat value
        + traffic — Traffic value
        > escaping — Escaping values
            + escape-character — Escape character
            + escaped-characters — List of characters to be escaped
    > server — Server address
        + facility — Facility (LOG_LOCAL0, LOG_LOCAL1, LOG_LOCAL2, LOG_LOCAL3, LOG_LOCAL4,
            LOG_LOCAL5, LOG_LOCAL6, LOG_LOCAL7, LOG_USER)
        + port — Port (1-65535)
        + server — IP address or FQDN of SYSLOG server to use
> system — System log settings (critical, high, informational, low, or medium)
    + send-to-panorama — Send to Panorama (no or yes)
    > send-email — Send email using email setting value
    > send-snmptrap — Send SNMP trap using SNMP trap setting value
    > send-syslog — Send syslog using syslog setting value
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared override

Configures overrides to risk and timeout attributes of App-IDs that are on the PAN-OS.

Syntax

```
set shared override
   {
   application <name>
     {
     risk <value> |
     tcp-half-closed-timeout <value> |
     tcp-time-wait-timeout <value> |
     tcp-timeout |
     timeout <value> |
     udp-timeout <value>
     }
   }
```

Options

> application — Select from the list or enter a name

+ risk — Risk (1-5)
+ tcp-half-closed-timeout — Timeout of the TCP session after the first FIN is seen by the firewall. Value is in seconds (0-604800). The default value is the value set at the global level.
+ tcp-time-wait-timeout — Timeout of the TCP session after the second FIN or a RST is seen by the firewall. Value is in seconds (0-600). The default value is the value set at the global level.
+ tcp-timeout — Timeout in seconds (0-604800) before an idle TCP application flow is terminated.
+ timeout — Timeout in seconds (0-604800) before an idle application flow is terminated. A setting of 0 indicates that the default timeout of the application will be used. This timer is for protocols other than TCP and UDP.
+ udp-timeout — Timeout in seconds (0-604800) before an idle UDP application flow is terminated. A setting of 0 indicates that the default timeout of the application will be used.

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared pdf-summary-report

Specifies shared format settings for PDF summary reports.

Syntax

```
set shared pdf-summary-report <name>
   {
   custom-widget <name> |
     {
     chart-type {bar | line | pie | table} |
     column <value> |
     row <value>
     }
   footer {note <value>} |
   header {caption <value>}|
   predefined-widget <name> |
     {
     chart-type {bar | line | pie | table} |
     column <value> |
     row <value>
     }
   }
```

Options

<name> — PDF report to configure
> custom-widget — Report widget layout information
   + chart-type — Chart type (bar, line, pie, or table)
   + column — Column number (1-3)
   + row — Row number (1-6)
> footer — Footer information for PDF summary layout
   + note — Static string to be printed as a note
> header — Header information for PDF summary layout
   + caption — Caption for the layout
> predefined-widget — Predefined report widget layout information
   + chart-type — Chart type (bar, line, pie, or table)
   + column — Column number (1-3)
   + row — Row number (1-6)

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared post-rulebase

(Panorama only) Configures an additional layer of rules that will be applied to all device groups managed by the Panorama instance. The rules will be applied after those configured by the **rulebase** command.

For information about the syntax and options for each configuration available, refer to “set rulebase or set vsys rulebase” on page 220.

Syntax

```
set shared post-rulebase [refer to “set rulebase or set vsys rulebase” on page 220]
   {
   application-override rules <name> |
   captive-portal rules <name> |
   decryption rules <name> |
   default-security-rules rules {intrazone-default | interzone-default}|
   dos rules <name> |
   nat rules <name> |
   pbf rules <name> |
   qos rules <name> |
   security rules <name>
   }
```

Required Configuration

The following command configures device group objects so that they cannot override corresponding objects of the same name from a shared location.

```
username@hostname> set deviceconfig setting management shared-objects-take-precedence
   yes

username@hostname>
```

Required Privilege Level

superuser

set shared pre-rulebase

(Panorama only) Configures an additional layer of rules that will be applied to all device groups managed by the Panorama instance. The rules will be applied before those configured by the **rulebase** command.

For information about the syntax and options for each configuration available, refer to "set rulebase or set vsys rulebase" on page 220.

Syntax

```
set shared pre-rulebase [refer to "set rulebase or set vsys rulebase" on page 220]
    {
    application-override rules <name> |
    captive-portal rules <name> |
    decryption rules <name> |
    dos rules <name> |
    nat rules <name> |
    pbf rules <name> |
    qos rules <name> |
    security rules <name>
    }
```

Required Configuration

The following command configures device group objects so that they cannot override corresponding objects of the same name from a shared location.

```
username@hostname> set deviceconfig setting management shared-objects-take-precedence
    yes

username@hostname>
```

Required Privilege Level

superuser

set shared report-group

Specifies settings for report groups. Report groups allow you to create sets of reports that the system can compile and send as a single aggregate PDF report with an optional title page and all the constituent reports included.

Syntax

```
set shared report-group <name> |
   {
   title-page {no | yes} |
   custom-widget <value> |
     {
     custom-report <value> |
     log-view <value> |
     pdf-summary-report <value>
     predefined-report <value>
     }
   predefined user-activity-report |
   variable <name> {value <value>}
   }
```

Options

<name> — Report group to configure
+ title-page — Include title page
> custom-widget — Custom-widget value
   > custom-report — Custom report value
   > log-view — Log view value
   > pdf-summary-report — PDF summary report value
   > predefined-report — Predefined report value
> predefined — Predefined user activity report
> variable — Variable name; option to include a value

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared reports

Specifies shared settings for generating reports.

Syntax

```
set shared reports <name>
    {
    caption <value> |
    disabled {no | yes} |
    end-time <value> |
    frequency daily |
    period {last-12-hrs | last-15-minutes | last-24-hrs | last-30-days | last-60-seconds
      | last-7-calendar-days | last-7-days | last-calendar-day | last-calendar-month |
      last-calendar-week | last-hour} |
    query <value> |
    start-time <value> |
    topm <value> |
    topn <value> |
    type
      {
      appstat |
         {
         group-by {category-of-name | container-of-name | day-of-receive_time | hour-
            of-receive_time | name | quarter-hour-of-receive_time | risk | risk-of-name
            | subcategory-of-name | technology-of-name | vsys} |
         sortby {nbytes | npkts | nsess | nthreats} |
         aggregate-by {category-of-name | container-of-name | day-of-receive_time |
            hour-of-receive_time | name | quarter-hour-of-receive_time | risk | risk-
            of-name | subcategory-of-name | technology-of-name | vsys | <value>} |
         labels <value> |
         values {nbytes | npkts | nsess | nthreats | <value>}
         }
      data |
         {
         group-by {action | app | category-of-app | container-of-app | day-of-
            receive_time | direction | dport | dst | dstloc | dstuser | from | hour-of-
            receive_time | inbound_if | misc | natdport | natdst | natsport | natsrc |
            outbound_if | proto | quarter-hour-of-receive_time | risk-of-app | rule |
            severity | sport | src | srcloc | srcuser | subcategory-of-app | subtype |
            technology-of-app | threatid | to | vsys} |
         sortby repeatcnt |
         aggregate-by {action | app | category-of-app | container-of-app | day-of-
            receive_time | direction | dport | dst | dstloc | dstuser | from | hour-of-
            receive_time | inbound_if | misc | natdport | natdst | natsport | natsrc |
            outbound_if | proto | quarter-hour-of-receive_time | risk-of-app | rule |
            severity | sport | src | srcloc | srcuser | subcategory-of-app | subtype |
            technology-of-app | threatid | to | vsys | <value>} |
         labels <value> |
         values {repeatcnt | <value>}
         }
      hipmatch |
         {
         group-by {day-of-receive_time | hour-of-receive_time | machinename | matchname
            | matchtype | quarter-hour-of-receive_time | src | srcuser | vsys} |
         last-match-by time_generated |
         aggregate-by {day-of-receive_time | hour-of-receive_time | machinename |
            matchname | matchtype | quarter-hour-of-receive_time | src | srcuser | vsys
            | <value>} |
         labels <value> |
         values {repeatcnt | <value>}
         }
      threat |
         {
         group-by {action | app | category-of-app | container-of-app | day-of-
            receive_time | direction | dport | dst | dstloc | dstuser | from | hour-of-
            receive_time | inbound_if | misc | natdport | natdst | natsport | natsrc |
            outbound_if | proto | quarter-hour-of-receive_time | risk-of-app | rule |
            severity | sport | src | srcloc | srcuser | subcategory-of-app | subtype |
            technology-of-app | threatid | to | vsys} |
         sortby repeatcnt |
         aggregate-by {action | app | category-of-app | container-of-app | day-of-
            receive_time | direction | dport | dst | dstloc | dstuser | from | hour-of-
            receive_time | inbound_if | misc | natdport | natdst | natsport | natsrc |
            outbound_if | proto | quarter-hour-of-receive_time | risk-of-app | rule |
            severity | sport | src | srcloc | srcuser | subcategory-of-app | subtype |
            technology-of-app | threatid | to | vsys | <value>} |
         labels <value> |
         values {repeatcnt | <value>}
         }
      thsum |
         {
         group-by {app | category-of-app | container-of-app | day-of-receive_time | dst
            | dstloc | dstuser | from | hour-of-receive_time | quarter-hour-of-
            receive_time | risk-of-app | rule | severity-of-threatid | src | srcloc |
            srcuser | subcategory-of-app | subtype | technology-of-app | threatid | to
            | vsys} |
         sortby count |
         aggregate-by {app | category-of-app | container-of-app | day-of-receive_time |
            dst | dstloc | dstuser | from | hour-of-receive_time | quarter-hour-of-
            receive_time | risk-of-app | rule | severity-of-threatid | src | srcloc |
            srcuser | subcategory-of-app | subtype | technology-of-app | threatid | to
            | vsys | <value>} |
         labels <value> |
         values {count | <value>}
         }
      traffic |
         {
         group-by {action | app | category | category-of-app | container-of-app | day-
            of-receive_time | dport | dst | dstloc | dstuser | from | hour-of-
            receive_time | inbound_if | natdport | natdst | natsport | natsrc |
            outbound_if | proto | quarter-hour-of-receive_time | risk-of-app | rule |
            sessionid | sport | src | srcloc | srcuser | subcategory-of-app |
            technology-of-app | to | vsys} |
         sortby {bytes | bytes_received | bytes_sent | elapsed | packets |
            ptks_received | pkts_sent | repeatcnt} |
         aggregate-by {action | app | category | category-of-app | container-of-app |
            day-of-receive_time | dport | dst | dstloc | dstuser | from | hour-of-
            receive_time | inbound_if | natdport | natdst | natsport | natsrc |
            outbound_if | proto | quarter-hour-of-receive_time | risk-of-app | rule |
            sessionid | sport | src | srcloc | srcuser | subcategory-of-app |
            technology-of-app | to | vsys | <value>} |
         labels <value> |
         values {bytes | bytes_received | bytes_sent | elapsed | packets |
            ptks_received | pkts_sent | repeatcnt | <value>}
         }
      trsum |
         {
         group-by {app | category | category-of-app | container-of-app | day-of-
            receive_time | dst | dstuser | from | hour-of-receive_time | quarter-hour-
            of-receive_time | risk-of-app | rule | src | srcuser | subcategory-of-app |
            technology-of-app | to | vsys} |
         sortby {bytes | sessions} |
         aggregate-by {app | category | category-of-app | container-of-app | day-of-
            receive_time | dst | dstuser | from | hour-of-receive_time | quarter-hour-
            of-receive_time | risk-of-app | rule | src | srcuser | subcategory-of-app |
            technology-of-app | to | vsys | <value>} |
         labels <value> |
         values {bytes | sessions | <value>}
         }
      url
         {
         group-by {action | app | category | category-of-app | container-of-app |
            contenttype | day-of-receive_time | direction | dport | dst | dstloc |
            dstuser | from | hour-of-receive_time | inbound_if | misc | natdport |
            natdst | natsport | natsrc | outbound_if | proto | quarter-hour-of-
            receive_time | risk-of-app | rule | severity | sport | src | srcloc |
            srcuser | subcategory-of-app | technology-of-app | to | vsys} |
         sortby repeatcnt |
         aggregate-by {action | app | category | category-of-app | container-of-app |
            contenttype | day-of-receive_time | direction | dport | dst | dstloc |
            dstuser | from | hour-of-receive_time | inbound_if | misc | natdport |
            natdst | natsport | natsrc | outbound_if | proto | quarter-hour-of-
            receive_time | risk-of-app | rule | severity | sport | src | srcloc |
            srcuser | subcategory-of-app | technology-of-app | to | vsys | <value>} |
         labels <value> |
         values {repeatcnt | <value>}
         }
      }
   }
```

Options

<name> — Report to configure
+ caption — Caption value
+ disabled — Disabled (no or yes)
+ end-time — End time (e.g. 2008/12/31 11:59:59)
+ frequency — Configure the report to automatically run daily.
+ period — Time period to include in report (last 12 hrs, last 15 minutes, last 24 hrs, last 30 days, last 60 seconds, last 7 calendar days, last 7 days, last calendar day, last calendar month, last calendar week, or last hour)

```
+ query — Query value
+ start-time — Start time (e.g. 2008/01/01 09:00:00)
+ topm — TopM value (1-50)
+ topn — TopN value (1-500)
> type — Report type
    > appstat — Appstat report
        + group-by — Group by category of name, container of name, day of receive time, hour of receive time, name, quarter
            hour of receive time, risk, risk of name, subcategory of name, technology of name, or virtual system
        + sortby — Sort by nbytes, npkts, nsess, or nthreats
        > aggregate-by — Aggregate by category of name, container of name, day of receive time, hour of receive time, name,
            quarter hour of receive time, risk, risk of name, subcategory of name, technology of name, virtual system, or list of
            values enclosed in [ ]
        > labels — Label value or list of values enclosed in [ ]
        > values — Values (nbytes, npkts, nsess, nthreats, or list of values enclosed in [ ])
    > data — Data report
        + group-by — Select from the list provided
        + sortby — Sort by repeat count
        > aggregate-by — Select from the list provided or specify a list of values enclosed in [ ]
        > labels — Label value or list of values enclosed in [ ]
        > values — Values (repeat count, or list of values enclosed in [ ])
    > hipmatch — HIP match report
        + group-by — Select from the list provided
        + last-match-by — Last match by time generated
        > aggregate-by — Select from the list provided or specify a list of values enclosed in [ ]
        > labels — Label value or list of values enclosed in [ ]
        > values — Values (repeat count, or list of values enclosed in [ ])
    > threat — Threat report
        + group-by — Select from the list provided
        + sortby — Sort by repeat count
        > aggregate-by — Select from the list provided or specify a list of values enclosed in [ ]
        > labels — Label value or list of values enclosed in [ ]
        > values — Values (repeat count, or list of values enclosed in [ ])
    > thsum — thsum report
        + group-by — Select from the list provided
        + sortby — Sort by count
        > aggregate-by — Select from the list provided or specify a list of values enclosed in [ ]
        > labels — Label value or list of values enclosed in [ ]
        > values — Values (count, or list of values enclosed in [ ])
    > traffic — Traffic report
        + group-by — Select from the list provided
        + sortby — Sort by bytes, bytes received, bytes sent, elapsed, packets, packets received, packets sent, or repeatcnt
        > labels — Label value or list of values enclosed in [ ]
        > aggregate-by — Select from the list provided or specify a list of values enclosed in [ ]
        > values — Values (bytes, bytes received, bytes sent, elapsed, packets, packets received, packets sent, repeatcnt, or list of
            values enclosed in [ ])
    > trsum — trsum report
        + group-by — Select from the list provided
        + sortby — Sort by bytes or sessions
        > aggregate-by — Select from the list provided or specify a list of values enclosed in [ ]
        > labels — Label value or list of values enclosed in [ ]
        > values — Values (bytes, sessions, or list of values enclosed in [ ])
    > url — URL report
        + group-by — Select from the list provided
        + sortby — Sort by repeat count
```

> aggregate-by — Select from the list provided or specify a list of values enclosed in [ ]
> labels — Label value or list of values enclosed in [ ]
> values — Values (repeat count, or list of values enclosed in [ ])

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared response-page

Specifies settings for custom response pages. Custom response pages are the web pages that are displayed when a user tries to access a URL. You can provide a custom HTML message that is downloaded and displayed instead of the requested web page or file.

Syntax

```
set shared response-page
   {
   application-block-page <value> |
   captive-portal-text <value> |
   file-block-continue-page <value> |
   file-block-page <value> |
   ssl-cert-status-page <value> |
   ssl-optout-text <value> |
   url-block-page <value> |
   url-coach-text <value> |
   virus-block-page <value> |
   global-protect-portal-custom-help-page <name> {page <value>} |
   global-protect-portal-custom-login-page <name> {page <value>} |
   global-protect-portal-custom-welcome-page <name> {page <value>} |
   }
```

Options

+ application-block-page — Application block page value
+ captive-portal-text — Captive portal text value
+ file-block-continue-page — File block continue page value
+ file-block-page — File block page value
+ ssl-cert-status-page — SSL certificate status page value
+ ssl-optout-text — SSL optout text value
+ url-block-page — URL block page value
+ url-coach-text — URL coach text value
+ virus-block-page — Virus block page value
> global-protect-portal-custom-help-page — GlobalProtect portal custom help page name
   + page — GlobalProtect portal custom help page value
> global-protect-portal-custom-login-page — GlobalProtect portal custom login page name
   + page — GlobalProtect portal custom login page value
> global-protect-portal-custom-welcome-page — GlobalProtect portal custom welcome page name
   + page — GlobalProtect portal custom welcome page value

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared server-profile

Specifies settings for Kerberos, Lightweight Directory Access Protocol (LDAP), NetFlow, and RADIUS servers.

Syntax

```
set shared server-profile
   {
   kerberos <name> |
     {
     admin-use-only {no | yes} |
     domain <name> |
     realm <name> |
     server <name> {host <value> | port <value>}
     }
   ldap <name> |
     {
     admin-use-only {no | yes} |
     base <value> |
     bind-dn <value> |
     bind-password <value> |
     bind-timelimit <value> |
     disabled {no | yes} |
     domain <name> |
     ldap-type {active-directory | e-directory | none | sun} |
     retry-interval <value> |
     ssl {no | yes} |
     timelimit <value> |
     server <name> {address <value> | port <value>}
     }
   netflow <name> |
     {
     active-timeout {value} |
     export-enterprise-fields {no | yes} |
     server <name> {host {{<ip address/netmask> | <address object>} | <value>} | port
        <value>} |
     template-refresh-rate {minutes <value> | packets <value>}
     }
   radius <name>
     {
     admin-use-only {no | yes} |
     checkgroup {no | yes} |
     domain <name> |
     retries <value> |
     timeout <value> |
     server <name> {ip-address <ip_address> | port <value> | secret <value>}
     }
   }
```

Options

> kerberos — Kerberos profile name

```
    + admin-use-only — Can only be used for administrative purposes
    + domain — Domain name to be used for authentication
    + realm — Realm name to be used for authentication
    > server — Server name
        + host — Hostname running Kerberos Domain Controller
        + port — Kerberos Domain Controller (0-65535)
> ldap — LDAP profile name
    + admin-use-only — Can only be used for administrative purposes
    + base — Default base distinguished name (DN) to use for searches
    + bind-dn — Bind distinguished name
    + bind-password — Bind password
    + bind-timelimit — Number of seconds to use for connecting to servers (1-30)
    + disabled — Disabled (no or yes)
    + domain — Domain name to be used for authentication
    + ldap-type — LDAP type (Active Directory, E Directory, SUN, or other)
    + retry-interval — Interval (seconds) for retrying connecting to ldap search (1-3600, default = 60 seconds)
    + ssl — SSL (no or yes)
    + timelimit — number of seconds to wait for performing searches (1-30)
    > server — Server specification
        + address — LDAP server IP address (x.x.x.x or IPv6) or host name
        + port — Port (0-65535)
> netflow — NetFlow profile name
    + active-timeout — Number of minutes for the profile to remain active (1-60)
    + export-enterprise-fields — Include PAN-OS-specific field types in the NetFlow record
    > server — Server name
        + host — NetFlow server IP address and network mask (x.x.x.x/y) or host name
        + port — Port (0-65535)
    > template-refresh-rate — Refresh the NetFlow template ID after the specified number of minutes or packets
        + minutes — Number of minutes before refreshing the NetFlow template ID (1-3600)
        + packets — Number of packets before refreshing the NetFlow template ID (1-600)
> radius — RADIUS profile name
    + admin-use-only — Can only be used for administrative purposes
    + checkgroup — Retrieve user group from RADIUS
    + domain — Domain name to be used for authentication
    + retries — Number of attempts before giving up authentication (1-5)
    + timeout — Number of seconds to wait when performing authentication (1-30)
    > server — Server name
        + ip-address — RADIUS server IP address (x.x.x.x or IPv6)
        + port — RADIUS server port (0-65535)
        + secret — Shared secret for RADIUS communication
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set shared ssl-decrypt

Configures shared settings for Secure Socket Layer (SSL) decryption policies, which specify the SSL traffic to be decrypted so that security policies can be applied.

Syntax

```
set shared ssl-decrypt
   {
   forward-trust-certificate <value> |
   forward-untrust-certificate <value> |
   root-ca-exclude-list <value> |
   ssl-exclude-cert <value> |
   trusted-root-CA <value>
   }
```

Options

+ forward-trust-certificate — CA certificate for trusted sites
+ forward-untrust-certificate — CA certificate for untrusted sites
> root-ca-exclude-list — List of predefined root CAs to not trust
> ssl-exclude-cert — SSL exclude certificate (member value or list of values enclosed in [ ])
> trusted-root-CA — Trusted root CA (member value or list of values enclosed in [ ])

Required Privilege Level

superuser, vsysadmin, deviceadmin

set template

(Panorama only) Configures templates to manage and deploy configurations to multiple devices that require similar settings.

For more information, refer to the *Panorama Administrator's Guide*.

Syntax

```
set template <name>
   {
   description <value> |
   config | [for available configurations, refer to the separate command pages in this chapter]
     {
     deviceconfig |
     mgt-config |
     network |
     shared |
     vsys
     }
   devices <value> |
   settings
     multi-vsys {no | yes} |
     operational-mode {cc | fips | normal} |
     vpn-disable-mode {no | yes}
   }
```

Options

<name> — Specifies template to configure
+ description — Template description text
> config — Configurations that can be included in the template
    > deviceconfig — Device configurations [*refer to separate command pages in this chapter*]
    > mgt-config — Management configurations [*refer to separate command pages in this chapter*]
    > network — Network configuration [*refer to separate command pages in this chapter*]
    > shared — Shared configurations [*refer to separate command pages in this chapter*]
    > vsys — Virtual system configurations [*refer to separate command pages in this chapter*]
> devices — Device serial numbers
> settings — Template settings
    + multi-vsys — Multiple virtual systems (no or yes)
    + operational-mode — Operational mode (Common Criteria, FIPS, or Normal)
    + vpn-disable-mode — VPN disable mode (no or yes)

Required Privilege Level

superuser, vsysadmin, deviceadmin

set threats

Specifies settings for threat definitions. Palo Alto Networks periodically posts updates with new or revised application definitions and information on new security threats, such as antivirus signatures (threat prevention license required). To upgrade the firewall, you can view the latest updates, read the release notes for each update, and then select the update you want to download and install.

Syntax

```
set threats
   {
   spyware <threat_id> |
     {
     comment <value> |
     direction <value> |
     severity <value> |
     threatname <name> |
     bugtraq <value> |
     cve <value> |
     default-action |
        {
        alert |
        block-ip |
           {
           duration <value> |
           track-by {source | source-and-destination}
           }
        drop-packets |
        reset-both |
        reset-client |
        reset-server
        }
     reference <value> |
     signature |
        {
        combination |
           {
           order-free {no | yes} |
           and-condition <name> {or-condition <name>} {threat-id <threat_id>} |
           time-attribute
              {
              interval <value> |
              threshold <value> |
              track-by {destination | source | source-and-desintation}
              }
           }
        standard <name>
           {
           comment <value> |
           order-free {no | yes} |
           scope {protocol-data-unit | session} |
           and-condition <name> {or-condition <name>}
```

```
               {
               operator {equal-to | greater-than | less-than} |
                  {
                  context <value> |
                  value <value> |
                  qualifier <name> {value <value>}
                  }
               operator pattern-match
                  {
                  context <value> |
                  pattern <value> |
                  qualifier <name> {value <value>}
                  }
               }
            }
         }
      vendor <value>
      }
   vulnerability <value>
      {
      comment <value> |
      direction {both | client2server | server2client} |
      severity {critical | high | informational | low | medium} |
      threatname <name> |
      affected-host {client | server} {no | yes} |
      bugtraq <value> |
      cve <value> |
      default-action |
         {
         alert |
         block-ip |
            {
            duration <value> |
            track-by {source | source-and-desintation}
            }
         drop-packets |
         reset-both |
         reset-client |
         reset-server
         }
      reference <value> |
      signature |
         {
         combination |
            {
            order-free {no | yes} |
            and-condition <name> {or-condition <name>} {threat-id <threat_id>} |
            time-attribute
               {
               interval <value> |
               threshold <value> |
               track-by {destination | source | source-and-desintation}
               }
            }
         standard <name>
            {
            comment <value> |
            order-free {no | yes} |
            scope {protocol-data-unit | session} |
            and-condition <name> {or-condition <name>}
               {
               operator {equal-to | greater-than | less-than} |
                  {
                  context <value> |
                  value <value> |
                  qualifier <name> {value <value>}
                  }
               operator pattern-match
                  {
                  context <value> |
                  pattern <value> |
                  qualifier <name> {value <value>}
                  }
               }
            }
         }
      vendor <value>
      }
   }
```

Options

> spyware — Spyware threat ID (15000-18000)
    + comment — Spyware threat ID comment
    + direction — Direction value
    + severity — Severity value
    + threatname — Threat name (alphanumeric string [0-9a-zA-Z._-])
    > bugtraq — Bugtraq ID value or list of values enclosed in [ ]
    > cve — Common Vulnerabilities and Exposures (CVE) number (e.g., CVE-1999-0001) or list of values enclosed in [ ]
    > default-action — Default action (block IP address, alert, drop packets, reset client, reset server, or reset both)
        > block-ip — Block IP address
            + duration — Duration for block IP address (1-3600)
            + track-by — Track by source or source and destination
    > reference — Reference URL or list of values enclosed in [ ]
    > signature — Spyware signature
        > combination — Combination signature
            + order-free — Order free (no or yes)
            > and-condition — And-condition name
                > or-condition — Or-condition name
                    + threat-id — Threat ID value
            > time-attribute — Time attribute options
                + interval — Interval value (1-3600)
                + threshold — Threshold value (1-255)
                + track-by — Track by destination, source, or source and destination
        > standard — Standard signature
            + comment — Signature comment
            + order-free — Order free (no or yes)
            + scope — Protocol data unit transaction or session

```
            > and-condition — And-condition name
                > or-condition — Or-condition name
                    > operator — Operator (equal to, greater than, or less than)
                        + context — Select from the list provided or specify a value
                        + value — Value (0-4294967295)
                        > qualifier — Qualifier name; option to specify value
                    > operator — Operator pattern match
                        + context — Select from the list provided or specify a value
                        + pattern — Pattern value
                        > qualifier — Qualifier name; option to specify value
    > vendor — Vendor reference ID (e.g., MS03-026) or list of values enclosed in [ ]
> vulnerability — Vulnerability threat ID (41000-45000)
    + comment — Spyware threat ID comment
    + direction — Direction value (client to server, server to client, or both)
    + severity — Severity value (critical, high, informational, low, medium)
    + threatname — Threat name (alphanumeric string [ 0-9a-zA-Z._-])
    > affected-host — Affected host client or server
    > bugtraq — Bugtraq ID value or list of values enclosed in [ ]
    > cve — CVE number (e.g., CVE-1999-0001) or list of values enclosed in [ ]
    > default-action — Default action (block IP address, alert, drop packets, reset client, reset server, or reset both)
        > block-ip — Block IP address
            + duration — Duration for block IP address (1-3600)
            + track-by — Track by source or source and destination
    > reference — Reference URL or list of values enclosed in [ ]
    > signature — Vulnerability signature
        > combination — Combination signature
            + order-free — Order free (no or yes)
            > and-condition — And-condition name
                > or-condition — Or-condition name
                    + threat-id — Threat ID value (select from list or enter a value)
            > time-attribute — Time attribute options
                + interval — Interval value (1-3600)
                + threshold — Threshold value (1-255)
                + track-by — Track by destination, source, or source and destination
        > standard — Standard signature
            + comment — Signature comment
            + order-free — Order free (no or yes)
            + scope — Protocol data unit transaction or session
            > and-condition — And-condition name
                > or-condition — Or-condition name
                    > operator — Operator (equal to, greater than, or less than)
                        + context — Select from the list provided or specify a value
                        + value — Value (0-4294967295)
                        > qualifier — Qualifier name; option to specify value
                    > operator — Operator pattern match
                        + context — Select from the list provided or specify a value
                        + pattern — Pattern value
                        > qualifier — Qualifier name; option to specify value
    > vendor — Vendor reference ID (e.g., MS03-026) or list of values enclosed in [ ]
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set ts-agent

Configures a terminal server (TS) agent on the firewall. The TS agent runs on a terminal server and identifies individual users that the terminal server supports. This arrangement allows the firewall to support multiple users with the same source IP address. The TS agent monitors the remote user sessions and reserves a different TCP/UDP source port range for each user session. After a port range is allocated for the user session, the TS agent provides information to map the source port range to the user name.

Syntax

```
set ts-agent <name>
   {
   disable {no | yes} |
   host {{<ip address/netmask> | <address object>} | <value>} |
   port <port_number> |
   ip-list <value>
   }
```

Options

<name> — Specifies the terminal server agent to configure
+ disabled — Terminal server agent disabled (no or yes)
+ host — IP address and network mask or hostname for agent
+ port — Terminal server agent listening port number (1-65535)
> ip-list — Terminal server alternative IP address list (x.x.x.x or IPv6 or list of values enclosed in [ ]))

Required Privilege Level

superuser, vsysadmin, deviceadmin

set url-admin-override

Configures URL administrative override settings that are used when a page is blocked by the URL filtering profile and the Override action is specified.

Syntax

```
set user-admin-override
   {
   password <value> |
   server-certificate <value> |
   mode
      {
      redirect address {<host_name> | {<ip address/netmask> | <address object>}} |
      transparent
      }
   }
```

Options

+ password — Password for URL administrative override
+ server-certificate — SSL server certificate file name
> mode — Override mode
> > redirect — Redirect mode
> > + address — Set IP address or host name for URL administrative override
> > transparent — Transparent mode

Required Privilege Level

superuser, vsysadmin, deviceadmin

set url-content-types

Defines the HTML content types that will be available for custom pages and other services.

Syntax

```
set url-content-types <value>
```

Options

+ url-content-types — Content type string or list of values enclosed in [ ]
  - application/pdf — Default URL content type: application/PDF
  - application/soap+xml — Default URL content type: application/SOAP+XML
  - application/xhtml+xml — Default URL content type: application/XHTML+XML
  - text/html — Default URL content type: text/HTML
  - text/plain — Default URL content type: text/plain
  - text/xml — Default URL content type: text/XML

Required Privilege Level

superuser, vsysadmin, deviceadmin

set user-id-agent

Configures a User Identification Agent (User-ID Agent). A User-ID Agent is a Palo Alto Networks application that is installed on your network to obtain needed mapping information between IP addresses and network users. The User-ID Agent collects user-to-IP address mapping information automatically and provides it to the firewall for use in security policies and logging.

Syntax

```
set user-id-agent <name>
   {
   collectorname <value> |
   disabled {no | yes} |
   host {{<ip address/netmask> | <address object>} | <value>} |
   ldap-proxy {no | yes} |
   ntlm-auth {no | yes} |
   port <port_number> |
   secret <value>
   }
```

Options

<name> — Specifies the User-ID agent to configure
+ collectorname — Collector name on peer PAN OS
+ disabled — Disabled (no or yes)
+ host — IP address and network mask or hostname for User-ID agent
+ ldap-proxy — LDAP proxy
+ ntlm-auth — NTLM authentication
+ port — PAN User-ID agent listening port (1-65535; default = 5007)
+ secret — Collector pre-shared key on peer PAN OS

Required Privilege Level

superuser, vsysadmin, deviceadmin

set user-id-agent-sequence

Determines the order in which to use the configured User Identification Agents. To configure a User ID Agent, refer to “set user-id-agent” on page 285.

Syntax

```
set user-id-agent-sequence user-id-agents <name>
```

Options

<name> — List of user-ID agent name or list of names enclosed in [ ]

Required Privilege Level

superuser, vsysadmin, deviceadmin

set user-id-collector

Configures a User Identification Collector. Specifies settings to use the PAN-OS User Mapping feature to provide accurate mappings between IP addresses and logged-in users, as well as user-to-group membership mapping. This option performs the same functions as the User-ID Agent but directly from the firewall, so no agent is required on the domain controllers.

For more information, refer to the User-ID section in the *PAN-OS Administrator's Guide*.

Syntax

```
set user-id-collector <name>
   {
   directory-server <name> |
     {
     disabled {no | yes} |
     host <value> |
     server-profile <name> |
     type {active-directory | e-directory | exchange}
     }
   ignore-user <value> |
   include-exclude-network <name> |
     {
     disabled {no | yes} |
     discovery {exclude | include} |
     network-address {<ip address/netmask> | <address object>}
     }

   include-exclude-network-sequence include-exclude-network <name> |
   server-monitor <name> |
     {
     description <value> |
     disabled {no | yes} |
     active-directory host {<ip address/netmask> | <address object>} |
     e-directory server-profile <value> |
     exchange host {<ip address/netmask> | <address object>} |
     syslog
     {
        address <value> |
        connection-type {ssl | udp} |
        default-domain-name <value> | syslog-parse-profile <value> |
     }
   setting
     {
     client-probing-interval <value> |
     collectorname <value> |
     edirectory-query-interval <value> |
     enable-mapping-timeout {no | yes} |
     enable-ntlm {no | yes} |
     enable-probing {no | yes} |
     enable-security-log {no | yes} |
     enable-session {no | yes} |
     ip-user-mapping-timeout <value> |
     ntlm-domain <value> |
     ntlm-password <value> |
     ntlm-username <value> |
     secret <value> |
     security-log-interval <value> |
     session-interval <value> |
     wmi-account <value> |
     wmi-password <value>
     }
  syslog-parse-profile <value>
     {
     description <value>;
     field-identifier
        {
        address-delimiter <value>;
        address-prefix <value>;
        event-string <value>;
        username-delimiter <value>;
        username-prefix <value>;
        }
     regex-identifier
        {
        address-regex <value>;
        event-regex <value>;
        username-regex <value>;
        }
     }
  }
```

Options

<name> — Specifies the User ID collector to configure

> directory-server — Directory servers to monitor

+ disabled — Disabled (no or yes)

+ host — IP address and network mask (x.x.x.x/y) or hostname for the directory server

+ server-profile — LDAP server object name

+ type — Type of directory server

active-directory — Microsoft Active Directory

e-directory — Novell eDirectory

exchange — Microsoft Exchange

> ignore-user — List of users to ignore (value or list of values enclosed in [ ])

> include-exclude-network — Enter a name to identify the profile that will include or exclude a network for User-ID discovery purposes. This option allows you to include or exclude a network range for IP address-to-user name mapping. Example, if you exclude 10.1.1.0/24, User-ID will not try to find user names for IP addresses in the excluded range. This in turn will also include or exclude ranges for mappings sent to other PAN-OS firewalls. When defining an include or exclude network range, an implicit exclude-all will be performed. For example, if you include 10.1.1.0/24, all other networks will be excluded. If you exclude 10.1.1.0/24, all networks will be excluded, so when using exclude you must also have an include network, otherwise all networks are excluded.

+ disabled — Disabled (no or yes)

+ discovery — Exclude or Include (default is Include)

+ network-address — Network address/prefix (x.x.x.x/y) to include or exclude

> include-exclude-network-sequence — Include or exclude a network sequence

> server-monitor — Settings for the server monitor

+ description — Specify description

```
    + disabled — Enable or disable the server monitor
    + active-directory host — Specify an Active Directory host
    + e-directory — Specify a Novell eDirectory server
    + exchange host - Specify a Microsoft Exchange host
    + syslog-parse-profile — Specify syslog message parse profile
          + address — IP address
          + connection-type — Type of connection (SSL or UDP)
          + default-domain-name — Specify value
          + syslog-parse-profile — Specify value
> setting — Settings for the User ID Collector
    + client-probing-interval — Windows Management Instrumentation (WMI) client probing frequency, in minutes (1-1440)
    + collectorname — Collector name for data re-distribution
    + edirectory-query-interval — Server session read frequency, in seconds (1-3600)
    + enable-mapping-timeout — Enable mapping timeout
    + enable-ntlm — Enable NTLM authentication processing
    + enable-probing — Enable probing
    + enable-security-log — Enable security log
    + enable-session — Enable session
    + ip-user-mapping-timeout — IP user mapping timeout, in minutes (1-1440)
    + ntlm-domain — NetBIOS domain name for NTLM domain
    + ntlm-password — Password for NTLM admin
    + ntlm-username — NTLM admin username (e.g., administrator)
    + secret — Pre-shared key for data re-distribution
    + security-log-interval — Security log monitor frequency, in seconds (1-3600)
    + session-interval — windows server session monitor frequency, in seconds (1-3600)
    + wmi-account — AD account name for WMI query (e.g., domain\username)
    + wmi-password — Password for AD account for WMI query
> syslog-parse-profile — Settings profile to parse syslog messages to extract user mapping information
    + description — Specify profile description
    > field-identifier — Specify values for any of the following types of field identifiers
       + address-delimiter
       + address-prefix
       + event-string
       + username-delimiter
       + username-prefix
    > regex-identifier — Specify values for any of the following types of regular expression identifiers
       + address-regex
       + event-regex
       + username-regex
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set vsys application

Specifies settings at the application level for a virtual system.

This command is available only when virtual systems are enabled. Refer to "set system" on page 456, and "Using Configuration Commands with Virtual Systems" on page 25.

Syntax

```
set vsys <name> application <name>
    {
    tcp-half-closed-timeout <value> |
    tcp-time-wait-timeout <value> |
    tcp-timeout |
    timeout |
    udp-timeout
    }
```

Options

* vsys <name> — Name of the virtual system.
* application <name> — Name of the application.

+ tcp-half-closed-timeout <value> — Maximum time after the virtual system sees the first FIN and before the TCP session closes, in seconds. (1-604800; default is the value of the global setting)
+ tcp-time-wait-timeout <value> — Maximum time after the virtual system sees the second FIN or a RST and before the TCP session closes, in seconds. (1-600; default is the value of the global setting)
+ tcp-timeout — Maximum time before an idle TCP application flow is terminated, in seconds. (0-604800; default is the value of the global setting)
+ timeout — Maximum time before an idle application flow is terminated, in seconds. This timer is for protocols other than TCP and UDP. (0-604800; default is the value of the global setting) A setting of 0 indicates that the default timeout of the application will be used.
+ udp-timeout — Maximum time before an idle UDP application flow is terminated, in seconds. (0-604800; default is the value of the global setting) A setting of 0 indicates that the default timeout of the application will be used.

Required Privilege Level

superuser, vsysadmin, deviceadmin

set vsys import

Specifies settings for importing configuration files to the firewall.

This command is available only when virtual systems are enabled. Refer to "set system" on page 456, and "Using Configuration Commands with Virtual Systems" on page 25.

Syntax

```
set vsys <name> import
   {
   dns-proxy <value> |
   network |
      {
      interface <value> |
      virtual-router {default | <value>} |
      virtual-wire {default-wire | <value>} |
      vlan <value>
      }
   resource |
      {
      max-application-override-rules <value> |
      max-concurrent-ssl-vpn-tunnels <value> |
      max-cp-rules <value> |
      max-dos-rules <value> |
      max-nat-rules <value> |
      max-pbf-rules <value> |
      max-qos-rules <value> |
      max-security-rules <value> |
      max-sessions <value> |
      max-site-to-site-vpn-tunnels <value> |
      max-ssl-decryption-rules <value>
      }
   visible-vsys <value>
   }
```

Options

+ dns-proxy — DNS proxy object to use for resolving FQDNs
> network — Network configuration
    > interface — Import interface (ethernet, loopback, tunnel, vlan, value or list of values enclosed in [ ])
    > virtual-router — Import virtual router (default, or value or list of values enclosed in [ ])
    > virtual-wire — Import virtual wire (default-wire, or value or list of values enclosed in [ ])
    > vlan — Import VLAN (value or list of values enclosed in [ ])
> resource — Limits on resources used by this virtual system
    + max-application-override-rules — Maximum number of application override rules allowed for this virtual system (0-2000)
    + max-concurrent-ssl-vpn-tunnels — Maximum number of concurrent SSL VPN tunnels allowed for this virtual system (0-10000)
    + max-cp-rules — Maximum number of captive portal rules allowed for this virtual system (0-2000)
    + max-dos-rules — Maximum number of Denial of Service (DoS) rules allowed for this virtual system (0-1000)
    + max-nat-rules — Maximum number of Network Address Translation (NAT) rules allowed for this virtual system (0-4000)

+ max-pbf-rules — Maximum number of Policy-based Forwarding (PBF) rules allowed for this virtual system (0-500)
+ max-qos-rules — Maximum number of Quality of Service (QoS) rules allowed for this virtual system (0-2000)
+ max-security-rules — Maximum number of security rules allowed for this virtual system (0-20000)
+ max-sessions — Maximum number of sessions allowed for this virtual system (0-4194290)
+ max-site-to-site-vpn-tunnels — Maximum number of site-to-site VPN tunnels allowed for this virtual system (0-10000)
+ max-ssl-decryption-rules — Maximum number of SSL decryption rules allowed for this virtual system (0-2000)

> visible-vsys — Makes the specified virtual system visible to this virtual system, to create inter-vsys traffic

Required Privilege Level

superuser, vsysadmin, deviceadmin

set zone

Configures security zones, which identify source and destination interfaces on the firewall for use in security policies. Zones that are set using this command will appear in the list of zones when defining security policies and configuring interfaces.

Syntax

```
set zone <name>
   {
   enable-user-identification {no | yes} |
   network |
     {
     log-setting <value> |
     zone-protection-profile <value> |
     layer2 <value> |
     layer3 <value> |
     tap <value> |
     virtual-wire <value>
     }
   user-acl
     {
     + exclude-list <value> |
     + include-list <value>
     }
   }
```

Options

<name> — Specifies the zone to configure. A zone name can be up to 15 characters and can include only letters, numbers, spaces, hyphens, periods, and underscores. The name is case-sensitive and must be unique.
+ enable-user-identification — Enable user identification
> network — Network configuration
   + log-setting — Log setting for forwarding scan logs
   + zone-protection-profile — Zone protection profile name
   > layer2 — Layer2 interfaces (member value or list of values enclosed in [ ])
   > layer3 — Layer3 interfaces (member value or list of values enclosed in [ ])
   > tap — Tap mode interfaces (member value or list of values enclosed in [ ])
   > virtual-wire — Virtual-wire interfaces (member value or list of values enclosed in [ ])
> user-acl — User Access Control List (ACL) configuration
   > exclude-list — Exclude list (IP address and network mask (x.x.x.x/y) or list of values enclosed in [ ])
   > include-list — Include list (IP address and network mask (x.x.x.x/y) or list of values enclosed in [ ])

Required Privilege Level

superuser, vsysadmin, deviceadmin

show

Displays information about the current candidate configuration.

Syntax

```
show <context>
```

Options

<context> — Specifies a path through the hierarchy. For available contexts in the hierarchy, press <tab>.

Sample Output

The following command shows the full candidate hierarchy.

```
username@hostname# show
```

The following commands can be used to display the hierarchy segment for *network interface*.

- Specify context on the command line:

  ```
  show network interface
  ```

- Use the **edit** command to move to the level of the hierarchy, and then use the **show** command without specifying context:

  ```
  edit network interface
  [edit network interface] show
  ```

Required Privilege Level

superuser, vsysadmin, deviceadmin

show deviceconfig setting ssl-decrypt

Displays the current key size setting of the certificates that the firewall uses for its connection with the client during SSL/TLS Forward Proxy Server communication. For more information, refer to the PAN-OS Administrator’s Guide.

Syntax

```
show deviceconfig setting ssl-decrypt
```

Options

None

Sample Output

The following command shows that the firewall generates certificates that use a 1024-bit RSA key for its connection with the client regardless of the key size that the destination server uses.

```
username@hostname> show deviceconfig setting ssl-decrypt
ssl-decrypt {
   notify-user no;
   url-proxy yes;
   answer-timeout 100;
   fwd-proxy-server-cert-key-size 1024;
   }
```

Required Privilege Level

superuser, superuser (read only), Panorama admin

top

Changes context to the top hierarchy level.

Syntax

```
top
```

Options

None

Sample Output

The following command changes context from the network level of the hierarchy to the top level.

```
[edit network]
username@hostname# top

[edit]                                                              username@hostname#
```

Required Privilege Level

All

up

Changes context to the next higher hierarchy level.

Syntax

```
up
```

Options

None

Sample Output

The following command changes context from the *network interface* level of the hierarchy to the network level.

```
[edit network interface]
   username@hostname# up

[edit network]
   username@hostname#
```

Required Privilege Level

All

Chapter 4
Operational Mode Commands

This chapter contains command reference pages for the following operational mode commands:

- “debug mprelay” on page 351
- “debug netconfig-agent” on page 352
- “debug pppoed” on page 353
- “debug rasmgr” on page 354
- “debug routing” on page 355
- “debug satd” on page 357
- “debug software” on page 358
- “debug ssl-vpn” on page 360
- “debug sslmgr” on page 361
- “debug swm” on page 363
- “debug system” on page 364
- “debug tac-login” on page 365
- “debug user-id” on page 366
- “debug vardata-receiver” on page 372
- “debug wildfire” on page 373
- “delete” on page 375
- “diff-all” on page 378
- “exit” on page 379
- “ftp” on page 381
- “grep” on page 382
- “less” on page 383
- “ls” on page 384
- “netstat” on page 385
- “ping” on page 387
- “quit” on page 389
- “request acknowledge” on page 390
- “request analyze-shared-policy” on page 391
- “request anti-virus” on page 392
- “request batch” on page 394
- “request certificate” on page 400
- “request chassis” on page 402

- “show dns-proxy” on page 480
- “show dos-protection” on page 481
- “show global-protect” on page 482
- “show global-protect-gateway” on page 483
- “show global-protect-mdm” on page 485
- “show global-protect-satellite” on page 486
- “show high-availability” on page 487
- “show hsm” on page 488
- “show interface” on page 489
- “show jobs” on page 491
- “show lacp aggregate-ethernet” on page 492
- “show location” on page 494
- “show log” on page 495
- “show log-collector” on page 511
- “show log-collector-group” on page 512
- “show logging-status” on page 514
- “show mac” on page 515
- “show management-clients” on page 516
- “show migration-log” on page 517
- “show neighbor” on page 518
- “show ntp” on page 519
- “show object” on page 520
- “show operational-mode” on page 521
- “show panorama-certificates” on page 522
- “show panorama-status” on page 523
- “show pbf” on page 524
- “show pppoe” on page 525
- “show qos” on page 526
- “show query” on page 527
- “show report” on page 528
- “show resource” on page 530

- “show routing” on page 531
- “show rule-use” on page 538
- “show running” on page 539
- “show session” on page 543
- “show sslmgr-store” on page 547
- “show statistics” on page 549
- “show system” on page 550
- “show templates” on page 554
- “show threat” on page 555
- “show url-cloud” on page 556
- “show user” on page 557
- “show virtual-wire” on page 561
- “show vlan” on page 562
- “show vm-monitor” on page 563
- “show vpn” on page 564
- “show wildfire” on page 566
- “show zone-protection” on page 569
- “ssh” on page 570
- “tail” on page 571
- “target” on page 572
- “tcpdump” on page 573
- “test” on page 574
- “tftp export” on page 579
- “tftp import” on page 581
- “traceroute” on page 583
- “view-pcap” on page 585

clear

Resets information, counters, sessions, or statistics.

Syntax

```
clear
   {
   application-signature statistics |
   arp {all | <interface_name>} |
   counter |
     {
     all |
     global |
        {
        filter |
           {
           aspect <value> |
           category <value> |
           packet-filter {no | yes} |
           severity <value>
           }
        name <value>
        }
     interface
     }
   dhcp lease |
     {
     all |
     interface <value>
        {
        expired-only |
        ip <ip> |
        mac <mac_address>
        }
     }
   dns-proxy |
     {
     cache {all | name <name>} domain-name <value> |
     statistics {all | name <value>}
     }
   dos-protection |
     {
     rule <name> statistics |
     zone <name> blocked {all | source <ip/netmask>}
     }
   high-availability {control-link statistics | transitions} |
   job id <value> |
   lacp counters aggregate-ethernet <all | ae-name>
   log {acc | alarm | config | hipmatch | system | threat | traffic | userid}
     |
   log-collector stats runtime ld <value> segment <value> {active-segments
```

```
  {no | yes}} |
log-receiver netflow counters |
mac {all | <value>} |
nat-rule-cache rule <name> |
neighbor {all | <interface_name>} |
object dynamic {all | id <value>} |
pbf |
  {
  return-mac {all | name <name>} |
  rule {all | name <name>}
  }
pppoe interface <name> |
query {all-by-session | id <value>} |
report {all-by-session | id <value>} |
routing |
  {
  bgp virtual-router <name> |
     {
     dampening {prefix <ip/netmask> | peer <value>} |
     stat peer <value>
     }
  multicast
     {
     igmp statistics {virtual-router <name>} |
     pim statistics {virtual-router <name>}
     }
  }
session |
  {
  all |
     {
     filter application <value> |
     filter destination <ip_address> |
     filter destination-port <port_number> |
     filter destination-user {known-user | unknown | <value>} |
     filter dos-rule <rule_name> |
     filter from <zone> |
     filter hw-interface <interface_name> |
     filter min-kb <value> |
     filter nat {both | destination | none | source} |
     filter nat-rule <rule_name> |
     filter pbf-rule <rule_name> |
     filter protocol <value> |
     filter qos-class <value> |
     filter qos-node-id <value> |
     filter qos-rule <rule_name> |
     filter rule <rule_name> |
     filter source <ip_address> |
     filter source-port <port_number> |
     filter source-user {known-user | unknown | <value>} |
     filter ssl-decrypt {no | yes} |
     filter state {active | closed | closing | discard | initial |
        opening} |
     filter to <zone> |
     filter type {flow | predict} |
     filter vsys-name <value>
     }
  id <value>
  }
statistics |
uid-gids-cache {all | uid <value>} |
url-cache {all | url <value>} |
user-cache {all | ip <ip/netmask>} |
user-cache-mp {all | ip <ip/netmask>} |
vpn
  {
  flow {tunnel-id <value>} |
  ike-sa {gateway <value>} |
  ipsec-sa {tunnel <value>}
  }
wildfire counters
}
```

Options

> application-signature — Clears application signature statistics
> arp — Clears Address Resolution Protocol (ARP) information for a specified interface, loopback, or VLAN, or all
> counter — Clears counters
> all — Clears all counters
> global — Clears global counters only
> filter — Apply counter filters
+ aspect — Counter aspect
aa — HA Active/Active mode
arp — ARP processing
dos — DoS protection
forward — Packet forwarding
ipfrag — IP fragment processing
mgmt — Management plane packet
mld — MLD processing
nd — ND processing
offload — Hardware offload
parse — Packet parsing
pktproc — Packet processing
qos — QoS enforcement
resource — Resource management
session — Session setup/teardown
system — System function
tunnel — Tunnel encryption/decryption
+ category — Counter category
aho — AHO match engine
appid — Application identification
ctd — Content identification
dfa — DFA match engine
dlp — DLP
flow — Packet processing
fpga — FPGA
ha — High Availability

```
                log — Logging
                nat — Network Address Translation
                packet — Packet buffer
                proxy — TCP proxy
                session — Session management
                ssh — SSH termination
                ssl — SSL termination
                tcp — TCP reordering
                url — URL filtering
                zip — ZIP processing
            + packet-filter — Counters for packet that matches debug filter (no or yes)
            + severity — Counter for severity (drop, error, informational, or warning)
        > name — Counter name
    > interface — Clears interface counters only
> dhcp — Clears Dynamic Host Configuration Protocol (DHCP) leases
    > all — Clears leases on all interfaces
    > interface — Clears leases on a specific interface
        > expired-only — Clears expired leases
        > ip — Clears lease for the specified IP address (x.x.x.x or IPv6)
        > mac — Clears lease for the specified MAC address (xx:xx:xx:xx:xx:xx)
> dns-proxy — Clears DNS proxy information
    > cache — Clears DNS proxy cache
        > all — Clears all DNS proxy caches (option to provide the domain name)
        > name — Clears DNS proxy object name (option to provide the domain name)
    > statistics — Clears DNS proxy statistics
        > all — Clears all DNS proxy statistics
        > name — Clears DNS proxy object name
> dos-protection — Clears Denial of Service (DoS) protection-related information
    > rule — DoS protection rule name
    > zone — Source zone name
        > all — Clears all IP addresses
        > source — Specify source IP addresses to unblock (x.x.x.x/y or IPv6/netmask)
> high-availability — Clears high-availability statistics
    > control-link — Clears high-availability control-link information
    > transitions — Clears high-availability transition statistics
> job — Clears download jobs (0-4294967295)
> lacp counters aggregate-ethernet <all | ae-name> — Clears Link Aggregation Control Protocol (LACP) statistics
> log — Removes logs on disk
    > acc — ACC database
    > alarm — Alarm logs
    > config — Configuration logs
    > system — System logs
    > threat — Threat logs
    > traffic — Traffic logs
```

Note: The **clear log** options to clear individual log types (acc, alarm, config, etc.) is not supported on the Panorama M-100 appliance. If you need to clear all logs, including the configuration, you can use the **request system private-data-reset** command. Do not run this command unless your configuration is backed up.

```
> log-collector — Clears the log collector statistics
    + active-segments — Only display active segments
    * ld — Logical disk number (1-4)
    * segment — Segment ID (all or 0-255)
> log-receiver — Clears the NetFlow counters
> mac — Clears MAC information (all or specific VLAN MAC information dot1q-vlan)
> nat-rule-cache — Clears the specified dynamic IP Network Address Translation (NAT) rule IP pool cache
> neighbor — Clears the neighbor cache (all or specified interface neighbor cache entries)
> object — Clears IP address object
    > all — Clears all dynamic address objects
    > id — Clears a dynamic address object by id
> pbf — Clears policy-based forwarding (PBF) runtime rules (all or specified)
    > return-mac — Clears PBF return mac info (all or specified)
    > rule — Clears PBF rule stats (all or specified)
> pppoe — Clears the specified Point-to-Point Protocol over Ethernet (PPPoE) interface connection
> query — Clears query jobs (all queries for the session, or by ID 0-4294967295)
> report — Clears report jobs (all reports for the session, or by ID 0-4294967295)
> routing — Clears routing information
    > bgp — Clears BGP counters
       > dampening — Resets BGP route dampening status (option to filter by prefix or by BGP peer)
       > stat — Clears statistic counters (option to filter by BGP peer)
    > multicast — Clears multicast statistics
       > igmp — Clears IGMP counters (option to filter by virtual router)
       > pim — Clears PIM counters (option to filter by virtual router)
> session — Clears a specified session or all sessions
    > all — Clears all sessions; the following filter options are available:
       + application — Application name (press <tab> for a list of applications)
       + destination — Destination IP address
       + destination-port — Destination port (1-65535)
       + destination-user — Destination user (select known-user or unknown, or enter a user name)
       + dos-rule — DoS protection rule name
       + from — From zone
       + hw-interface — Hardware interface
       + min-kb — Minimum KB of byte count (1-1048576)
       + nat — If session is NAT (select Both source and destination NAT, Destination NAT, No NAT, or
          Source NAT)
       + nat-rule — NAT rule name
       + pbf-rule — Policy-based forwarding rule name
       + protocol — IP protocol value (1-255)
       + qos-class — QoS class (1-8)
       + qos-node-id — QoS node-id value (-2 for bypass mode; 0-5000 for regular or tunnel mode)
       + qos-rule — QoS rule name
       + rule — Security rule name
       + source — Source IP address
       + source-port — Source port (1-65535)
       + source-user — Source user (select known-user or unknown, or enter a user name)
       + ssl-decrypt — Session is decrypted (no or yes)
       + state — Flow state
          active — Active state
          closed — Closed state
          closing — Closing state
          discard — Discard state
          initial — Initial state
          opening — Inactive state
       + to — To zone
       + type — Flow type (flow = regular flow; predict = predict flow)
       + vsys-name — Virtual system name
    > id — Clears specific session (1-2147483648)
> statistics — Clears all statistics
> uid-gids-cache — Clears the user ID to group IDs (uid-gids) cache in the data plane (all or specified user ID, 1-
    2147483647)
> url-cache — Clears the URL cache in the data plane
    > all — Clears all URLS in data plane
```

  > url — Clears the specified URL from data plane (For the Palo Alto Networks URL filtering database only)
> user-cache — Clears the IP-to-user cache in the data plane (all or specified IP, x.x.x.x/y or IPv6)
> user-cache-mp — Clears the management plane user cache
  > all — Clears all ip to user cache in management plane
  > ip — Clears the specified IP to user cache in management plane (IP address and network mask, x.x.x.x/y)
> vpn — Clears Internet Key Exchange (IKE) or IP Security (IPSec) VPN runtime objects
  > flow — Clears the VPN tunnel on the data plane. Specify the tunnel or press **Enter** to apply to all tunnels.
  > ike-sa — Removes the active IKE Security Association (SA) and stops all ongoing key negotiations. Specify the gateway or press **Enter** to apply to all gateways.
  > ipsec-sa — Deactivates the IPsec SA for a tunnel or all tunnels. Specify the tunnel or press **Enter** to apply to all tunnels.
> wildfire — Clears the Wildfire statistics counters

Sample Output

The following command clears the session with ID 2245.

```
username@hostname> clear session id 2245
Session 2245 cleared
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

commit-all

(Panorama only) Commits a specified configuration, policy, or template. Applies the candidate configuration to the firewall. A committed configuration becomes the active configuration for the device.

Syntax

```
commit-all
   {
   log-collector-config log-collector-group <name> |
   shared-policy |
     {
     device <value> |
     include-template {no | yes} |
     merge-with-candidate-cfg {no | yes} |
     remove-overridden-objects {no | yes} |
     device-group <value> |
     vsys <value>
     }
   template
     {
     merge-with-candidate-cfg {no | yes} |
     remove-overridden-objects {no | yes} |
     name <value> |
     device <value>
     }
   }
```

Options

> log-collector-config — Log collector configuration to commit
  + log-collector-group — Log collector group name
> shared-policy — Shared policy to commit
  + device — Device serial number
  + include-template — Whether to include relevant template
  + merge-with-candidate-cfg — Whether to merge with candidate configuration
  + remove-overridden-objects — Whether to remove overridden template objects on the device
  * device-group — Device group name
  > vsys — Virtual system name, or list of names separated by [ ]
> template — Template to commit
  + merge-with-candidate-cfg — Whether to merge with candidate configuration
  + remove-overridden-objects — Whether to remove overridden template objects on the device
  * name — Template name
  > device — Device name, or list of names separated by [ ]

Required Privilege Level

superuser, vsysadmin, deviceadmin

configure

Enters Configuration mode.

Syntax

```
configure
```

Options

None

Sample Output

To enter Configuration mode from Operational mode, enter the following command.

```
username@hostname> configure
Entering configuration mode

[edit]
    username@hostname#
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

debug authd

Defines settings for authd service debug logging.

Syntax

```
debug authd {off | on | show}
```

Options

> off — Turns off debug logging
> on — Turns on authd service debug logging
> show — Displays current debug logging setting

Sample Output

The following command turns the authd debugging option on.

```
admin@PA-HDF> debug authd on
admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug cli

Defines settings and display information for debugging the CLI connection.

Syntax

```
debug cli
   {
   detail |
   off |
   on |
   show
   }
```

Options

> detail — Shows details information about the CLI connection
> off — Turns the debugging option off
> on — Turns the debugging option on
> show — Shows whether this command is on or off

Sample Output

The following command shows details of the CLI connection.

```
admin@PA-HDF> debug cli detail
Environment variables :
(USER . admin)
(LOGNAME . admin)
(HOME . /home/admin)
(PATH . /usr/local/bin:/bin:/usr/bin)
(MAIL . /var/mail/admin)
(SHELL . /bin/bash)
(SSH_CLIENT . 10.31.1.104 1109 22)
(SSH_CONNECTION . 10.31.1.104 1109 10.1.7.2 22)
(SSH_TTY . /dev/pts/0)
(TERM . vt100)
(LINES . 24)
(COLUMNS . 80)
(PAN_BASE_DIR . /opt/pancfg/mgmt)

PAN_BUILD_TYPE : DEVELOPMENT

Total Heap : 7.00 M
Used       : 5.51 M
Nursery    : 0.12 M
admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug cryptod

Sets the debug options for the cryptod daemon.

Syntax

```
debug cryptod
   {
   global {off | on | show}
   show counters
   }
```

Options

> global — Controls debug levels
>   > show — Shows whether this command is on or off
>   > off — Turns the debugging option off
>   > on — Turns the debugging option on
> show — Shows Cryptod debug counters

Sample Output

The following command displays the current cryptod debugging setting.

```
admin@PA-HDF> debug cryptod global show

sw.cryptod.runtime.debug.level: debug


admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug dataplane

Configures settings for debugging the data plane.

Syntax

```
debug dataplane
   {
   device switch-dx |
     {
     fdb {dump | index <value>} |
     port-based-vlan port <value> |
     register read <value> |
     uplink |
     vlan-table {dump | index <value>} |
     }
   flow-control {disable | enable} |
   fpga |
     {
     set {sw_aho | sw_dfa | sw_dlp} {no | yes} |
     state
     }
   internal |
     {
     pdt |
        {
        lion |
           {
           egr |
              {
              nexthop dump |
              queues type {active | all | flags | high} |
              route dump |
              stats
              }
           igr |
              {
              drops |
              flow dump {id <value> | offset <value> | verbose {no | yes}} |
              info |
              interface {dump | info} |
              mac dump |
              port {dump | stats} |
              queues type {active | all | flags | high}
              }
           mac stats |
           spi stats
           }
        nac |
           {
           aho dump {table <value>} instance <value> |
           dfa dump {table <value>} instance <value> |
   info instance <value> |
   stats instance <value>
   }
fe20
(
   acl dump {slot <slot>} |
   flow dump verbose {yes | no} {id <value>} {count <value>} {slot
       <value>} |
   flow count {slot <value>} |
   lif map dump count <value> {slot <value>} |
   lif dump count <value> table <0|1> {slot <value>} |
   port mac dump {slot <value>} |
   port mac dump {slot <value>} |
   port stats clear {yes | no}  {slot value} |
   lagmap dump {slot <value>} |
   mac dump {slot <value>} |
   mymac dump {slot <value>} |
   nexthop dump type {DIRECT|IPV4|IPV6|MAC|QMV4|QMV6} {slot <value>}
       |
   qmap dump {slot <value>} |
   route dump {slot <value>} |
   stats clear {yes | no}  {slot <value>} |
   rd offset <value> count <value> {slot <value>} |
   show config {slot <value>} |
   show version {slot <value>} |
   spaui epb_status {slot <value>} |
   spaui info {slot <value>} |
   spaui stats clear {yes | no}  {slot <value>} |
   sram dump offset <value> len <value> {slot <value>} |
   sram info {slot <value>} |
   xaui info {slot <value>} |
   xge epb_status {slot <value>} |
   xge info {slot <value>} |
   xge stats clear {yes | no}  {slot <value>} |
   xge20g epb_status {slot <value>} |
   xge20g info {slot <value>} |
   xge20g stats clear {yes | no}  {slot <value>} |
}
{
marvell
{
   portmap slot {slot <value>}
   porttag port <0-128> slot {slot <value>}
   stats clear {yes | no} {slot <value>} proc {mp|cp|dp0|dp1|fpp}
}
{
jaguar
   cip ififo instance <0-1> slot {slot <value>}
   cip ofifo instance <0-1> slot {slot <value>}
   cip status instance <0-1> slot {slot <value>}
   rd instance <0-1> offset <0-65535> count <0-1024> slot {slot
       <value>}
   show clocks instance <0-1> slot {slot <value>}
   show version instance <0-1> slot {slot <value>}
```

```
         xaui info instance <0-1> slot {slot <value>}
         xge epb_status instance <0-1> slot {slot <value>}
         xge info instance <0-1> slot {slot <value>}
         xge stats instance <0-1> clear {yes | no}  slot {slot <value>}
      }
      {
      petra
      {
         counters chip slot {slot <value>}
         counters port slot {slot <value>}
         lport shaper get lport <value> fport <value> type <value> index
            <value5> {slot <value>}
         show non_empty_queues {slot <value>}
         show traffic_info {slot <value>}
      }
      {
      se20
      {
         aurora info slot <s0|s1|s2|s3|s4|s5|s6|s7|s8> proc
            {mp|cp|dp0|dp1|fpp}
         aurora stats clear {yes | no} {slot <value>} proc
            {mp|cp|dp0|dp1|fpp}
         sram info {slot <value>} proc {mp|cp|dp0|dp1|fpp}
         stats chip {slot <value>} proc {mp|cp|dp0|dp1|fpp}
         show clocks {slot <value>} proc {mp|cp|dp0|dp1|fpp}
         show version {slot <value>} proc {mp|cp|dp0|dp1|fpp}
         xaui info {slot <value>} proc {mp|cp|dp0|dp1|fpp}
         xge info {slot <value>} proc {mp|cp|dp0|dp1|fpp}
         xge stats clear {yes | no} {slot <value>} proc
            {mp|cp|dp0|dp1|fpp}
      oct
         {
         bootmem {avail | named} {slot <slot>} | {proc <value>} |
         csr rd {reg <value> | slot <slot> | proc <value>} |
         fpa show | {slot <slot> | proc <value>} |
         pip stats {port <port_number>} | {slot <slot>} | {proc <value>}}
            |
         pko |
            {
            debug {port <port_number>} | {slot <slot>} | {proc <value>}} |
            stats {all {no | yes} | {port <port_number>} | {slot <slot>} |
               {proc <value>}} |
         pow debug {all {no | yes}} | {port <port_number>} | {slot <slot>}
            |
         }
      }
   vif {address | link | route <value> | rule | vr}
   }
memory status |
monitor detail {off | on | show} |
nat sync-ippool rule <rule_name> |
packet-diag |
   {
   clear |
      {
      all |
      capture |
         {
         all |
         snaplen |
         stage {drop | firewall | receive | transmit} |
         trigger application
         }
      filter {all | <filter_index>} |
      log
         {
         counter {all | <value>} |
         feature |
            {
            all |
            appid {agt | all | basic | dfa | policy} |
            cfg {agent | all | basic | config} |
            ctd {all | basic | detector | sml | url} |
            flow {ager | all | arp | basic | ha | nd | np | receive} |
            misc {all | misc} |
            module {aho | all | dfa | scan | url} |
            pow {all | basic} |
            proxy {all | basic} |
            ssl {all | basic} |
            tcp {all | fptcp | reass} |
            tunnel {ager | flow} |
            zip {all | basic}
            }
         log
         }
      }
   set |
      {
      capture |
         {
         off |
         on |
         snaplen <value> |
         stage {drop | firewall | receive | transmit} file <file_name> |
            {
            byte-count <value> |
            packet-count <value>
            }
         trigger application file <file_name> from <application_name> to
            <application_name>
            {
            byte-count <value> |
            packet-count <value>
            }
         }
      filter |
         {
         index <value> |
        match |
            {
            destination <ip_address> |
            destination-port <port> |
            ingress-interface <interface_name> |
            ipv6-only {no | yes} |
            non-ip {exclude | include | only} |
            protocol <value> |
            source <ip_address> |
            source-port <port>
            }
        off |
        on |
        pre-parse-match {yes | no}
        }
     log
        {
        counter <value> |
        feature |
            {
            all |
            appid {agt | all | basic | dfa | policy} |
            cfg {agent | all | basic | config} |
            ctd {all | basic | detector | sml | url} |
            flow {ager | all | arp | basic | ha | nd | np | receive} |
            misc {all | misc} |
            module {aho | all | dfa | scan | url} |
            pow {all | basic} |
            proxy {all | basic} |
            ssl {all | basic} |
            tcp {all | fptcp | reass} |
            tunnel {ager | flow} |
            url_trie {all | basic | stat} |
            zip {all | basic}
            }
        log-option throttle {no | yes} |
        off |
        on
        }
     }
  show setting
  }
pool |
  {
  check {hardware <value> | software <value>} |
  mem file <file_name> size <value> start <value> {mode <value>} |
  statistics
  }
pow |
  {
  performance {all} |
  status
  }
process {comm | ha-agent | mprelay | task} {on | off | show} |
reset |
  {
  appid {cache | statistics | unknown-cache {destination <ip_address>}} |
  ctd {regex-stats | url-block-cache {lockout}} |
  dos |
     {
     block-table |
     classification-table |
     rule <name> classification-table |
     zone <name> block-table {all | source <ip_address>}
     }
  logging |
  pow |
  ssl-decrypt
     {
     certificate-cache |
     certificate-status |
     exclude-cache |
     host-certificate-cache |
     notify-cache {source <ip_address>}
     }
  username-cache
  }
show |
  {
  cfg-memstat statistics |
  com statistics |
  ctd |
     {
     aggregate-table |
     athreat {tid <value>} |
     driveby-table |
     pcap-cache |
     regex-group {dump} |
     regex-stats {dump} |
     sml-cache |
     threat cid <value> id <value> |
     version
     }
  dos |
     {
     block-table |
     classification-table |
     rule <name> classification-table |
     zone <name> block-table
     }
  url-cache statistics |
  username-cache
  }
task-heartbeat {off| on | show} |
tcp state |
test
  {
  nat-policy-add |
     {
     destination <ip_address> |
     destination-port <port_number> |
     from <zone> |
     protocol <value> |
     source <ip_address> |
     source-port <port_number> |
     to <zone>
     }
  nat-policy-del |
     {
     destination <ip_address> |
     destination-port <port_number> |
     from <zone> |
     protocol <value> |
     source <ip_address> |
     source-port <port_number> |
     to <zone> |
     translate-source <ip_address> |
     translate-source-port <port_number>
     }
  url-cache-resolve-path {max-per-sec <value>
  url-resolve-path <value> |
  }
}
```

Options

> device — Debugs data plane hardware component
  > fdb — Debugs fdb (option to dump or provide index, 0-65535)
  > port-based-vlan — Debugs port-based VLAN port (0-32)
  > register — Debugs register read (0-4294967295)
  > uplink — Debugs uplink
  > vlan-table — Debugs VLAN table (option to dump or provide index, 0-4095)
> flow-control — Enables or disables flow control
> fpga — Debugs the field programmable gate array (FPGA) content
  > set — Sets the runtime flag (option to use only software for aho, dfa, or dlp)
  > state — Shows the FPGA state
> internal — Debugs data plane internal state
  > fpp statistics— Shows FPP state
  > path — Shows sample and display debugging counters along a path
    > nodes — Show the nodes available on this system
    > sample — Sample counters along a path
      + filter   Counter filter setting
      + show-zero   Enable display of empty counters
      * nodes   List of nodes describing a path to sample, like: "s1.p1 s1.dp0"
  > pdt — Internal diagnostic tool
    > lion — Options are egr, igr, mac, and spi
    > fe20 — Options are acl, flow, lagmap, lif, mac, mymac, nexthop, port, qmap, rd, route, show, spaui, sram, stats, xaui, xge, xge20g
    > fpp — Options are event, gft, predict, show, sw, vsys, xaui, xge
    > jaguar — Options are cip, rd, show, xaui, xge
    > marvell — Options are portmap, porttag, stats
    > nac — Options are aho dump, dfa dump, info, and stats

```
        > oct — Options are bootmem, csr, fpa, pip, pko, and pow
        > petra — Options are counter, lport, show
        > se20 — Options are aurora, show, sram, stats, xaui, xge
    > vif — Shows virtual interface configuration (address, link, route, rule, or vr)
> memory — Examines data plane memory
> monitor — Debugs data plane monitor details (off, on, or show current debug setting)
> nat — Debugs the specified Network Address Translation (NAT) sync IP pool rule
> packet-diag — Performs packet captures and configures pcap filter and trigger criterion
    > clear — Clears packet-related diagnosis parameters
        > all — Clears all settings and turns off log/capture
        > capture — Clears capture setting
            > all — All settings
            > snaplen — Packet capture snap length
            > stage — Capture at processing stage (drop, firewall, receive, or transmit)
            > trigger — Capture triggered by event
        > filter — Clears packet filter (all or specified filter index, 1-4)
        > log — Clears log setting
            > counter — Disables logging for global counter changes (all or specified counter value)
            > feature — Disables feature/module to log
                > all — Disables all
                > appid — Disables appid logging (agt, all, basic, dfa, or policy)
                > cfg — Disables cfg logging (agent, all, basic, or config)
                > ctd — Disables ctd logging (all, basic, detector, sml, or url)
                > flow — Disables flow logging (ager, all, arp, basic, ha, nd, np, or receive)
                > misc — Disables misc logging (all or miscellaneous)
                > module — Disables module logging (aho, all, dfa, scan, or url)
                > pow — Disables pow logging (all or basic)
                > proxy — Disables proxy logging (all or basic)
                > ssl — Disables SSL logging (all or basic)
                > tcp — Disables TCP logging (all, fptcp, or reass)
                > tunnel — Disables tunnel logging (ager or flow)
                > zip — Disables zip logging (all or basic)
            > log — Clears debug logs
    > set — Sets packet-related debugging parameters
        > capture — Debugs capture setting
            > off — Disables debug capture
            > on — Enables debug capture
            > snaplen — Packet capture snap length (40-65535)
            > stage — Packet capture at processing stage (drop, firewall, receive, or transmit)
                + byte-count — Maximum byte count before filter stops (1-1073741824)
                + packet-count — Maximum packet count before filter stops (1-1073741824)
                * file — Saved file name (alphanumeric string [ 0-9a-zA-Z._-])
            > trigger — Packet capture triggered by event
                + byte-count — Maximum byte count before filter stops (1-1073741824)
                + packet-count — Maximum packet count before filter stops (1-1073741824)
                * file — Saved file name (alphanumeric string [ 0-9a-zA-Z._-])
                * from — From application (enter an application name or press <tab> to view a list)
                * to — To application (enter an application name or press <tab> to view a list)
        > filter — Debugs filter setting
            > index — Modifies debug filter with specified index (1-4)
            > match — Adds a new debug filter and specifies matching options
                + destination — Destination IP address (x.x.x.x or IPv6)
                + destination-port — Destination port (1-65535)
                + ingress-interface — Ingress hardware interface name
        + ipv6-only — IPv6 packet only (no or yes)
        + non-ip — Non-IP packet
          exclude — Exclude non-IP packet
          include — Include non-IP packet
          only — Non-IP packet only
        + protocol — IP protocol value (1-255)
        + source — Source IP address (x.x.x.x or IPv6)
        + source-port — Source port (1-65535)
      > off — Disables debug filter
      > on — Enables debug filter
      > pre-parse-match — Matches value for packet before parsing (no or yes)
    > log — Debugs log setting
      > counter — Enables logging for global counter changes (enter a value or press <tab> to view a list)
      > feature — Enables feature/module to log
        > all — Enables all
        > appid — Enables appid logging (agt, all, basic, dfa, or policy)
        > cfg — Enables cfg logging (agent, all, basic, or config)
        > ctd — Enables ctd logging (all, basic, detector, sml, or url)
        > flow — Enables flow logging (ager, all, arp, basic, ha, nd, np, or receive)
        > misc — Enables misc logging (all or miscellaneous)
        > module — Enables module logging (aho, all, dfa, scan, or url)
        > pow — Enables pow logging (all or basic)
        > proxy — Enables proxy logging (all or basic)
        > ssl — Enables SSL logging (all or basic)
        > tcp — Enables TCP logging (all, fptcp, or reass)
        > tunnel — Enables tunnel logging (ager or flow)
        > url_trie — Enables URL logging (all, basic, or stat)
        > zip — Enables zip logging (all or basic)
      > log-option — Logging output options
        > throttle — Enables log throttling to minimize performance impact (no or yes)
      > off — Disables debug logging
      > on — Enables debug logging
  > show — Shows packet-related diagnosis information
> pool — Debugs buffer pools, including checks of hardware and software utilization and buffer pool statistics
  > check — Checks buffer pools utilization
    > hardware — Checks hardware-managed pools utilization (0-255)
    > software — Checks software-managed pools utilization (0-255)
  > mem — Dumps memory to a file
    + mode — Specify file mode e.g, (w, a)
    * file — Specify file name
    * size — Specify memory size (1-2147483648)
    * start — Specify start address, in hex format
  > statistics — Shows buffer pools statistics
> pow — Debugs the packet scheduling engine
  > performance — Shows performance
  > status — Displays packet scheduling engine status
> process — Debugs specified data plane process
  > comm — Debugs pan_comm process (off, on, or show)
  > ha-agent — Debugs dataplane high-availability agent (off, on, or show)
  > mprelay — Debugs management plane relay agent (off, on, or show)
  > task — Debugs packet processing tasks (off, on, or show)
> reset — Resets the settings for debugging the data plane
  > appid — Clears appid unknown cache
    > cache — cache
```

```
        > statistics — statistics
        > unknown-cache — Clears all unknown cache in dataplane
            + destination — destination IP address (x.x.x.x/y or IPv6/netmask)
    > ctd — Clears ctd setting
        > regex-stats — Clears regular expression statistics
        > url-block-cache — Clears URL block cache
            + lockout — URL block cache lockout
    > dos — Resets DoS protection dataplane information
        > block-table — Resets whole block table
        > classification-table — Resets whole classification table
        > rule — DoS protection rule name
        > zone — Source zone name
            > all — Clears all IPs
            > source — Specify Source IP(s) to unblock (x.x.x.x/y or IPv6/netmask)
    > logging — Resets data plane logging settings
    > pow — Resets pow performance stats
    > ssl-decrypt — Clears ssl-decrypt certificate cache
        > certificate-cache — Clears all ssl-decrypt certificate cache in dataplane
        > certificate-status — Clears all ssl-decrypt certificate CRL status cached in dataplane
        > exclude-cache — Clears all exclude cache in dataplane
        > host-certificate-cache — Clears all SSL certificates stored in host
        > notify-cache — Clears all ssl-decrypt notify-user cache in dataplane
            + source — Source IP address (x.x.x.x/y or IPv6/netmask)
    > username-cache — Clears DP user ID to name cache
> show — Shows data plane running information
    > cfg-memstat — Shows DP config memory statistics
    > com — Shows debug COM message
    > ctd — Shows debug CTD information
        > aggregate-table — Shows aggregate table
        > athreat — Shows active threats stat
            + tid — Shows tid mask stat (0-0x0fffffff)
        > driveby-table — Shows drive by table
        > pcap-cache — Shows PCAP cache table
        > regex-group — Shows regular expression group information
            + dump — Option to save the output for exporting
        > regex-stats — Shows regular expression statistics
            + dump — Option to save the output for exporting
        > sml-cache — Shows sml cache table
        > threat — Shows threat db
            * cid — Shows details for condition id (0-1024)
            * id — Shows threat id (0-0x0fffffff)
        > version — Shows ctd content version
    > dos — Shows DoS protection dataplane information
            > block-table — Shows whole block table
            > classification-table — Shows whole classification table
            > rule — DoS protection rule name
            > zone — Source zone name
    > url-cache — Shows url-cache statistics
    > username-cache — Shows DP user ID to name cache
> task-heartbeat — Debugs data plane task heartbeat (off, on, or show)
> tcp — Examines the TCP state of the data plane
> test — Uses test cases to verify system settings
    > nat-policy-add — Tests NAT policy translate
        + destination — Destination IP address (x.x.x.x or IPv6)
```

+ destination-port — Destination port (1-65535)
+ from — From zone
+ protocol — IP protocol value (1-255)
+ source — Source IP address (x.x.x.x or IPv6)
+ source-port — Source port (1-65535)
+ to — To zone

> nat-policy-del — Tests NAT policy delete

+ destination — Destination IP address (x.x.x.x or IPv6)
+ destination-port — Destination port (1-65535)
+ from — From zone
+ protocol — IP protocol value (1-255)
+ source — Source IP address (x.x.x.x or IPv6)
+ source-port — Source port (1-65535)
+ to — To zone
+ translate-source — Translated source IP address (x.x.x.x or IPv6)
+ translate-source-port — Translated source port (1-65535)

> url-cache-resolve-path — Tests the URL resolution process triggered by a DP for list of URLs

+ max-per-sec — maximum per second (1-65535)

> url-resolve-path — Tests the URL resolution process triggered by a dataplane thread

Sample Output

The following command shows the statistics for the data plane buffer pools.

```
admin@PA-HDF> debug dataplane pool statistics

Hardware Pools
[ 0] Packet Buffers           :    57241/57344    0x8000000410000000
[ 1] Work Queue Entries       :   229284/229376   0x8000000417000000
[ 2] Output Buffers           :     1000/1024     0x8000000418c00000
[ 3] DFA Result               :     2048/2048     0x8000000419100000
     DFA Result               :
[ 4] Timer Buffers            :     4092/4096     0x8000000418d00000
     Timer Buffers            :
[ 5] PAN_FPA_LWM_POOL         :     8192/8192     0x8000000419300000
[ 6] PAN_FPA_ZIP_POOL         :     1024/1024     0x8000000419500000
[ 7] PAN_FPA_BLAST_POOL       :       64/64       0x8000000419700000

Software Pools
[ 0] software packet buffer 0  :    16352/16384    0x8000000021b40680
[ 1] software packet buffer 1  :     8192/8192     0x8000000022354780
[ 2] software packet buffer 2  :     8191/8192     0x8000000022b5e880
[ 3] software packet buffer 3  :     4191/4192     0x8000000023b68980
[ 4] software packet buffer 4  :      256/256      0x800000002c079c00
[ 5] Pktlog logs               :    10000/10000    0x800000002d0a74e0
[ 6] Pktlog threats            :     4999/5000     0x800000002d2c2ea0
[ 7] Pktlog packet             :     5000/5000     0x800000002d3d0c00
[ 8] Pktlog large              :       56/56       0x800000002dc626a0
[ 9] CTD Flow                  :   261712/262144   0x80000000412e3080
[10] CTD AV Block              :       32/32       0x8000000058ef02e8
[11] SML VM Fields             :   261695/262144   0x8000000058ef8468
[12] SML VM Vchecks            :    65536/65536    0x8000000059838568
[13] Detector Threats          :   261699/262144   0x8000000059988668
[14] CTD DLP FLOW              :    65532/65536    0x800000005adf24d0
[15] CTD DLP DATA              :     4096/4096     0x800000005b6425d0
[16] CTD DECODE FILTER         :    16380/16384    0x800000005ba476d8
```

```
[17] Regex Results             :     2048/2048     0x800000005bafc088
[18] TIMER Chunk               :   131072/131072   0x8000000063f3a7c0
[19] FPTCP segs                :    32768/32768    0x8000000065fda8c0
[20] Proxy session             :     1024/1024     0x80000000660829c0
[21] SSL Handshake State       :     1024/1024     0x80000000660d9ec0
[22] SSL State                 :     2048/2048     0x80000000662773c0
[23] SSH Handshake State       :       64/64       0x80000000662edcc0
[24] SSH State                 :      512/512      0x800000006633b8c0

Software Packet Buffer Usage Stats
AskSize      UseSize      AllocSize    MaxRawPerc   MaxPerc
2295         9207         9472         53           100
0            0            0            99           100
1396         1612         1832         99           100
33064        33064        33064        100          100
0            0            0            0            0
```

The following command displays the settings for data plane packet diagnostics.

```
admin@PA-HDF> debug dataplane packet-diag show setting

-----------------------------------------------------------------------
Packet diagnosis setting:
-----------------------------------------------------------------------
Packet filter
  Enabled:                   no
  Match pre-parsed packet:   no
-----------------------------------------------------------------------
Logging
  Enabled:                   no
  Log-throttle:              no
  Output file size:          3306 of 10485760 Bytes
  Features:
  Counters:
-----------------------------------------------------------------------
Packet capture
  Enabled:                   no
-----------------------------------------------------------------------
```

The following example sets up a packet capture session. ***Note***: *For detailed technotes, search the Palo Alto Networks support site at https://live.paloaltonetworks.com/community/knowledgepoint.*

1. Create a filter to limit the amount of data that the packet capture will collect. In this configuration, only traffic for sessions sourced from IP 10.16.0.33 will be captured.

```
admin@PA-HDF> debug dataplane packet-diag set filter match source 10.16.0.33
```

2. Enable the filter.

```
admin@PA-HDF> debug dataplane packet-diag set filter on
```

3. Create a capture trigger that will begin capturing the pcap when an App-ID changes from web-browsing to gmail.

```
admin@PA-HDF> debug dataplane packet-diag set capture trigger application
    from web-browsing to gmail-base file gmailpcap
```

4. Enable the capture.

```
admin@PA-HDF> debug dataplane packet-diag set capture on
```

5. Verify that the packet capture collected data.

```
admin@PA-HDF> debug dataplane packet-diag show setting
```

6. After the capture is complete, disable it to prevent performance degradation due to filtering and PCAP.

```
admin@PA-HDF> debug dataplane packet-diag set filter off
admin@PA-HDF> debug dataplane packet-diag set capture off
```

7. View the packet capture on the firewall.

```
admin@PA-HDF> view-pcap filter-pcap gmailpcap
```

Or, export the packet capture for viewing on another machine.

```
admin@PA-HDF> scp export filter-pcap from gmailpcap to account@10.0.0.1:/
```

Required Privilege Level

superuser vsysadmin

debug device-server

Configures settings for debugging the device server.

Syntax

```
debug device-server
   {
   bc-url-db |
     {
     bloom-stats |
     bloom-verify-basedb |
     cache-clear |
     cache-enable {no | yes} |
     cache-load |
     cache-resize <value> |
     cache-save |
     db-info |
     show-stats
     }
   clear |
   dump |
     {
     com {all | opcmd | sshkey | status | url} |
     dynamic-url |
        {
        database {category <value> | start-from <value>} |
        statistics
        }
     idmgr |
        {
        high-availability state |
        type
           {
           custom-url-filter {all | id <value> | name <name>} |
           global-interface {all | id <value> | name <name>} |
           global-rib-instance {all | id <value> | name <name>} |
           global-tunnel {all | id <value> | name <name>} |
           global-vlan {all | id <value> | name <name>} |
           global-vlan-domain {all | id <value> | name <name>} |
           global-vrouter {all | id <value> | name <name>} |
           ike-gateway {all | id <value> | name <name>} |
           nat-rule {all | id <value> | name <name>} |
           pbf-rule {all | id <value> | name <name>} |
           security-rule {all | id <value> | name <name>} |
           shared-application {all | id <value> | name <name>} |
           shared-custom-url-category {all | id <value> | name <name>} |
           shared-gateway {all | id <value> | name <name>} |
           shared-region {all | id <value> | name <name>} |
           ssl-rule {all | id <value> | name <name>} |
           vsys {all | id <value> | name <name>} |
           vsys-application {all | id <value> | name <name>} |
           vsys-custom-url-category {all | id <value> | name <name>} |
           vsys-region {all | id <value> | name <name>} |
           zone {all | id <value> | name <name>}
           }
        }
     logging statistics |
     memory {detail | summary} |
     pan-url-db statistics
     regips {ip <ip/netmask> | summary | tag <value>} |
     tag-table tag <value>
     }
  off |
  on |
  pan-url-db |
     {
     cloud-reelect |
     cloud-static-list-disable |
     cloud-static-list-enable <value> |
     db-backup back-duration <value> back-threshold <value> |
     db-info |
     db-perf |
     show-stats
     }
  reset |
     {
     brightcloud-database |
     com statistics |
     config |
     id-manager type |
        {
        all |
        global-interface |
        global-rib-instance |
        global-tunnel |
        global-vlan |
        global-vlan-domain |
        global-vrouter |
        ikey-gateway |
        nat-rule |
        pbf-rule |
        security-rule |
        shared-application |
        shared-custom-url-category |
        shared-gateway |
        shared-region |
        ssl-rule |
        vsys |
        vsys-application |
        vsys-custom-url-category |
        vsys-region |
        zone
        }
     logging statistics |
     url {dynamic-url-size <value> | dynamic-url-timeout <value>}
```

```
          }
        save dynamic-url-database |
        set |
          {
          all |
          base {all | config | ha | id} |
          config {all | basic | fpga | tdb} |
          misc {all | basic} |
          tdb {aho | all | basic} |
          third-party {all | libcurl} |
          url {all | basic | cloud | ha | match | rfs | stat} |
          url_trie {all | basic | stat}
          }
        show |
        test |
          {
          admin-override-password <value> |
          botnet-domain |
          dynamic-url {async | cloud | unknown-only} {no | yes} |
          url-category <value> |
          url-update-server
          }
        unset
          {
          all |
          base {all | config | ha | id} |
          config {all | basic | fpga | tdb} |
          misc {all | basic} |
          tdb {aho | all | basic} |
          third-party {all | libcurl} |
          url {all | basic}
          }
        }
```

Options

> bc-url-db — Debugs BrightCloud URL database (for BrightCloud only)
  > bloom-stats — Shows bloom filter stats
  > bloom-verify-basedb — Verifies base database with bloom filter
  > cache-clear — Clears database access cache
  > cache-enable — Enables/disables cache for database access
  > cache-load — Loads database access cache
  > cache-resize — Resizes database cache (1-1000000)
  > cache-save — Saves database access cache
  > db-info — Shows database info
  > show-stats — Shows URL database access statistics
> clear — Clears all debug logs
> dump — Dumps the debug data
  > com — Dumps com messages statistics
    > all — Dumps all messages statistics
    > opcmd — Dumps opcmd messages statistics
    > sshkey — Dumps SSH key messages statistics
    > status — Dumps status messages statistics
    > url — Dumps URL messages statistics

```
        > dynamic-url — Dumps dynamic URLs
            > database — Dumps dynamic url db (for BrightCloud only)
                + category — Dumps only the URL category (press <tab> for a list of categories)
                + start-from — Dumps dynamic URL database starting from index (1-1000000)
            > statistics — Dumps URL categorization statistics
        > idmgr — Dumps ID manager data
            > high-availability — Dumps high availability state
            > type — Dumps specific type
                > custom-url-filter — Dumps only custom URL filter name and ID
                > global-interface — Dumps only global interface name and ID
                > global-rib-instance — Dumps only global RIB instance name and ID
                > global-tunnel — Dumps only global tunnel name and ID
                > global-vlan — Dumps only global VLAN name and ID
                > global-vlan-domain — Dumps only global VLAN domain name and ID
                > global-vrouter — Dumps only global virtual router name and ID
                > ike-gateway — Dumps only IKE gateway name and ID
                > nat-rule — Dumps only NAT rule name and ID
                > pbf-rule — Dumps only PBF rule name and ID
                > security-rule — Dumps only security rule name and ID
                > shared-application — Dumps only shared application name and ID
                > shared-custom-url-category — Dumps only shared custom URL category name and ID
                > shared-gateway — Dumps only shared gateway
                > shared-region — Dumps only shared region code name and ID
                > ssl-rule — Dumps only SSL rule name and ID
                > vsys — Dumps only virtual system name and ID
                > vsys-application — Dumps only virtual system application name and ID
                > vsys-custom-url-category — Dumps only virtual system custom URL category name and ID
                > vsys-region — Dumps only virtual system region code name and ID
                > zone — Dumps only zone name and ID
        > logging — Dumps logging statistics
        > memory — Dumps memory statistics (detail or summary)
        > pan-url-db — Dumps Palo Alto Networks URL filtering database statistics
        > regips— Dumps registered IP information (specify ip/netmask, summary, or tag with value)
        > tag-table— Dumps tag table
    > off — Turns off debug logging
    > on — Turns on debug logging
    > pan-url-db — Debugs the PAN URL filtering database (for the Palo Alto Networks URL filtering database only)
        > cloud-reelect — Reelects the current PAN URL cloud
        > cloud-static-list-disable — Disables the PAN static cloud list
        > cloud-static-list-enable — Enables the specified PAN cloud list(s) (separated by commas)
        > db-backup — Debugs URL database backup
            * back-duration — URL database backup duration, in minutes (5-480)
            * back-threshold — URL database backup threshold, in minutes (3-30)
        > db-info — Displays PAN database information
        > db-perf — Displays PAN host performance information
        > show-stats — Displays PAN URL database access statistics
    > reset — Clears logging data
        > brightcloud-database — Deletes the BrightCloud database to allow a fresh restart
        > com — Clears com messages statistics
        > config — Clears the last configuration object
        > id-manager — Clears the specified ID manager cache file
            > all — Resets all types
            > global-interface — Resets the global interfaces IDs
            > global-rib-instance — Resets global RIB instances IDs
            > global-tunnel — Resets global tunnels IDs
            > global-vlan — Resets global VLAN IDs
            > global-vlan-domain — Resets global VLAN domains IDs
            > global-vrouter — Resets global virtual routers IDs
            > ike-gateway — Resets IKE gateways IDs
            > nat-rule — Resets NAT rules IDs
            > pbf-rule — Resets PBF rules IDs
            > security-rule — Resets security rules IDs
            > shared-application — Resets shared applications IDs
            > shared-custom-url-category — Resets shared custom URL categories IDs
            > shared-gateway — Resets shared gateways IDs
            > shared-region — Resets shared regions IDs
            > ssl-rule — Resets SSL rules IDs
            > vsys — Resets virtual systems IDs
            > vsys-application — Resets virtual system applications IDs
            > vsys-custom-url-category — Resets virtual system custom URL categories IDs
            > vsys-region — Resets virtual system regions IDs
            > zone — Resets zones IDs
        > logging — Clears logging statistics
        > url — Resets URL (for BrightCloud only)
            > dynamic-url-size — Sets dynamic URL maximum entry count (10-1000000)
            > dynamic-url-timeout — Sets dynamic URL entry timeout in minutes (1-43200)
    > save — Saves the dynamic URL database (for BrightCloud only)
    > set — Sets debugging values
        > all — Sets all debugging values
        > base — Sets base debugging values (all, config, ha, id)
        > config — Sets configuration debugging values (all, basic, fpga, tdb)
        > misc — Sets miscellaneous debugging values (all, basic)
        > tdb — Sets tdb debugging values (aho, all, basic)
        > third-party — Sets third party debugging values (all, libcurl)
        > url — Sets URL debugging values (all, basic, cloud (for the PAN URL filtering database only), ha, match,
            rfs, stat)
        > url_trie — Sets URL trie debugging values (all, basic, stat)
    > show — Displays current debug log settings
    > test — Tests the current settings
        > admin-override-password — Tests URL admin override password
        > botnet-domain — Tests batch botnet domain categorization
        > dynamic-url — Tests batch dynamic URL categorization
            + async — Run test asynchronously or not
            + cloud — Send to cloud or not
            + unknown-only — Only output URL if category is unknown
        > url-category — Gets URL categorization from code (1-16383)
        > url-update-server — Tests URL database server connectivity
    > unset — Removes current settings
        > all — Removes all current settings
        > base — Removes current base settings (all, config, ha, id)
        > config — Removes current config settings (all, basic, fpga, tdb)
        > misc — Removes current misc settings (all, basic)
        > tdb — Removes current tdb settings (aho, all, basic)
        > third-party — Removes current third party settings (all, libcurl)
        > url — Removes current URL settings (all, basic)
```

Sample Output

The following command turns off debug logging for the device server.

```
admin@PA-HDF> debug device-server off
admin@PA-HDF>
```

Required Privilege Level

superuser vsysadmin

debug dhcpd

Configures settings for debugging the Dynamic Host Configuration Protocol (DHCP) daemon.

Syntax

```
debug dhcpd
   {
   global {on | off | show} |
   pcap {delete | on | off | show | view} |
   show objects
   }
```

Options

> global — Defines settings for the global DHCP daemon
> pcap — Defines settings for debugging packet capture
> show — Displays DHCP client debug information

Sample Output

The following command displays current global DHCP daemon settings.

```
admin@PA-HDF> debug dhcpd global show

sw.dhcpd.runtime.debug.level: debug

admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug dnsproxyd

Configures settings for the Domain Name Server (DNS) proxy daemon.

Syntax

```
debug dnsproxyd
   {
   global {off | on | show} |
   show {batches | connections | objects | persistent}
   }
```

Options

> global — Controls debug levels
> show — Shows DNS proxy debug information
    \> batches — Displays DNS proxy batch requests
    \> connections — Displays DNS proxy connections
    \> objects — Displays DNS proxy object debug
    \> persistent — Displays DNS proxy persistent cache entries on disk

Sample Output

The following command displays the DNS proxy object debug.

```
admin@PA-HDF> debug dnsproxyd show objects

--------------CFG OBJS---------------
CFG obj name: mgmt-obj (0x1039ff74)

--------------RT OBJS---------------
RT obj name: mgmt-obj (0x1020ae28)
  obj addr:0x1020ae28
  def_name_servers:0x1037a384

  tom:0x101b08e4
  dnscache:0x101b09e4

  Interface:mgmt-if
    10.1.7.16

-------IP OBJ HASH TBL--------------
  ip: 10.1.7.16 for dns rt obj:mgmt-obj


admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug global-protect

Configures settings for debugging the GlobalProtect portal.

Syntax

```
debug global-protect portal {interval <value> | off | on}
```

Options

> interval — Interval to send HIP report (60-86400)
> off — Turn off debugging
> on — Turn on debugging

Sample Output

The following command turns on GlobalProtect debugging.

```
admin@PA-HDF> debug global-protect portal on

admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug high-availability-agent

Configures settings for debugging the high availability agent.

Syntax

```
debug high-availability-agent
   {
   internal-dump |
   off |
   on |
   show
   }
```

Options

> internal-dump — Dumps the internal state of the agent to its log
> off — Turns the debugging option off
> on — Turns the debugging option on
> show — Displays current debug logging setting

Required Privilege Level

superuser, vsysadmin

debug ike

Configures settings for debugging Internet Key Exchange (IKE) daemon.

Syntax

```
debug ike
   {
   global {off | on | show} |
   pcap {delete | off | on | show | view} |
   socket |
   stat
   }
```

Options

> global — Configures global settings
> pcap — Configures packet capture settings
> socket — Configures socket settings
> stat — Shows IKE daemon statistics

Sample Output

The following command turns on the global options for debugging the IKE daemon.

```
admin@PA-HDF> debug ike global on
admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug keymgr

Configures settings for debugging the key manager daemon.

Syntax

```
debug keymgr
   {
   list-sa |
   off |
   on |
   show
   }
```

Options

> list-sa — Lists the IPSec security associations (SAs) that are stored in the key manager daemon
> off — Turns the settings off
> on — Turns the settings on
> show — Shows key manager daemon information

Sample Output

The following command shows the current information on the key manager daemon.

```
admin@PA-HDF> debug keymgr show

sw.keymgr.debug.global: normal

admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug l3svc

Configures settings for debugging the Layer 3 Switched Virtual Connection (L3SVC).

Syntax

```
debug l3svc
   {
   clear |
   off |
   on {debug | dump | error | info | warn} |
   pcap {delete | off | on | show | view} |
   reset user-cache {all | <value>} |
   show user-cache
   }
```

Options

> clear — Clears the debug logs
> off — Turns the debugging option off
> on — Turns the debugging option on
> pcap — Configures packet capture settings
> reset — Resets the user cache
> show — Displays the user cache

Sample Output

The following command turns on L3SVC debugging.

```
admin@PA-HDF> debug l3svc on debug

admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug log-card-interface

Shows log-card networking interface information.

Syntax

```
debug log-card-interface
   {
   info slot <value> |
   ping host <value> slot <value> |
   }
```

Options

> info— Show log card networking interface information.
> ping — Perform ping operation from the log card interface

Required Privilege Level

superuser, vsysadmin

debug log-collector-group

Configures settings for debugging log collector groups.

Syntax

```
debug log-collector-group show
   {
   local {no | yes} |
   name <value> |
   segment <value>
   }
```

Options

+ local — Show local ring (yes/no)
+ name — Log collector group name
+ segment — Show segment ID (0-1000000)

Required Privilege Level

superuser, vsysadmin

debug log-receiver

Configures settings for debugging the log receiver daemon.

Syntax

```
debug log-receiver
   {
   container-page {entries <value> | off | on | timeout <value>} |
   fwd {off | on | show} |
   netflow {clear | statistics}
   off |
   on {debug | dump | normal} |
   show |
   statistics |
   }
```

Options

> container-page — Configures container page usage
>   > entries — Specifies cache entries (4-65536)
>   > off — Turns off container page caching
>   > on — Turns on container page caching
>   > timeout — Specifies cache timeout (1-86400)
> fwd — Configures forwarding
>   > off — Turns off forwarding
>   > on — Turns on forwarding
>   > show — Shows whether this command is on or off
> netflow — NetFlow log receiver clear and show statistics commands
> off — Turns the debugging option off
> on — Turns the debugging option on (option to select debug, dump, or normal)
> show — Shows whether this command is on or off
> statistics — Shows log receiver daemon statistics

Sample Output

The following command turns log receiver debugging on.

```
admin@PA-HDF> debug log-receiver on
admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug logview

Shows log-card networking interface information.

Syntax

```
debug log-card-interface
   {
   component <value> |
   display-forward {no | yes} |
   end-time <value> |
   max-logs <value> |
   quiet {no | yes} |
   role <value> |
   severity <value> |
   slot <value> |
   start-time <value> |
   thorough {no | yes} |
   }
```

Options

+ component — For multiple components specify with comma separated. ex: dagger,sysd
+ display-forward — default display is reverse
+ end-time — Datetime YYYY/MM/DD@hh:mm:ss (e.g. 2013/03/02@10:00:00)
+ max-logs — Number of logs to display min 100 and max 20000. Default 2000
+ quiet — Quiet mode: Just print log count default is false
+ role — For multiple roles specify with comma separated. ex: mp,cp,dp
+ severity — For multiple severities specify with comma separated. ex: error,info
+ slot — For multiple slots specify with comma separated. ex: 1,2
+ start-time — Datetime YYYY/MM/DD@hh:mm:ss (e.g. 2013/03/01@10:00:00)
+ thorough — Perform thorough search default is quick mode

Required Privilege Level

superuser, vsysadmin

debug management-server

Configures settings for debugging the management server.

Syntax

```
debug management-server

    clear |
    client {disable <value> | enable <value>} |
    conn |
    db-intervals db {dailythsum | dailytrsum | hourlythsum | hourlytrsum |
      thsum | trsum | weeklythsum | weeklytrsum} |
      {
      end-time <value> |
      period {last-12-hours | last-24-hrs | last-30-days | last-7-calendar-
         days | last-7-days | last-calendar-day | last-calendar-month | last-
         calendar-week | last-hour} |
      start-time <value>
      }
    db-rollup {off | on} |
    inter-log-collector status |
    off |
    on {debug | dump | error | info | warn} |
    rolledup-intervals db {thsum | trsum} |
      {
      end-time <value> |
      period {last-12-hours | last-24-hrs | last-30-days | last-7-calendar-
         days | last-7-days | last-calendar-day | last-calendar-month | last-
         calendar-week | last-hour} |
      start-time <value>
      }
    set |
      {
      all |
      auth {all | basic | detail} |
      cfg {all | basic | detail} |
      comm {all | basic | detail} |
      dynupdsch {all | basic | detail} |
      commit {all | basic | detail} |
      commoncriteria {all | basic | detail} |
      content {all | basic | detail} |
      fqdn {all | basic | detail} |
      log {all | basic | detail} |
      logaction {all | basic | detail} |
      logforwarding {all | basic | detail} |
      logquery {all | basic | detail} |
      panorama {all | basic | detail} |
      proxy {all | basic | detail} |
      report {all | basic | detail} |
      schema {all | basic | detail} |
      server {all | basic | detail} |
      settings {all | basic | detail}
      }
   show |
   template dump-config from {local | merged | template} {xpath <value>} |
   unset |
      {
      all |
      auth {all | basic | detail} |
      cfg {all | basic | detail} |
      comm {all | basic | detail} |
      commit {all | basic | detail} |
      commoncriteria {all | basic | detail} |
      content {all | basic | detail} |
      dynupdsch {all | basic | detail} |
      fqdn {all | basic | detail} |
      log {all | basic | detail} |
      logaction {all | basic | detail} |
      logforwarding {all | basic | detail} |
      logquery {all | basic | detail} |
      panorama {all | basic | detail} |
      proxy {all | basic | detail} |
      report {all | basic | detail} |
      schema {all | basic | detail} |
      server {all | basic | detail} |
      settings {all | basic | detail}
      }
   user info name <value>
   }
```

Options

> clear — Clears all debug logs
> client — Enables or disables management server client processes
authd — authd daemon
device — Device server
dhcpd — DHCP server
ha_agent — High-Availability server
ikemgr — IKE manager
l3svc — HTTP Daemon
ldapd — LDAP Daemon
logrcvr — Log Receiver daemon
npagent — Network Processor agent
pppoed — PPPoE daemon
rasmgr — Remote Access Daemon
routed — Routing daemon
sslmgr — sslmgr daemon
sslvpn — sslvpn daemon
> conn — Prints management server conn entries
> db-intervals — Displays available summary intervals for a given period
+ end-time — End Time, e.g. 2008/12/31 11:59:59
+ period — Select from available time periods
+ start-time — Start Time, e.g. 2008/01/01 09:00:00
* db — Database to display
> db-rollup — Enables or disables summary database roll up

```
> inter-log-collector — Management server log forwarding/collection
> off — Turns off debug logging
> on — Turns on management server debug logging
    debug — Only output error, warning, info and debug logs
    dump — Output all logs
    error — Only output error logs
    info — Only output error, warning and info logs
    warn — Only output error and warning logs
> rolledup-intervals — Displays summary intervals rolled up optimally into summary-based partial reports
    + end-time — End Time, e.g. 2008/12/31 11:59:59
    + period — Select from available time periods
    + start-time — Start Time, e.g. 2008/01/01 09:00:00
    * db — Database to display
> set — Turns on management server component debug logging
    > all — Debug logging for all components
    > auth — Auth debug logging (all, basic, detail)
    > cfg — CFG debug logging (all, basic, detail)
    > comm — Comm debug logging (all, basic, detail)
    > commit — Commit debug logging (all, basic, detail)
    > commoncriteria — Common Criteria debug logging (all, basic, detail)
    > content — Content debug logging (all, basic, detail)
    > dynupdsch — Debugging for dynamic update schedules
    > fqdn — FQDN debug logging (all, basic, detail)
    > log — Log debug logging (all, basic, detail)
    > logaction — Log action debug logging (all, basic, detail)
    > logforwarding — Log forwarding debug logging (all, basic, detail)
    > logquery — Log query debug logging (all, basic, detail)
    > panorama — Panorama debug logging (all, basic, detail)
    > proxy — Proxy debug logging (all, basic, detail)
    > report — Report debug logging (all, basic, detail)
    > schema — Schema debug logging (all, basic, detail)
    > server — Server debug logging (all, basic, detail)
    > settings — Settings debug logging (all, basic, detail)
> show — Displays current debug logging setting
> template — Helpers for debugging templates
    + xpath — XPath of part to be dumped
    * from — Dump from specified config tree
       - local — Dumps non-template part of local config
       - merged — Dumps the merged config
       - template — Dumps template part of the local config
> unset — Turns off management server component debug logging
    > all — Debug logging for all components
    > auth — Auth debug logging (all, basic, detail)
    > cfg — CFG debug logging (all, basic, detail)
    > comm — Comm debug logging (all, basic, detail)
    > commit — Commit debug logging (all, basic, detail)
    > commoncriteria — Common Criteria debug logging (all, basic, detail)
    > content — Content debug logging (all, basic, detail)
    > dynupdsch — Debugging for dynamic update schedules
    > fqdn — FQDN debug logging (all, basic, detail)
    > log — Log debug logging (all, basic, detail)
    > logaction — Log action debug logging (all, basic, detail)
    > logforwarding — Log forwarding debug logging (all, basic, detail)
    > logquery — Log query debug logging (all, basic, detail)
    > panorama — Panorama debug logging (all, basic, detail)
    > proxy — Proxy debug logging (all, basic, detail)
    > report — Report debug logging (all, basic, detail)
    > schema — Schema debug logging (all, basic, detail)
    > server — Server debug logging (all, basic, detail)
    > settings — Settings debug logging (all, basic, detail)
> user — Shows user name information
```

Sample Output

The following example turns management server debugging on.

```
admin@PA-HDF> debug management-server on
(null)
admin@PA-HDF>
```

The following example enables the management server network processor agent.

```
admin@PA-HDF> debug management-server client enable npagent

admin@PA-HDF>
```

The following example displays all of the available hourly summary intervals for the trsum database.

```
username@hostname> debug management-server db-intervals period last-calendar-
    day db hourlytrsum

hourlytrsum periods from 2011/06/15 00:00:00 to 2011/06/15 23:59:59

    hourlytrsum 2011/06/15 00:00:00 to 2011/06/15 11:59:59
    hourlytrsum 2011/06/15 13:00:00 to 2011/06/15 23:59:59
```

The following example displays the breakdown of the trsum report into summary-based partial reports.

```
username@hostname> debug management-server rolledup-intervals period last-7-
    days db trsum

Rolled up periods from 2011/02/17 14:03:38 to 2011/02/24 14:03:37

          trsum 2011/02/17 14:03:38 to 2011/02/19 23:59:59
     dailytrsum 2011/02/20 00:00:00 to 2011/02/23 23:59:59
    hourlytrsum 2011/02/24 00:00:00 to 2011/02/24 13:59:59
```

Required Privilege Level

superuser, vsysadmin

debug master-service

Configures settings for debugging the master service.

Syntax

```
debug master-service
    {
    internal-dump |
    off |
    on {debug | dump | error | info | warn} |
    show
    }
```

Options

> internal-dump — Dumps internal state of service to its log
> off — Turns off debug logging
> on — Turns on masterd service debug logging
    debug — Only output error, warning, info and debug logs
    dump — Output all logs
    error — Only output error logs
    info — Only output error, warning and info logs
    warn — Only output error and warning logs
> show — Displays current debug logging setting

Sample Output

The following command dumps the internal state of the master server to the log.

```
admin@PA-HDF> debug master-service internal-dump

admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug mprelay

Configures settings for debugging management plane relay.

Syntax

```
debug mpreplay
   {
   off |
   on {debug | dump | error | info | warn} |
   show
   }
```

Options

> off — Turns off debug logging
> on — Turns on debug logging
   debug — Only output error, warning, info and debug logs
   dump — Output all logs
   error — Only output error logs
   info — Only output error, warning and info logs
   warn — Only output error and warning logs
> show — Displays current debug logging setting

Required Privilege Level

superuser, vsysadmin

debug netconfig-agent

Defines settings for debugging the network configuration agent.

Syntax

```
debug netconfig-agent {off | on | show}
```

Options

> off — Turns off network configuration agent debugging
> on — Turns on network configuration agent debugging
> show — Displays current debug setting

Sample Output

The following command turns on debugging of the network configuration agent.

```
admin@PA-HDF> debug netconfig-agent on
admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug pppoed

Configures settings for debugging the Point-to-Point Protocol over Ethernet (PPPoE) daemon. The firewall can be configured to be a PPPoE termination point to support connectivity in a Digital Subscriber Line (DSL) environment where there is a DSL modem but no other PPPoE device to terminate the connection.

Syntax

```
debug pppoed
   {
   global {off | on | show} |
   pcap |
     {
     delete |
     off |
     on {virtualrouter <value>} |
     show |
     view
     }
   show interface {all | <interface_name>}
   }
```

Options

> global — Sets debugging options
> pcap — Performs packet capture (option to filter result by virtual router)
> show interface — Shows PPPoE debug information (all or specify an interface)

Sample Output

The following command turns packet capture debugging off.

```
admin@PA-HDF> debug pppoed pcap off
debug level set to error

admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug rasmgr

Configures settings for debugging the remote access service daemon.

Syntax

```
debug rasmgr
   {
   off |
   on {debug | dump | normal} |
   show |
   statistics {all | reset}
   }
```

Options

> off — Turns the debugging option off
> on — Turns the debugging option on (option to specify debug, dump, or normal)
> show — Shows whether this command is on or off
> statistics — Shows or resets statistics counters

Sample Output

The following command shows the debug settings for the remote access service daemon.

```
admin@PA-HDF> debug rasmgr show

sw.rasmgr.debug.global: normal

admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug routing

Configures settings for debugging the route daemon.

Syntax

```
debug routing
    {
    fib {flush | stats} |
    global {off | on | show} |
    ifmon |
    list-mib |
    mib <value> |
    mpf stats |
    pcap |
      {
      all {delete | off | on | view} |
      bgp {delete | off | on | view} |
      igmp {delete | off | on | view} |
      ospf {delete | off | on | view} |
      pim {delete | off | on | view} |
      rip {delete | off | on | view} |
      show
      }
    restart |
    socket
    }
```

Options

> fib — Turns on debugging for the forwarding table
>   > flush — Forces forwarding table sync
>   > stats — Shows route message stats

> global — Turns on global debugging

> ifmon — Shows interface monitor status

> list-mib — Shows the routing list with management information base (MIB) names

> mib — Shows the MIB tables

> mpf — Displays multicast packet forwarder statistics

> pcap — Shows packet capture data (all, BGP, OSPF, RIP)

> restart — Restarts the routing process

> socket — Shows socket data

Sample Output

The following command displays the MIB tables for routing.

```
admin@PA-HDF> debug routing list-mib

i3EmuTable (1 entries)
==========================
sckTable (0 entries)
sckSimInterfaceTable (0 entries)
```

```
sckEiTable (0 entries)
sckEaTable (0 entries)
i3Table (0 entries)
i3EiTable (0 entries)
i3EaTable (0 entries)
i3EtTable (0 entries)
i3EmTable (0 entries)
dcSMLocationTable (0 entries)
dcSMHMTestActionObjects (0 entries)
siNode (0 entries)
siOSFailures (0 entries)
siTraceControl (0 entries)
siExecAction (0 entries)
...
admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug satd

Configures settings for debugging the satellite daemon.

Syntax

```
debug satd
   {
   failed-refresh-timeout satellite gateway-refresh-time <value> name
     <value> portal-refresh-time <value>
   off |
   on {debug | dump | normal} |
   show |
   statistics {all |reset}
   }
```

Options

> failed-refresh-timeout — Sets GlobalProtect satellite configuration failed refresh timeout
   * gateway-refresh-time — Time in minutes (0-10)
   * name — GlobalProtect satellite name
   * portal-refresh-time — Time in minutes (0-10)

> off — Turns the debugging option off

> on — Turns the debugging option on (option to specify debug, dump, or normal)

> show — Shows whether this command is on or off

> statistics — Shows or resets statistics counters

Required Privilege Level

superuser, vsysadmin

debug software

Configures software processes debugging features.

Syntax

```
debug software
   {
   core {device-server | l3-service | log-receiver | management-server | pan-
     comm | rasmgr | routed | sslvpn-web-server | user-id | vardata-receiver
     | web-server} |
   fd-limit {limit <value> | service <value>} |
   no-fd-limit service <value> |
   no-virt-limit service <value> |t
   restart {device-server | l3-service | log-receiver | management-server |
     ntp | pan-comm | rasmgr | routed | snmpd | sslmgr | sslvpn-web-server |
     user-id | vardata-receiver | web-server} |
   trace {device-server | l3-service | log-receiver | management-server |
     sslvpn-web-server | user-id | vardata-receiver | web-server} |
   virt-limit {limit <value> | service <value>}
   }
```

Options

> core — Debugs process core
    > device-server — Device server process
    > l3-service — L3 services server process
    > log-receiver — Log Receiver server process
    > management-server — Management server process
    > pan-comm — Data plane communication process
    > rasmgr — SSL VPN daemon
    > routed — Routing process
    > sslvpn-web-server — SSL VPN Web server process
    > user-id — User ID process
    > vardata-receiver — Vardata Receiver server process
    > web-server — Web server process
> fd-limit — Sets open fd limit (0-4294967295) and service value
> no-fd-limit — Disables open fd limit service
> no-virt-limit — Disables maximum virtual memory limit service
> restart — Restarts processes
    > device-server — Device server process
    > l3-service — L3 services server process
    > log-receiver — Log Receiver server process
    > management-server — Management server process
    > ntp — Restart and re-synchronize NTP service
    > pan-comm — Data plane communication process
    > rasmgr — SSL VPN daemon
    > routed — Routing process
    > satd — Satellite daemon
    > snmpd — SNMP process
    > sslmgr — SSL manager daemon
    > sslvpn-web-server — SSL VPN Web server process

> user-id — User ID process
> vardata-receiver — Vardata Receiver server process
> web-server — Web server process
> trace — Gets process backtraces
> device-server — Device server process
> l3-service — L3 services server process
> log-receiver — Log Receiver server process
> management-server — Management server process
> sslvpn-web-server — SSL VPN Web server process
> user-id — User ID process
> vardata-receiver — Vardata Receiver server process
> web-server — Web server process
> virt-limit — Sets maximum virtual memory limit (0-4294967295) and service value

Sample Output

The following command restarts the web server.

```
admin@PA-HDF> debug software restart web-server

admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug ssl-vpn

Sets debugging options for the Secure Socket Layer (SSL)-virtual private network (VPN) web server.

Syntax

```
debug ssl-vpn
    {
    global |
       {
       off |
       on {debug | dump | error | info} |
       show
       }
    socket
    }
```

Options

> global — Turns debugging on or off at on the global level and shows debugging results (option to turn on debug, dump, error, or info)
> socket — Debugs on the socket level

Sample Output

The following command displays socket level information.

```
admin@PA-HDF> debug ssl-vpn socket

Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/
    Program name
tcp        0      0 0.0.0.0:20077               0.0.0.0:*                   LISTEN      1674/
    appweb
tcp        0      0 0.0.0.0:20088               0.0.0.0:*                   LISTEN      1674/
    appweb
admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug sslmgr

Sets debugging options for the Secure Socket Layer (SSL) manager daemon that validates certificates for the Certificate Revocation List (CRL) and the Online Certificate Status Protocol (OCSP). Each trusted certificate authority (CA) maintains CRLs to determine if an SSL certificate is valid (not revoked) for SSL decryption. The OCSP can also be used to dynamically check the revocation status of a certificate.

Syntax

```
debug sslmgr
   {
   delete {crl | ocsp} {all | <value>} |
   off |
   on {debug | dump | error | info | warn} |
   reset rsa-key |
   save oscp |
   set ocsp-next-update-time <value> |
   show {ocsp-next-update-time | setting} |
   statistics |
   tar-all-crl |
   view {crl <value> | ocsp {all | <value>}}
   }
```

Options

> delete — Removes the CRL/OCSP cache
   > crl — Delete CRL cache (all or specify CRL to delete)
   > ocsp — Delete OCSP cache (all or specify URL)
> off — Turns the manager daemon off
> on — Turns the manager daemon on (debug, dump, error, info, or warn)
> reset — Resets the SSL decrypt key
> save — Saves the contents of the OCSP cache
> set — Sets the OCSP next update time, in minutes (1-10080)
> show — Displays the SSL manager
   > ocsp-next-update-time — Shows the OCSP next update time
   > setting — Shows the debug setting
> statistics — Displays the CRL/OCSP statistics
> tar-all-crl — Saves all CRL files to a tar file
> view — Displays the CRL/OCSP cache
   > crl — View CRL cache
   > ocsp — View OCSP cache (all or specify URL)

Sample Output

The following command displays the CRL cache.

```
admin@PA-HDF> debug sslmgr view crl
http://EVIntl-crl.verisign.com/EVIntl2006.crl
 http://EVSecure-crl.verisign.com/EVSecure2006.crl
 http://EVSecure-crl.verisign.com/pca3-g5.crl
  http://SVRC3SecureSunMicrosystems-MPKI-crl.verisign.com/
```

```
    SunMicrosystemsIncClassBUnified/LatestCRLSrv.crl
 http://SVRIntl-crl.verisign.com/SVRIntl.crl
 http://SVRSecure-crl.verisign.com/SVRSecure2005.crl
  http://certificates.godaddy.com/repository/gdroot.crl
...
admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug swm

Configures settings for debugging the Palo Alto Networks software manager.

Syntax

```
debug swm
   {
   history |
   info {image <image_name>} |
   install {image <image_name> | patch <value>} |
   list |
   log |
   refresh content |
   revert |
   status |
   unlock
   }
```

Options

> history — Shows history of software install operations
> info — Displays info on current or specified image
> install — Installs specified image and optional patch
> list — Lists software versions available for install
> log — Shows log of PAN Software Manager
> refresh — Reverts back to last successfully installed content
> revert — Reverts back to last successfully installed software
> status — Shows status of PAN Software Manager
> unlock — Unlocks PAN Software Manager

Sample Output

The following command shows the list of available software versions.

```
admin@PA-HDF> debug swm list

3.1.0-c4.dev
3.1.0-c1.dev_base
3.0.0-c207
3.0.0-c206
admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug system

Defines settings for system debugging actions.

Syntax

```
debug system
   {
   check-fragment |
   disk-sync |
   maintenance-mode |
   ssh-key-reset {all | high-availability | management}
   }
```

Options

> check-fragment — Checks disk fragmentation
> disk-sync — Flushes all writes out to disk
> maintenance-mode — Reboots the system to maintenance mode
> ssh-key-reset — Resets high availability and management SSH keys

Sample Output

The following command reboots the system to maintenance mode.

```
admin@PA-HDF> debug system maintenance-mode
admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug tac-login

Configures settings for debugging the Palo Alto Networks Technical Assistance Center (TAC) connection.

Syntax

```
debug tac-login {challenge | permanently-disable | response}
```

Options

> challenge — Gets challenge value for TAC login
> permanently-disable — Permanently turns off TAC login debugging
> response — Runs verification of challenge response for TAC login

Sample Output

The following command turns TAC login debugging on.

```
admin@PA-HDF> debug tac-login on

admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug user-id

Configures settings for debugging user ID agents.

Syntax

```
debug user-id
   {
   agent <value> |
      {
      clear |
         {
         group-mapping {all | <value>} |
         log
         }
      group-mapping <value> group {list | name <value>} |
      off |
      on {debug | error | info | verbose | warn} |
      receive {no | yes} |
      status
      }
   clear |
      {
      domain-map
      gm-srvc-query {all | <value>} |
      group {all | <value>} |
      log
      registered-ip
      {
         all |
         ip <ip/netmask> |
         vm-info-source {all | <name>}
      }
      }
   dump |
      {
      com statistics |
      domain-map |
      edir-user {all | user <user_name>} |
      ha |
      hip-profile-database {start-from <value>} |
      hip-report {computer <value> | ip <value> | user <value>} |
      idmgr type |
         {
         high-availability state |
         type
            {
            computer {all | id <value> | name <value>} |
            gp-gateway {all | id <value> | name <value>} |
            hip-object {all | id <value> | name <value>} |
            hip-profile {all | id <value> | name <value>} |
            user {all | id <value> | name <value>} |
            user-group {all | id <value> | name <value>}
            }
      log-stats |
      memory {detail | summary} |
      ntlm-stats |
      objects-in-policy |
      probing-stats |
      state |
      ts-agent {config | user-IDs} |
      uid-req-stats |
      vm-monitored-objects {all | ref-id <value> | source-name <value> | type
         <value> |
      xmlapi-stats
      }
   get |
   log-ip-user-mapping {no | yes} |
   off |
   on {debug | dump | error | info | warn} |
   refresh |
      {
      dp-uid-gid |
      group-mapping |
         {
         all |
         group-mapping-name <value> |
         xmlapi-groups
         }
      user-id {ip <ip_address> | agent {all | <value>}
      }
   reset |
      {
      captive-portal ip-address <ip/netmask> |
      com statistics |
      directory-server {all | <value>} |
      global-protect-mdm {all | <value>} |
      group-mapping {all | <value>} |
      ntlm |
      server-monitor {all | <value>} |
      ts-agent {all | <value>} |
      user-id-agent {all | <value>} |
      user-id-manager type {all | computer | gp-gateway | hip-object | hip-
         profile | user | user-group}
      vm-info-source {all | <value>}
      }
   save hip-profile-database |
   set |
      {
      agent {all | basic | conn | detail | group | ntlm | sslvpn | tsa} |
      all |
      base {all | config | ha | id} |
      hip {all | basic | detail | ha} |
      ldap {all | basic | detail} |
      misc {all | misc} |
      userid {all | basic | detail | dirserver | mdm | probing |
         servermonitor | service | syslog | vmmonitor | xmlapi}
      }
   test |
      {
      cp-login ip-address <ip_address> user <value> |
      dynamic-obj-download |
      hip-profile-database {size <value>} |
      hip-report computer <value> ip <ip_address> user <value> {copy {no |
         yes}} |
      ntlm-login ip-address <ip_address> user <value> |
      probing
      }
   unset |
      {
      agent {all | basic | conn | detail | group | ntlm | sslvpn | tsa} |
      all |
      base {all | config | ha | id} |
      hip {all | basic | detail | ha} |
      ldap {all | basic | detail} |
      misc {all | misc} |
      userid {all | basic | detail}
      }
   use-modify-for-group-mapping {no | yes}
   }
```

Options

> agent — Debugging commands for the specified user ID agent
>> clear — Clears agent data
>>> group-mapping — Clears group mapping data on agent (all or specified group mapping)
>>> log — Clears local agent debug logs

```
> agent — Debugging commands for the specified user ID agent
   > clear — Clears agent data
      > group-mapping — Clears group mapping data on agent (all or specified group mapping)
      > log — Clears local agent debug logs
   > group-mapping — Shows proxied group mapping data on agent
      * group — Shows user groups data
         > list — Lists all groups on agent
         > name — Shows group's members on agent
   > off — Turns off agent debug logging
   > on — Turns on agent debug logging
      debug — Only output error, warning, info and debug logs
      error — Only output error logs
      info — Only output error, warning and info logs
      verbose — Output error, warning, info, debug and verbose logs
      warn — Only output error and warning logs
   > receive — Sets whether to receive log from agent
   > status — Displays agent status
> clear — Clears data
   > gm-srvc-query — Clears group query in GM service
   > group — Clears data of specified group(s)
   > log — Clears debug logs
   > registered-ip
      > all — Clears all register IP addresses
      > ip — Clears all registered IP addresses in the specified subnet
      > vm-info-source — Clears registered IP addresses monitored by one or all of the specified VM
         information sources
> dump — Dumps debug data
```

```
    > com — Dumps com messages statistics
    > domain-map — Dumps the domain map
    > edir-user — Dumps edirectory users
        > all — Shows all edirectory users
        > user — Shows edirectory user by username
    > ha — Dumps high availability state
    > hip-profile-database — Dumps HIP profile database
        + start-from — Dumps HIP profile db starting from index (1-131072)
    > hip-report — Dumps HIP report (computer, IP address, or user)
    > idmgr — Dumps ID manager data
        > high-availability — Displays the High Availability state
        > type — Dumps specified type
            > computer — Displays only computer name and/or ID (1-4294967295)
            > gp-gateway — Displays only GlobalProtect gateway name and/or ID (1-4294967295)
            > hip-object — Displays only HIP object name and/or ID (1-65535)
            > hip-profile — Displays only HIP profile name and/or ID (1-1024)
            > user — Displays only user name and/or ID (1-4294967295)
            > user-group — Displays only user-group name and/or ID (1-4294967295)
    > log-stats — Dumps log statistics
    > memory — Dumps memory usage (detail or summary)
    > ntlm-stats — Dumps NTLM statistics
    > objects-in-policy — Shows groups and HIP profiles used in current policy
    > probing-stats — Dumps probing statistics
    > state — Dumps user-id daemon state
    > ts-agent — Dumps terminal server agent data
        > config — Dumps terminal server agent configuration data
        > user-IDs — Dumps terminal server agent user-IDs
    > uid-req-stats — Dumps user ID req statistics
    > vm-monitored-objects — Specify all, reference ID, source name, or type
    > xmlapi-stats — Dumps XML API statistics
> get — Displays current debug logging setting
> log-ip-user-mapping — Whether to generate logs for IP user mapping
> off — Turns off debug logging
> on — Turns on user-id debug logging
    debug — Only output error, warning, info and debug logs
    dump — Output all logs
    error — Only output error logs
    info — Only output error, warning and info logs
    warn — Only output error and warning logs
> refresh — Refreshes data
    > dp-uid-gid — Refreshes DP's user group info
    > group-mapping — Refreshes group mapping data
        > all — Refreshes all groups
        > group-mapping-name — Refreshes specified group mapping data
        > xmlapi-groups — Groups added via XML API
    > user-id — Refetches from user-id agents (query IP address or specify user ID agent)
> reset — Resets data
    > captive-portal — Clears captive portal info (IP address and network mask, x.x.x.x/y)
    > com — Clears com messages statistics
    > directory-server — Reconnects directory server
    > global-protect-mdm— Resets Mobile Security Manager
    > group-mapping — Resets group mapping data (all or specify group)
    > ntlm — Clears NTLM state
    > server-monitor— Resets server monitor
```

```
        > ts-agent — Reconnects TS agent (all or specify agent)
        > user-id-agent — Reconnects user-id agent (all or specify agent)
        > user-id-manager — Clears ID manager cache file
            > all — Resets all types
            > computer — Resets computer IDs
            > gp-gateway — Resets GP gateway IDs
            > hip-object — Resets Host IP object IDs
            > hip-profile — Resets Host Ip profile IDs
            > user — Resets user IDs
            > user-group — Resets user group IDs
        > user-info-source — Reconnects the VM info source (all or specify source)
    > save — Saves HIP profile database data
    > set — Sets user-id debug options
        > agent — Sets agent (all, basic, conn, detail, group, NTLM, SSL VPN, and TS agent)
        > all — Sets all
        > base — Sets base (all, config, HA, and ID)
        > hip — Sets HIP (all, basic, detail, and HA)
        > ldap — Sets LDAP (all, basic, and detail)
        > misc — Sets miscellaneous
        > userid — Sets userid (all, basic, detail, directory server, Mobile Security Manager, probing, server monitor,
            service, syslog, VM monitor, or XML API)
    > test — Tests user-id debugging
        > cp-login — Tests captive portal login
            * ip-address — Dot format IP address
            * user — Fully qualified user name
        > dynamic-obj-download — Triggers dynamic objects download
        > hip-profile-database — Tests batch HIP profile database population
            + size — Batch size (1-65536)
        > hip-report — Tests HIP report creation
            + copy — Copy (no or yes)
            * computer — Computer value
            * ip — IP address
            * user — User value
        > ntlm-login — Tests NTLM login
            * ip-address — Dot format IP address
            * user — Fully qualified user name
        > probing — Triggers periodic WMI probing
    > unset — Unsets user-id debug options
        > agent — Unsets agent (all, basic, conn, detail, group, NTLM, SSL VPN, and TS agent)
        > all — Unsets all
        > base — Unsets base (all, config, HA, and ID)
        > hip — Unsets HIP (all, basic, detail, and HA)
        > ldap — Unsets LDAP (all, basic, and detail)
        > misc — Unsets miscellaneous
        > userid — Unsets userid (all, basic, detail, directory server, probing, service, or XML API)
    > use-modify-for-group-mapping — Specifies whether to use modify timestamp in group mapping
```

Sample Output

The following command displays the current debug logging setting.

```
username@hostname> debug user-id get
```

```
Debug level is info

username@hostname>
```

Required Privilege Level

superuser, vsysadmin

debug vardata-receiver

Configures settings for debugging the variable data daemon.

Syntax

```
debug vardata-receiver
   {
   off |
   on {debug | dump | normal} |
   set {all | third-party {all | libcurl}} |
   show
   statistics
   unset {all | third-party {all | libcurl}}
   }
```

Options

> off — Turns the debugging option off
> on — Turns the debugging option on (debug, dump, or normal)
> set — Sets the variable data receiver (all, third party, libcurl)
> show — Shows whether this command is on or off
> statistics — Shows variable data daemon statistics
> unset — Unsets the variable data receiver (all, third party, libcurl)

Sample Output

The following command shows statistics for the variable data daemon.

```
admin@PA-HDF> debug vardata-receiver statistics

admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug wildfire

Configures settings for debugging the Wildfire services.

Syntax

```
debug wildfire
    {
    cloud-info set
      {add-file-type <value> |
      cloud-type <value> |
      delete-file-type <value>} |
    dp-status |
    file-cache {disable | enable} |
    file-digest sha256 <value> |
    reset {all | dp-receiver | file-cache | forwarding | log-cache | report -
      cache}
    server-selection {enable | disable} |
    }
```

Options

> cloud-info set —
>> add-file-type — Specify type of file
>> cloud-type — Specify type of cloud
>> delete-file-type — Delete previously specified file type
> dp-status — Displays the Wildfire DP status
> file-cache — Enables or disables file caching
> file-digest — Checks sample file
> reset — Resets Wildfire services
>> all — Resets all Wildfire services
>> dp-receiver — Resets the Wildfire DP receiver
>> file-cache — Resets the Wildfire file cache
>> forwarding — Resets the Wildfire service connection
>> log-cache — Resets the Wildfire log cache
>> report-cache — Resets the Wildfire report cache
> server selection— Enable or disable server selection
> transition-file-list— Include transition file list

Sample Output

The following command displays the Wildfire DP status.

```
username@hostname> debug wildfire dp-status

DP status:
        DP:                            123.4.5.6:7890

username@hostname>
```

Required Privilege Level

superuser, vsysadmin

delete

Removes specified types of files from disk or restore the default comfort pages that are presented when files or URLs are blocked.

Syntax

```
delete
   {
   admin-sessions |
   anti-virus update <file_name> |
   config |
     {
     repo device <device_name> {file <value> | running-config device
        <value>} |
     saved <file_name>
     }
   config-audit-history |
   content |
     {
     cache |
        {
        curr-content type {aho-regex | all | decoder | dfa | sml | tdb}
           version <value> |
        old-content
        }
     update <file_name>
     }
   core {data-plane file <file_name> | management-plane file <file_name>} |
   data-capture directory <directory_name> |
   debug-filter file <file_name> |
   dynamic-url host {all | name <value>} |
   global-protect-client {image <file_name> | version <value>} |
   high-availability-key |
   hip-profile-database |
   hip-report |
     {
     all |
     report computer <value> ip <value> user <value>
     }
   license key <value> |
   logo |
   migration-log |
   pcap directory <directory_name> |
   policy-cache |
   report |
     {
     custom scope <name> report-name <name> file-name <name> |
     predefined scope <name> report-name <name> file-name <name> |
     summary scope <name> report-name <name> file-name <name>
     }
   runtime-user-db |
   software {image <file_name> | version <value>} |
   ssh-authentication-public-key |
   sslmgr-store |
     {
     certificate-info {portal} |
        {
        db-serialno <value> |
        name <value> |
        serialno <value>
        }
     satellite-info {portal} |
        {
        name <value> |
        serialno <value> |
        state {assigned | unassigned}
        }
     satellite-info-revoke-certificate portal <value> {serialno <value>}
     }
   threat-pcap directory <directory_name> |
   unknown-pcap directory <directory_name> |
   url-database {all | url <value>} |
   user-file ssh-known-hosts |
   user-group-cache |
   wildfire update <file_name>
   }
```

Options

- > admin-sessions — Removes all active administrative sessions
- > anti-virus — Removes anti-virus updates on disk
- > config — Removes configuration files on disk
  - > repo — Config repository
    - * device — Device name
    - > file — Named snapshot
    - > running-config — Versioned running configuration
  - > saved — Filename
- > config-audit-history — Removes the configuration audit history
- > content — Removes content images or cache on disk
  - > cache — Removes cache files based
    - > curr-content — Removes cache files based on Engine version and type
      - * type — Type of content to be deleted
        - aho-regex — Aho-regex cache
        - all — All caches
        - decoder — Decoder cache
        - dfa — DFA cache
        - sml — SML cache
        - tdb — TDB cache
      - * version — Content version to delete
    - > old-content — Remove ALL old content
  - > update — Filename to remove
- > core — Removes core management or data plane cores on disk
- > data-capture — Removes data capture files
- > debug-filter — Removes debugging packet capture files on disk
- > dynamic-url — Deletes the specified dynamic database(s) (for BrightCloud only)
- > global-protect-client — Removes GlobalProtect client software images on disk
- > high-availability-key — Removes the high availability peer encryption key

```
> hip-profile-database — Deletes the HIP profile database
> hip-report — Deletes Host IP (HIP) reports in disk
     > all — Deletes all Host IP reports
     > report — Deletes specified reports
         * computer — Computer identifier
         * ip — IP address and network mask (x.x.x.x/y)
         * user — User identifier
> license — Removes a license key file
> logo — Removes a custom logo file
> migration-log — (Panorama only) Removes log file created during migration
> pcap — Removes packet capture files
> policy-cache — Removes cached policy compilations from disk
> report — Removes specified reports (custom, predefined, or summary)
> runtime-user-db — Deletes runtime user database (requires commit for rebuilding)
> software — Removes a software image
> ssh-authentication-public-key — Deletes SSH authentication public key
> sslmgr-store — Deletes the specified SSL manager dynamic configuration
> threat-pcap — Removes threat packet capture files in a specified directory
> unknown-pcap — Removes packet capture files for unknown sessions
> url-database — Deletes all or part of the URL database (for the Palo Alto Networks URL filtering database only)
     > all — Clears the URL cache in the management plane
     > url — Clears a specified URL from management plane> user-file — Removes user account settings
> user-group-cache — Deletes user group cache files in disk
> wildfire — Removes Wildfire updates on disk
```

Sample Output

The following command deletes the saved configuration file named *running-config.xml.bak*.

```
username@hostname> delete config saved running-config.xml.bak
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

diff-all

(Panorama only) Diffs shared policy and device configurations.

Syntax

```
diff-all
   {
   shared-policy |
     {
     device <value> |
     include-template {no | yes} |
     merge-with-candidate-cfg {no | yes} |
     remove-overridden-objects {no | yes} |
     vsys <value> |
     device-group <value> |
     num-context-lines <value>
     }
   template
     {
     merge-with-candidate-cfg {no | yes} |
     remove-overridden-objects {no | yes} |
     name <value> |
     num-context-lines <value> |
     device <value>
     }
   }
```

Options

> shared-policy — Diff shared policies

+ device — device name

+ include-template — Whether to include relevant template

+ merge-with-candidate-cfg — Whether to merge with candidate configuration

+ remove-overridden-objects — Whether to remove overridden template objects on the device

+ vsys — Virtual system name

* device-group — Device group name

* num-context-lines — Number of lines of context in the diff (0, 1, 10, 20, 5, all)

> template — Diff templates

+ merge-with-candidate-cfg — Whether to merge with device candidate configuration

+ remove-overridden-objects — Whether to remove overridden objects on the device

* name — Template name

* num-context-lines — Number of lines of context in the diff (0, 1, 10, 20, 5, all)

> device — Device name or list of names enclosed in [ ]

Required Privilege Level

All

exit

Exits the PAN-OS CLI.

> ***Note:*** *The **exit** command is the same as the **quit** command.*

Syntax

```
exit
```

Options

None

Required Privilege Level

All

find

Lists CLI commands containing the specified keyword.

Syntax

```
find command keyword <value>
```

Options

<value> — Specifies a keyword.

Sample Output

The following command lists all CLI commands containing the keyword hsm.

```
username@hostname# find command keyword hsm
set profiles decryption <name> ssl-inbound-proxy block-if-hsm-unavailable
    {yes | no}
set profiles decryption <name> ssl-forward-proxy block-if-hsm-unavailable
    {yes | no}
username@hostname#
```

Required Privilege Level

All

ftp

Uses FTP to export log files. The logs that may be exported are data, threat, traffic or URL logs.

Syntax

```
ftp export log {data | threat | traffic | url} end-time equal <value> start-
   time equal <value> to <value>
   {
   max-log-count <value> |
   passive-mode equal {no | yes} |
   query <value> |
   remote-port <port_number> |
   unexported-only equal {no | yes}
   }
```

Options

+ max-log-count — Maximum number of logs to export (0-65535)
+ passive-mode — Use ftp passive mode
+ query — Query value
+ remote-port — FTP port number on remote host (1-65535)
+ unexported-only — Filter logs that are not previously exported
* end-time — End date and time YYYY/MM/DD@hh:mm:ss (e.g. 2006/08/01@10:00:00)
* start-time — Start date and time YYYY/MM/DD@hh:mm:ss (e.g. 2006/08/01@10:00:00)
* to — Destination (username:password@host) or (username@host)

Required Privilege Level

All

grep

Finds and lists lines from log files that match a specified pattern.

Syntax

```
grep pattern <value>
    {
    after-context <number> |
    before-context <number> |
    context <number> |
    count |
    ignore-case {no | yes} |
    invert-match {no | yes} |
    line-number {no | yes} |
    max-count <number> |
    no-filename {no | yes} |
    dp-log <file_name> |
    mp-log <file_name>
    }
```

Options

+ after-context — Prints the matching lines plus the specified number of lines that follow the matching lines
+ before-context — Prints the matching lines plus the specified number of lines that precede the matching lines
+ context — Prints the specified number of lines in the file for output context
+ count — Specifies whether a count is included in the results
+ ignore-case — Ignores case distinctions
+ invert-match — Selects non-matching lines instead of matching lines
+ line-number — Adds the line number at the beginning of each line of output
+ max-count — Stops reading a file after the specified number of matching lines
+ no-filename — Does not add the filename prefix for output
* pattern — Indicates the string to be matched
> dp-log — Indicates the data plane log file to search for the pattern (press <tab> for a list of file names)
> mp-log — Indicates the management plane log file to search for the pattern (press <tab> for a list of file names)

Sample Output

The following command searches the *brdagent.log* file for occurrences of the string “HEARTBEAT.”

```
username@hostname> grep dp-log sysdagent.log pattern HEARTBEAT
*
Jan 20 14:35:48 HEARTBEAT: Heartbeat failure on core 4
Jan 20 14:35:53 HEARTBEAT: Heartbeat failure on core 1
Jan 20 14:35:54 HEARTBEAT: Heartbeat failure on core 8
Jan 20 14:35:55 HEARTBEAT: Heartbeat failure on core 2
username@hostname>
```

Required Privilege Level

All

less

Lists the contents of the specified log file.

Note: The `dp-log` option will not be available on devices that do not have a dataplane, such as the PA-200.

Syntax

```
less
   {
   agent-log <value> |
   custom-page <filename> |
   dp-backtrace <filename> |
   dp-log <filename> |
   mp-backtrace <filename> |
   mp-global <filename> |
   mp-log <filename> |
   webserver-log <filename>
   }
```

Options

> agent-log — Lists contents of the specified agent log directory (press <tab> for a list of log directories)
> custom-page — Lists contents of the specified custom page file (press <tab> for a list of log files)
> dp-backtrace — Lists contents of the specified data plane backtrace file (press <tab> for a list of log files)
> dp-log — Lists contents of the specified data plane log file (press <tab> for a list of log files)
> mp-backtrace — Lists contents of the specified management plane backtrace file (press <tab> for a list of log files)
> mp-global — Lists contents of the specified management plane global log file (press <tab> for a list of log files)
> mp-log — Lists contents of the specified management plane log file (press <tab> for a list of log files)
> webserver-log — Lists contents of the specified webserver log file (press <tab> for a list of log files)

Sample Output

The following command lists the contents of the web server error log.

```
username@hostname> less webserver-log error.log
   default:2 main  Configuration for Mbedthis Appweb
   default:2 main  ------------------------------------------
   default:2 main  Host:                pan-mgmt2
   default:2 main  CPU:                 i686
   default:2 main  OS:                  LINUX
   default:2 main  Distribution:        unknown Unknown
   default:2 main  OS:                  LINUX
   default:2 main  Version:             2.4.0.0
   default:2 main  BuildType:           RELEASE
   default:2 main  Started at:          Mon Mar  2 12
   ...
```

Required Privilege Level

All

ls

Displays debug file listings.

Syntax

```
ls
   {
   long-format {no | yes} |
   reverse-order {no | yes} |
   sort-by-time {no | yes} |
   content {apps | cache | decoders | global | pan_appversion |
     pan_threatversion | scripts | threats | <content>} |
   custom-page <value> |
   dp-backtrace <filename> |
   dp-log <filename> |
   global <filename> |
   mp-backtrace <filename> |
   mp-global <filename> |
   mp-log <filename> |
   webserver-log <filename>
   }
```

Options

+ long-format — File listing format (use long format)

+ reverse-order — File listing order (list in reverse order)

+ sort-by-time — Sort file listing by time

> content — Specify content to display

> custom-page — Custom page (select value from the list provided; press <tab> for list)

> dp-backtrace — DP backtrace file (select file from the list provided; press <tab> for list)

> dp-log — DP logs (select file from the list provided; press <tab> for list)

> global — Global files (select file from the list provided; press <tab> for list)

> mp-backtrace — MP backtrace file (select file from the list provided; press <tab> for list)

> mp-global — MP global files (select file from the list provided; press <tab> for list)

> mp-log — MP logs (select file from the list provided; press <tab> for list)

> webserver-log — Web server logs (select file from the list provided; press <tab> for list)

Required Privilege Level

All

netstat

Displays network connections and statistics.

Syntax

```
netstat
   {
   all {no | yes} |
   cache {no | yes} |
   continuous {no | yes} |
   extend {no | yes} |
   fib {no | yes} |
   groups {no | yes} |
   interfaces {no | yes} |
   listening {no | yes} |
   numeric {no | yes} |
   numeric-hosts {no | yes} |
   numeric-ports
   numeric-users {no | yes} |
   programs {no | yes} |
   route {no | yes} |
   statistics {no | yes} |
   symbolic {no | yes} |
   timers {no | yes} |
   verbose {no | yes}
   }
```

Options

+ all — Display all sockets (default = connected)
+ cache — Display routing cache instead of Forwarding Information Base (FIB)
+ continuous — Continuous listing
+ extend — Display other/more information
+ fib — Display FIB (default)
+ groups — Display multicast group memberships
+ interfaces — Display interface table
+ listening — Display listening server sockets
+ numeric — Do not resolve names
+ numeric-hosts — Do not resolve host names
+ numeric-ports — Do not resolve port names
+ numeric-users — Do not resolve user names
+ programs — Display PID/Program name for sockets
+ route — Display routing table
+ statistics — Display networking statistics (like SNMP)
+ symbolic — Resolve hardware names
+ timers — Display timers
+ verbose — Display full details

Sample Output

The following command shows an excerpt from the output of the **netstat** command.

```
username@hostname> netstat all yes
...
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     5366   /tmp/ssh-lClRtS1936/
    agent.1936
unix  2     [ ]         DGRAM                  959    @/org/kernel/udev/udevd
unix  18     [ ]         DGRAM                     4465   /dev/log
...
```

Required Privilege Level

All

ping

Checks network connectivity to a host.

Syntax

```
ping host <value>
   {
   bypass-routing {no | yes} |
   count <value> |
   do-not-fragment {no | yes} |
   inet6 {no | yes} |
   interval <value> |
   no-resolve {no | yes} |
   pattern <value> |
   size <value> |
   source <value> |
   tos <value> |
   ttl <value> |
   verbose {no | yes}
   }
```

Options

> bypass-routing — Sends the ping request directly to the host on a direct attached network, bypassing usual routing table
> count — Specifies the number of ping requests to be sent (1-2,000,000,000)
> do-not-fragment — Prevents packet fragmentation by use of the do-not-fragment bit in the packet’s IP header
> inet6 — Specifies that the ping packets will use IP version 6
> interval — Specifies how often the ping packets are sent (0 to 2000000000 seconds)
> no-resolve — Provides IP address only without resolving to hostnames
> pattern — Specifies a custom string to include in the ping request (you can specify up to 12 padding bytes to fill out the packet that is sent as an aid in diagnosing data-dependent problems)
> size — Specifies the size of the ping packets (0-65468 bytes)
> source — Specifies the source IP address for the ping command
> tos — Specifies the type of service (TOS) treatment for the packets by way of the TOS bit for the IP header in the ping packet (1-255)
> ttl — Specifies the time-to-live (TTL) value for the ping packet (IPv6 hop-limit value) (0-255 hops)
> verbose — Requests complete details of the ping request.
* host — Specifies the host name or IP address of the remote host

Sample Output

The following command checks network connectivity to the host 66.102.7.104, specifying 4 ping packets and complete details of the transmission.

```
username@hostname> ping count 4 verbose yes host 66.102.7.104
PING 66.102.7.104 (66.102.7.104) 56(84) bytes of data.
64 bytes from 66.102.7.104: icmp_seq=0 ttl=243 time=316 ms
64 bytes from 66.102.7.104: icmp_seq=1 ttl=243 time=476 ms
64 bytes from 66.102.7.104: icmp_seq=2 ttl=243 time=376 ms
64 bytes from 66.102.7.104: icmp_seq=3 ttl=243 time=201 ms

--- 66.102.7.104 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3023ms
rtt min/avg/max/mdev = 201.718/342.816/476.595/99.521 ms, pipe 2

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

quit

Exits the current session for the firewall.

> ***Note:** The **quit** command is the same as the **exit** command.*

Syntax

```
quit
```

Options

None

Required Privilege Level

All

request acknowledge

Acknowledges alarm logs.

Syntax

```
request acknowledge logid <value>
```

Options

<value> — Specifies the log ID

Required Privilege Level

superuser, vsysadmin, deviceadmin

request analyze-shared-policy

(Panorama only) Displays shadowed object analysis.

Syntax

```
request analyze-shared-policy
```

Options

None.

Required Privilege Level

superuser, vsysadmin, deviceadmin

request anti-virus

Upgrade and downgrade antivirus packages and obtain information about the packages.

Syntax

```
request anti-virus
   {
   downgrade install <value> |
   upgrade
     {
     check |
     download latest {sync-to-peer {no | yes}} |
     info |
     install
        {
        commit {no | yes} |
        sync-to-peer {no | yes} |
        file <filename> |
        version latest
        }
     }
   }
```

Options

> downgrade — Installs a previous version
> upgrade — Performs anti-virus upgrade functions
    > check — Obtains information on available packages from the Palo Alto Networks server
    > download — Downloads anti-virus packages
        + sync-to-peer — Sends a copy to HA peer
    > info — Shows information about available anti-virus packages
    > install — Installs anti-virus packages
        + commit — Indicates whether the installed package will be committed to the firewall
        + sync-to-peer — Indicates whether a copy of the package will be provided to another high-availability peer firewall
        > file — Specifies the name of the file containing the anti-virus package
        > version — Specifies the latest version of the anti-virus software package

Sample Output

The following command displays information on the anti-virus packages that are available for installation.

```
username@hostname> request anti-virus upgrade info
Version                Size          Released on Downloaded
-------------------------------------------------------------------------
46-93                  44MB 2009/11/19  11:50:38        yes
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request batch

(Panorama only) Performs operations on groups of devices.

Syntax

```
request batch
   {
   anti-virus |
     {
     check |
     delete <value> |
     download <value> |
     eligible {file | uploaded-files} <value> |
     info |
     upload-install
        {
        devices <value> |
        file <value> |
        log-collector <value> |
        uploaded-file <value>
        }
     }
   content |
     {
     check |
     delete <value> |
     download <value> |
     eligible {file | uploaded-files} <value> |
     info |
     upload-install
        {
        devices <value> |
        file <value> |
        log-collector <value> |
        uploaded-file <value>
        }
     }
   global-protect-client |
     {
     activate devices <value> {file | uploaded-file} <value> |
     check |
     delete <value> |
     download <value> |
     eligible {file | uploaded-files} <value> |
     info |
     upload devices <value> {file | uploaded-file} <value> |
     upload-activate devices <value> {file | uploaded-file} <value>
     }
   license |
     {
     activate authcodes <value> devices <value> |
     info |
     refresh <value>
     }
  reboot |
     {
     devices <value> |
     log-collector <value>
     }
  software |
     {
     check |
     delete <value> |
     download <value> |
     eligible {file | uploaded-files} <value> |
     info |
     install |
        {
        devices <value> |
        file <value> |
        log-collector <value> |
        uploaded-file <value>
        }
     upload |
        {
        devices <value> |
        file <value> |
        log-collector <value> |
        uploaded-file <value>
        }
     upload-install
        {
        reboot {no | yes} |
        devices <value> |
        file <value> |
        log-collector <value> |
        uploaded-file <value>
        }
     }
  url-filtering |
     {
     check |
     delete <value> |
     download <value> |
     eligible {file | uploaded-files} <value> |
     info |
     upload |
        {
        devices <value> |
        file <value> |
        log-collector <value> |
        uploaded-file <value>
        }
     upload-install
        {
```

```
            reboot {no | yes} |
            devices <value> |
            file <value> |
            log-collector <value> |
            uploaded-file <value>
            }
         }

      vpnclient |
         {
         activate devices <value> {file | uploaded-file} <value> |
         check |
         delete <value> |
         download <value> |
         eligible {file | uploaded-files} <value> |
         info |
         upload devices <value> {file | uploaded-file} <value> |
         upload-activate devices <value> {file | uploaded-file} <value>
         }
      wildfire
         {
         check |
         delete <value> |
         download <value> |
         eligible {file | uploaded-files} <value> |
         info |
         upload-install
            {
            devices <value> |
            file <value> |
            log-collector <value> |
            uploaded-file <value>
            }
         }
      }
```

Options

> anti-virus — Performs antivirus package operations
    > check — Checks for available antivirus package versions
    > delete — Deletes a given antivirus package
    > download — Downloads antivirus packages to Panorama
    > eligible — Gets a list of devices eligible for a given antivirus package
        > file — File containing list of eligible devices
        > uploaded-file — Uploaded file name
    > info — Displays available antivirus packages on Panorama
    > upload-install — Uploads and installs an antivirus package
        > devices — List of devices to upload package onto
        > file — Antivirus package filename
        > log-collector — List of log-collectors to upload package onto
        > uploaded-file — Antivirus package filename
> content — Performs content operations
    > check — Checks for available content versions
    > delete — Deletes a given content package

```
    > download — Downloads content packages to Panorama
    > eligible — Gets a list of devices eligible for a given content package
      > file — File containing list of eligible devices
      > uploaded-file — Uploaded file name
    > info — Displays available content packages on Panorama
    > upload-install — Uploads and installs a content package
      > devices — List of devices to upload package onto
      > file — Content package filename
      > log-collector — List of log-collectors to upload package onto
      > uploaded-file — Content package filename
> global-protect-client — Performs GlobalProtect client package operations
    > activate — Activates a downloaded GlobalProtect client package onto devices
      * devices — List of comma-separated devices to activate GlobalProtect client on
      > file — GlobalProtect client package filename
      > uploaded-file — Uploaded GlobalProtect client package filename
    > check — Checks for available GlobalProtect client packages on the Palo Alto Networks server
    > delete — Deletes a given GlobalProtect client package
    > download — Downloads GlobalProtect client packages to Panorama
    > eligible — Gets a list of devices eligible for a given GlobalProtect client package
      > file — File containing list of eligible devices
      > uploaded-file — Uploaded file name
    > info — Displays available GlobalProtect client packages on Panorama
    > upload — Uploads a downloaded GlobalProtect client package onto devices
      * devices — List of comma-separated devices to install GlobalProtect client on
      > file — GlobalProtect client package filename
      > uploaded-file — Uploaded GlobalProtect client package filename
    > upload-activate — Uploads and activates a downloaded GlobalProtect client package onto devices
      * devices — List of comma-separated devices to install and activate GlobalProtect client on
      > file — GlobalProtect client package filename
      > uploaded-file — Uploaded GlobalProtect client package filename
> license — Performs license operations
    > activate — Activates new license on given devices
      * authcodes — List of comma-separated authcodes to associate with list of devices
      * devices — List of comma-separated devices
    > info — Gets license info for all manager devices on Panorama
    > refresh — Refreshes license check of given devices (list of comma-separated devices)
> reboot — Reboots devices
    > devices — List of devices to reboot
    > log-collector — List of log-collectors to reboot
> software — Performs system software operations
    > check — Checks for available software versions on the Palo Alto Networks server
    > delete — Deletes a given software package
    > download — Downloads software packages to Panorama
    > eligible — Gets a list of devices eligible for a given software package
      > file — File containing list of eligible devices
      > uploaded-file — Uploaded file name
    > info — Displays available software versions on Panorama
    > install — Installs a downloaded software package
      > devices — List of devices to install software onto
      > file — Software package filename
      > log-collector — List of log-collectors to install software onto
      > uploaded-file — Uploaded software package filename
    > upload — Uploads a downloaded software package onto devices
      > devices — List of devices to upload software onto
```

```
            > file — Software package filename
            > log-collector — List of log-collectors to upload software onto
            > uploaded-file — Uploaded software package filename
        > upload-install — Uploads and installs a downloaded software package
            + reboot — Reboots after install
            > devices — List of devices to upload and install software onto
            > file — Software package filename
            > log-collector — List of log-collectors to upload and install software onto
            > uploaded-file — Uploaded software package filename
    > url-filtering— Performs URL filtering database operations
        > check — Checks for available URL filtering database versions on the Palo Alto Networks server
        > delete — Deletes a given URL filtering database
        > download — Downloads a URL filtering database package to Panorama
        > eligible — Gets a list of devices eligible for a given URL filtering database
        > info — Displays available URL filtering database versions on Panorama
        > upload-install — Uploads and installs a downloaded URL filtering database
            > devices — List of devices to upload and install URL filtering database onto
            > file — URL filtering database filename
            > log-collector — List of log-collectors to upload and install URL filtering database onto
    > vpnclient — Performs VPN client package operations
        > activate — Activates a downloaded VPN client package onto devices
            * devices — List of comma-separated devices to activate VPN client on
            > file — VPN client package filename
            > uploaded-file — Uploaded VPN client package filename
        > check — Checks for available VPN client packages on the Palo Alto Networks server
        > delete — Deletes a given VPN client package
        > download — Downloads VPN client packages to Panorama
        > eligible — Gets a list of devices eligible for a given VPN client package
            > file — File containing list of eligible devices
            > uploaded-file — Uploaded file name
        > info — Displays available VPN client packages on Panorama
        > upload — Uploads a downloaded VPN client package onto devices
            * devices — List of comma-separated devices to install VPN client on
            > file — VPN client package filename
            > uploaded-file — Uploaded VPN client package filename
        > upload-activate — Uploads and activates a downloaded VPN client package onto devices
            * devices — List of comma-separated devices to install and activate VPN client on
            > file — VPN client package filename
            > uploaded-file — Uploaded VPN client package filename
    > wildfire — Performs Wildfire package operations
        > check — Checks for available Wildfire package versions
        > delete — Deletes a given Wildfire package
        > download — Downloads antivirus Wildfire to Panorama
        > eligible — Gets a list of devices eligible for a given Wildfire package
            > file — File containing list of eligible devices
            > uploaded-file — Uploaded file name
        > info — Displays available Wildfire packages on Panorama
        > upload-install — Uploads and installs an Wildfire package
            > devices — List of devices to upload package onto
            > file — Wildfire package filename
            > log-collector — List of log-collectors to upload package onto
            > uploaded-file — Wildfire package filename
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request certificate

Generate a self-signed security certificate.

Syntax

```
request certificate
   {
   generate certificate-name <value> name <value> |
     {
     ca {no | yes} |
     country-code <value> |
     days-till-expiry <value> |
     digest <value> |
     email <value> |
     filename <value> |
     locality <value> |
     nbits <value> |
     ocsp-responder-url <value> |
     organization <value> |
     signed-by <value> |
     state <value> |
     passphrase <value> |
     alt-email <value> |
     hostname <value> |
     ip <ip/netmask> |
     organization-unit <value>
     }
   renew certificate-name <value> {days-till-expiry <value>} |
   revoke {certificate-name <value> | sslmgr-store db-serialno <value>
   }
```

Options

> generate — Generate certificate

+ ca — Make this a signing certificate
+ country-code — Two-character code for the country in which the certificate will be used
+ days-till-expiry — Number of days until expiry (1-7300)
+ digest — Digest Algorithm (md5, sh1, sha256, sha384, sha512)
+ email — Email address of the contact person
+ filename — File name for the certificate
+ locality — Locality (city, campus, or other local area)
+ nbits — Length of the key (number of bits in the certificate 1024, 15360, 2048, 3072, 512)
+ organization — Organization using the certificate
+ signed-by — CA for the signing certificate
+ state — Two-character code for the state or province in which the certificate will be used
* certificate-name — Name of the certificate object
* name — IP address or fully qualified domain name (FQDN) to appear on the certificate
> alt-email — Subject alternate email type (value or list of values enclosed in [ ])
> hostname — Subject alternate name DNS type (value or list of values enclosed in [ ])
> ip — Subject alternate name IP type (IP address and network mask; value or list of values enclosed in [ ])
> organization-unit — Department using the certificate (value or list of values enclosed in [ ])

> renew — Renew certificate
>
> + days-till-expiry   Number of days till expiry (1-7300)
> * certificate-name   Name of the certificate object
>
> > revoke — Revoke certificate
> > certificate-name — Certificate name
> > sslmgr-store — Revoke dynamic generated certificate status (serial number)

Sample Output

The following command requests a self-signed certificate for the web interface with length 1024 and IP address 1.1.1.1.

```
username@hostname> request certificate self-signed nbits 1024 name 1.1.1.1
   for-use-by web-interface
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request chassis

Use chassis control commands.

Syntax

```
request chassis
   {
   admin-power-off slot <value> target <value> {now | time-to-wait <value>} |
   admin-power-on slot <value> target <value> |
   enable slot <value> target <value> |
   power-off slot <value> target <value> {now | time-to-wait <value>} |
   power-on slot <value> target <value> |
   restart slot <value> target <value> |
   }
```

Options

> admin-power-off —Power off a slot and keep powered down across reboots and card events - specify slot, target (whether to perform operation locally (default) or on the HA peer device as well), and timing

> admin-power-on —Power on a slot even if in admin power down mode - specify slot, target (whether to perform operation locally (default) or on the HA peer device as well)

> enable—Enable slot for traffic - specify slot and target (whether to perform operation locally (default) or on the HA peer device as well)

> power-off —Power off a slot - specify slot, target (whether to perform operation locally (default) or on the HA peer device as well), and timing

> power-on —Power on a slot - specify slot, target (whether to perform operation locally (default) or on the HA peer device as well)

> restart—Restart slot - specify slot and target (whether to perform operation locally (default) or on the HA peer device as well)

Required Privilege Level

superuser, vsysadmin, deviceadmin

request commit-lock

Sets options for locking commits.

Syntax

```
request commit-lock
   {
   add {comment <value>} |
   remove {admin <value>}
   }
```

Options

> add — Prevents other users from committing
   + comment — Comment value
> remove — Releases commit lock previously held
   + admin — Administrator holding the lock

Required Privilege Level

superuser, vsysadmin, deviceadmin

request config-backup

(Panorama only) Sets device configuration backups.

Syntax

```
request config-lock device <value>
   {
   file <value> |
   running-config <value>
   }
```

Options

* device — Device name
> file — Named snapshot
> running-config — Versioned running config

Required Privilege Level

superuser, vsysadmin, deviceadmin

request config-lock

Sets options for locking configurations.

Syntax

```
request config-lock {add {comment <value>} | remove}
```

Options

> add — Prevents other users from changing the configuration
> remove — Releases a previously held configuration lock

Required Privilege Level

superuser, vsysadmin, deviceadmin

request content

Perform application level upgrade operations.

Syntax

```
request content
   {
   downgrade install {<value> |
   upgrade
     {
     check |
     download latest {sync-to-peer {no | yes}} |
     info |
     install
        {
        commit {no | yes} |
        sync-to-peer {no | yes} |
        file <filename> |
        version latest
        }
     }
   }
```

Options

> downgrade — Installs a previous content version
> upgrade — Performs content upgrade functions
   > check — Obtains information on available packages from the Palo Alto Networks server
   > download — Downloads content packages
      + sync-to-peer — Sends a copy to HA peer
   > info — Shows information about available content packages
   > install — Installs content packages
      + commit — Indicates whether the installed package will be committed to the firewall
      + sync-to-peer — Indicates whether a copy of the package will be provided to another high-availability peer firewall
      > file — Specifies the name of the file containing the content package
      > version — Specifies the latest version of the content software package

Sample Output

The following command lists information about the firewall server software.

```
username@hostname> request content upgrade check

Version                 Size          Released on Downloaded
--------------------------------------------------------------------------
13-25                   10MB 2007/04/19  15:25:02        yes

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request data-filtering

Assign passwords for data filtering.

Syntax

```
request data-filtering access-password
   {
   create password <value> |
   delete |
   modify new-password <value> old-password <value>
   }
```

Options

> create — Creates the specified password
> delete — Deletes the data filtering password (when this command is issued, the system prompts for confirmation and warns that logged data will be deleted and logging will be stopped)
> modify — Changes the specified old password to the new password

Sample Output

The following command assigns the specified password for data filtering.

```
username@hostname> request data-filtering access-password create password
   mypwd

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request device-registration

Performs device registration.

Syntax

```
request device-registration password <pwd> username <user>
```

Options

* password — Specifies the support portal password for device access
* username — Specifies the support portal user name for device access

Sample Output

The following command registers the device with the specified user name and password.

```
username@hostname> request device-registration username admin password
   adminpwd

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request dhcp

Manages the Dynamic Host Configuration Protocol (DHCP) leases with specified client interfaces.

Syntax

```
request dhcp client
   {
   release {all | vlan | <value>} |
   renew {all | vlan | <value>}
   }
```

Options

> release — Interface name to release DHCP lease on (all, VLAN, or interface name)
> renew — Interface name to renew DHCP lease on (all, VLAN, or interface name)

Sample Output

The following command releases the specified interface from its DHCP lease.

```
username@hostname> request dhcp client release ethernet1

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request global-protect-client

Performs GlobalProtect client package operations.

Syntax

```
request global-protect-client software
   {
   activate {file <file_name> | version <value>} |
   check |
   download |
     {
     sync-to-peer {no | yes} |
     file <file_name> |
     version <value>
     }
   info
   }
```

Options

> activate — Activates a downloaded software package
>
>   > file — Upgrades to a software package by filename (press <tab> for list)
>
>   > version — Upgrades to a software package by version (press <tab> for list)

```
> activate — Activates a downloaded software package
   > file — Upgrades to a software package by filename (press <tab> for list)
   > version — Upgrades to a software package by version (press <tab> for list)
> check — Gets information from Palo Alto Networks server
> download — Downloads software packages
   + sync-to-peer — Sends a copy to HA peer
   > file — Downloaded software packages by filename (press <tab> for list)
   > version — Download software packages by version (press <tab> for list)
> info — Shows information about available software packages
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request global-protect-gateway

Requests performance of GlobalProtect gateway functions.

Syntax

```
request global-protect-gateway
   {
   client-logout gateway <value> reason force-logout user <value> |
     {
     computer <value> |
     domain <value>
     }
   satellite-logout gateway <value> reason force-logout serialno <value> |
   unlock auth-profile <value> user <value> vsys <value> {is-seq {no | yes}}
   }
```

Options

> client-logout — GlobalProtect gateway user logout
   + computer — User's computer name
   + domain — User's domain name
   * gateway — Name of the GlobalProtect gateway remote user tunnel name
   * reason — Reason for logout (force)
   * user — User name
> satellite-logout — GlobalProtect gateway satellite logout
   * gateway — Name of the GlobalProtect gateway site-to-site tunnel name
   * reason — Reason for logout (force)
   * serialno — Device serial number
> unlock — Unlock locked users
   + is-seq — Is this authentication sequence?
   * auth-profile — Auth Profile
   * user — User name
   * vsys — Virtual System

Required Privilege Level

superuser, vsysadmin, deviceadmin

request global-protect-portal

Requests performance of GlobalProtect portal functions.

Syntax

```
request global-protect-portal ticket duration <value> portal <value> request
   <value>
```

Options

* duration — Agent user override duration in minutes (0-65535)
* portal — Name of the GlobalProtect portal
* request — Request string in format ^[0-9A-F]{4}-[0-9A-F]{4}$

Required Privilege Level

superuser, vsysadmin, deviceadmin

request global-protect-satellite

Requests performance of GlobalProtect satellite functions.

Syntax

```
request global-protect-satellite
   {
   get gateway-config gateway-address <value> satellite <value> |
   get-portal-config satellite <value>
     {
     password <value> |
     username <value>
     }
   }
```

Options

> get-gateway-config — GlobalProtect satellite get config from gateway
   * gateway-address — GlobalProtect gateway address
   * satellite — GlobalProtect satellite
> get-portal-config — GlobalProtect satellite get config from portal
   + password — Password to login into GlobalProtect portal
   + username — User name to login into GlobalProtect portal
   * satellite — GlobalProtect satellite

Required Privilege Level

superuser, vsysadmin, deviceadmin

request high-availability

Performs high-availability operations.

Syntax

```
request high-availability
   {
   state {functional | suspend} |
   sync-to-remote
     {
     candidate-config |
     clock |
     id-manager {base | user-id} |
     running-config |
     runtime-state
     }
   }
```

Options

> state — Sets the HA state of the device
   > functional — Enables the HA state
   > suspend — Sets the HA state to suspended
> sync-to-remote — Performs configuration sync operations
   > candidate-config — Syncs candidate configuration to peer
   > clock — Syncs the local time and date to the peer
   > id-manager — Syncs ID manager to peer
      > base — Syncs the base id manager to the peer
      > user-id — Syncs the user id manager to the peer
   > running-config — Syncs running configuration to peer
   > runtime-state — Syncs the runtime synchronization state to peer

Sample Output

The following command sets the high-availability state of the device to the suspended state.

```
username@hostname> request high-availability state suspend

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request hsm

Performs Hardware Security Module (HSM) operations.

Syntax

```
request hsm
   {
   authenticate password <password> server <name> |
   ha {create-ha-group password <password> | recover | replace-server
     password <password> | synchronize password <password>} |
   login <password> |
   mkey-wrapping-key-rotation |
   reset |
   rfs-setup |
   rfs-sync |
   server-enroll <value> |
   support-into
   }
```

Options

> authenticate — HSM server name (specify password)
> ha — HSM HA setup
    > create-ha-group — HSM create HA group (specify password)
    > recover — Recovery
    > replace-server — Replace one HSM server in the HA group (specify password)
    > synchronize — HSM synchronize the contents of members of the HA group (specify password)
> login — Specify password for login
> mkey-wrapping-key-rotation — Encrypt the master key with a new wrapping key on HSM
> reset — Clean up HSM client side data: cert, key files, cache, and so on
> rfs-setup — Set up RFS
> rfs-sync — Get update from RF
> server-enroll — Specify HSM server name
> support-info — Create HSM support info. Valid only for Luna SA

Sample Output

The following command sets the high-availability state of the device to the suspended state.

```
username@hostname> request high-availability state suspend

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request last-acknowledge-time

Displays the last alarm acknowledgement time.

Syntax

```
request last-acknowledge-time
```

Options

None

Sample Output

The following command provides the last alarm acknowledgement time.

```
username@hostname> request last-acknowledge-time

0

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request license

Performs license-related operations.

Syntax

```
request license {fetch <auth-code> | info | install}
```

Options

> fetch — Gets a new license key using an authentication code
    + auth-code — Specifies the authentication code to use in fetching the license
> info — Displays information about currently owned licenses
> install — Installs a license key

Sample Output

The following command requests a new license key with the authentication code **123456**.

```
username@hostname> request license fetch auth-code 123456

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request log-fwd-ctrl

Controls device log forwarding.

Syntax

```
request log-fwd-ctrl action {live | start | start-from-lastack | stop} device
    <value>
```

Options

* action — Start or stop log forwarding
    live — Start log forwarding with no buffering
    start — Start log forwarding with buffering
    start-from-lastack — Start log forwarding with buffering, starting from last ack'ed logid
    stop — Stop log forwarding
* device — Serial number of device

Required Privilege Level

superuser, vsysadmin, deviceadmin

request master-key

Changes the master key.

Syntax

```
request master-key lifetime <value> new-master-key <value>
   {
   current-master-key <value> |
   reminder <value> |
   }
```

Options

+ on-hsm — Encrypt the master key on hardware security module (HSM) (yes or no, default is no)
+ current-master-key — Specifies the current master key (64-bit encoded public key)
+ reminder — When to send expiry reminder, in hours (1-8760)
* lifetime — Lifetime of the new key, in hours (1-17520)
* new-master-key — Specifies a new master key (64-bit encoded public key)

Required Privilege Level

superuser, vsysadmin, deviceadmin

request password-change-history

Displays the history of the user password and re-encrypts it.

Syntax

```
request password-change-history
   {
   dump-history {master-key <value>} |
   re-encrypt old-master-key <value> {master-key <value>}
   }
```

Options

> dump-history — Dumps contents of password history

```
   + master-key — Master key used to encrypt passwords
```

> re-encrypt — Re-encrypts password

```
   + master-key — Masterkey to encrypt historical passwords
   * old-master-key — Old masterkey used to encrypt historical passwords
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request password-hash

Generates a hashed string for the user password.

Syntax

```
request password-hash password <pwd>
```

Options

password — Specifies the plain text password that requires the hash string

Sample Output

The following command generates a hash of the specified password.

```
username@hostname> request password-hash password mypassword
```

```
$1$flhvdype$qupuRAx4SWWuZcjhxn0ED.
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request push-report-definitions

(Panorama only) Requests that report definitions are pushed to devices.

Syntax

```
request push-report-definitions
```

Options

None

Sample Output

The following command pushes report definitions to the Panorama managed devices.

```
username@hostname> request push-report-definitions
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request quota-enforcement

Enforces disk quotas for logs and packet captures.

Syntax

```
request quota-enforcement
```

Options

None

Sample Output

The following command enforces the disk quotas.

```
username@hostname> request quota-enforcement
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request restart

Restarts the system or software modules.

> ***CAUTION:*** *Using this command causes the firewall to reboot, resulting in the temporary disruption of network traffic. Unsaved or uncommitted changes will be lost.*

Syntax

```
request restart {dataplane | software | system}
```

Options

> dataplane — Restarts the data plane software
> software — Restarts all system software
> system — Reboots the system

Sample Output

The following command restarts all the firewall software.

```
username@hostname> request restart software
```

Required Privilege Level

superuser, deviceadmin

request shutdown

Performs a clean shutdown of the system.

> ***CAUTION:*** *Using this command causes the firewall to shut down, and network traffic will be disrupted. In addition, unsaved or uncommitted changes will be lost.*

Syntax

```
request shutdown system
```

Options

None

Sample Output

The following command shuts down the firewall.

```
username@hostname> request shutdown system
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request stats

Generates a dump of the statistics.

Syntax

```
request stats dump
```

Options

None

Sample Output

The following command orders a statistics dump.

```
username@hostname> request stats dump

Exec job enqueued with jobid 56
56

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request support

Obtains technical support information.

Syntax

```
request support {check | info}
```

Options

> check — Gets support information from the Palo Alto Networks update server
> info — Shows downloaded support information

Sample Output

The following command shows downloaded support information.

```
username@hostname> request support info
0
Support Home
https://support.paloaltonetworks.com
Manage Cases
https://support.paloaltonetworks.com/pa-portal/
    index.php?option=com_pan&task=vie
wcases&Itemid=100
Download User Identification Agent
https://support.paloaltonetworks.com/pa-portal/
    index.php?option=com_pan&task=sw_
updates&Itemid=135
866-898-9087
support@paloaltonetworks.com
November 07, 2009
Standard
10 x 5 phone support; repair and replace hardware service

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request system

Performs system functions, including self testing, downloading system software, and requesting information about the available software packages.

Syntax

```
request system
   {
   external-list |
     {
     refresh name <value> vsys <value> |
     show name <value> vsys <value> |
     url-test <value>
     }
   fqdn {refresh {force {no | yes}} | show} |
   private-data-reset |
   raid
   {
   slot <value> add <drive> force no-format |
   slot <value> copy from <drive> to <drive> |
   slot <value> remove <drive>
   }
   self-test |
     {
     crypto |
     force-crypto-failure {dp <value> | mp <value>} |
     software-integrity
     }
   self-test-job {crypto | software-integrity} |
   software
     {
     check |
     download {sync-to-peer {no | yes} | file <file> | version <version>} |
     info |
     install {load-config <value> | file <file> | version <version>}
     }
   }
```

Options

> external-list — Performs external-list refresh/sanity functions
   > refresh — Refreshes external-lists
      * name — Name of list
      * vsys — Virtual system
   > show — Prints IPs in an external list
      * name — Name of list
      * vsys — Virtual system
   > url-test — Test accessibility for URL
> fqdn — Performs FQDN refresh/reset functions
   > refresh — Force-refreshes all FQDNs used in rules (option to force)
   > show — Displays FQDNs used in rules and their IP addresses

- > private-data-reset — Removes all of the logs and resets the configuration but does not reset content and software versions
- > raid — Perform operations on RAID (add drive to array, copy and migrate one drive to another in the bay, or remove a drive from the bay)
- > self-test — This option is available in Common Criteria (CC) mode and Federal Information Processing Standard 140-2 (FIPS 140-2) mode (for more information, refer to Chapter 6, “Maintenance Mode”)
  - > crypto — Performs a self-test on all of the cryptographic algorithms the system has on it; if a failure occurs, the system will go into maintenance mode
  - > force-crypto-failure — Causes the system to reboot and fail the specified cryptographic self-test when it reboots; if a failure occurs, the system will go into maintenance mode
    - > dp — Fail test on data plane
    - > mp — Fail test on management plane
  - > software-integrity — Performs a software integrity test; if a failure occurs, the system will go into maintenance mode
- > self-test-job — Runs FIPS/CC self-test jobs
  - > crypto — Runs crypto self-test job
  - > software-integrity — Runs software integrity self-test job
- > software — Performs system software installation functions
  - > check — Gets information from Palo Alto Networks server
  - > download — Downloads software packages
    - + sync-to-peer — Sends a copy to HA peer
    - > file — Downloads software packages by filename
    - > version — Downloads software packages by version
  - > info — Shows information about available software packages
  - > install — Installs a downloaded software package
    - + load-config — Configuration to use for booting new software
    - > file — Upgrades to a software package by filename
    - > version — Upgrades to a software package by version

Sample Output

The following command requests information about the software packages that are available for download.

```
username@hostname> request system software info

Version       Filename                          Size   Released Downloaded
-------------------------------------------------------------------------
3.0.1        panos.4050-3.0.1.tar.gz        127MB 2010/02/07  00:00:00
    no
3.1.0        panos.4050-3.1.0.tar.gz        127MB 2009/02/07  00:00:00
    no

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request tech-support

Obtains information to assist technical support in troubleshooting.

Syntax

```
request technical support dump
```

Options

None

Sample Output

The following command creates a dump for technical support.

```
username@hostname> request tech-support dump

Exec job enqueued with jobid 1
1

username@hostname>
```

Required Privilege Level

superuser

request url-filtering

Performs URL filtering operations.

Syntax

```
request url-filtering
   {
   download |
     {
     paloaltonetworks {region <value>} |
     status vendor {brightcloud | paloaltonetworks}
     }
   install |
     {
     database major-version <value> md5 <value> minor-version <value> |
     signed-database
     }
   revert |
   save url-database |
   update url <value> |
   upgrade {brightcloud {test}}
   }
```

Options

> download — Shows download information for URL filtering
   > paloaltonetworks — Downloads seed database for Palo Alto Networks URL filtering (option to specify APAC, Japan, North America, or other region) (for the Palo Alto Networks URL filtering database only)
   > status — Displays the URL database download status (specify BrightCloud or Palo Alto Networks vendor)
> install — Installs uploaded URL database
   > database — Installs uploaded BrightCloud database (for BrightCloud only)
     * major-version — Major BrightCloud database version
     * md5 — MD5 of BrightCloud database
     * minor-version — Minor BrightCloud database version
   > signed-database — Installs signed uploaded BrightCloud database
> revert — Reverts last URL database (for BrightCloud only)
> save — Saves the Palo Alto Networks URL database cache in the management plane (for the Palo Alto Networks URL filtering database only)
> update — Updates the specified URL category from the cloud (for the Palo Alto Networks URL filtering database only)
> upgrade — Upgrades to latest version (for BrightCloud only)
   + brightcloud — Upgrades BrightCloud database (where present)
     + test — Captures initial download in filter-pcap test_bc_download.pcap

Sample Output

The following command upgrades the BrightCloud database.

```
username@hostname> request url-filtering upgrade brightcloud
```

The following command downloads the North American seed database for the Palo Alto Networks URL filtering database.

```
username@hostname> request url-filtering download paloaltonetworks region
    North-America
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

request wildfire

Performs Wildfire maintenance operations.

For more information on WildFire, refer to the *WildFire Administrator's Guide*.

Syntax

```
request wildfire
   {
   downgrade install <value> |
   registration |
   upgrade
     {
     check |
     download latest {sync-to-peer {no | yes} |
     info |
     install
        {
        commit {no | yes} |
        sync-to-peer {no | yes} |
        file <value> |
        version latest
        }
     }
   }
```

Options

> downgrade — Performs Wildfire downgrade functions (installs Wildfire packages)
> registration — Performs Wildfire registration
> upgrade — Performs Wildfire upgrade functions
   > check — Gets information from Palo Alto Networks server
   > download — Downloads Wildfire packages
      + sync-to-peer — Sends a copy to HA peer
   > info — Shows information about available Wildfire packages
   > install — Installs Wildfire packages
      + commit — Skips commit after installing Wildfire
      + sync-to-peer — Sends a copy to HA peer
      > file — Installs imported Wildfire package
      > version — Installs latest version

Required Privilege Level

superuser, vsysadmin, deviceadmin

schedule

Schedules botnet and UAR reports.

Syntax

```
schedule
   {
   botnet-report topn <value> |
     {
     period {last-24-hrs | last-calendar-day} |
     query <value>
     }
   dlc-query dir {bkwd | fwd} nlogs <value> type <value> |
     {
     count-only {no | yes} |
     csv {no | yes} |
     ini_only {no | yes} |
     query <value>
     }
   uar-report user <username>
     {
     end-time <value> |
     period <value> |
     skip-detailed-browsing {no | yes} |
     start-time <value> |
     title <value>
     user <value> |
     user-group <value> |
     vsys <value> |
     }
   }
```

Options

> botnet-report — Schedule botnet report
   + period — Report period (last 24 hours or last calendar day)
   + query — Query value
   * topn — TopN value (1-500)
> dlc-query — Schedule a DLC query
   + count-only — Report the count only
   + csv — Use Comma Separated Values (CSV) format
   + init_only — Report to include inits only
   + query — Query value
   * dir — Query direction (backward or forward)
   * nlogs — NLogs value (1-100)
   * type — Query type
> uar-report — Schedule user access UAR report
   + end-time — Report end time
   + period — Period to be covered in report
   + skip-detailed-browsing (no or yes)
   + start-time — Report start time

+ title — Report title
+ user — Specify user
+ user-group — Specify user group
+ vsys — Specify vsys

Required Privilege Level

superuser, vsysadmin, deviceadmin

scp export

Uses SCP (secure copy) to upload files from the device to another system. Use this command to copy files between the firewall and another host.

Syntax

```
scp export <option> to <target> {remote-port <port_number> | source-ip
   <ip_address>}
   {
   application-block-page |
   application-pcap from <file_name> |
   captive-portal-text |
   configuration from <file_name> |
   core-file {data-plane | management-plane} from <file_name> |
   crl from <file_name> |
   debug-pcap from <file_name> |
   device-state |
   file-block-continue-page |
   file-block-page |
   filter-pcap from <file_name> |
   global-protect-portal-custom-help-page name <file_name> |
   global-protect-portal-custom-login-page name <file_name> |
   global-protect-portal-custom-welcome-page name <file_name> |
   high-availability-key from <file_name> |
   inbound-proxy-key from <value> |
   log {data | threat | traffic | url} end-time equal <value> start-time
     equal <value> |
     {
     max-log-count <value> |
     query <value> |
     unexported-only equal {no | yes}
     }
   log-file {data-plane | management-plane} |
   logdb |
```

Because the file for the entire log database is too large for an export to be practical on the following platforms, they do not support the **scp export logdb** command: Panorama virtual appliance running Panorama 6.0 or later releases, Panorama M-Series appliances (all releases), and PA-7050 firewall (all releases).

```
   mgmt-pcap from <file_name> |
   pan-url-db |
   pdf-reports from <file_name> |
   ssl-cert-status-page |
   ssl-optout-text |
   stats-dump {end-time equal <value> | start-time equal <value>} |
   tech-support |
   threat-pcap from <file_name> |
   url-block-page |
   url-coach-text |
   virus-block-page |
   web-interface-certificate
   }
```

Options

```
+ remote-port — SSH port number on remote host (1-65535)
+ source-ip — Set source address to specified interface address (x.x.x.x or IPv6)
* to — Destination (username@host:path)
> application-block-page — Use scp to export application block comfort page
> application-pcap — Use scp to export an application packet capture file
    * from — pcap file name
> captive-portal-text — Use scp to export text to be included in a captive portal
> configuration — Use scp to export a configuration file
    * from — File name
> core-file — Use scp to export a core file
    > data-plane — Use scp to export a data plane core file
      * from — File name
    > management-plane — Use scp to export a management plane core file
      * from — File name
> crl — Use scp to export a crl.tgz file
    * from — File name
> debug-pcap — Use scp to export packet capture generated for the purpose of debugging daemons
    * from — pcap file name
> device-state — Use scp to export device state files from a GlobalProtect Portal
> file-block-continue-page — Use scp to export a file containing comfort pages to be presented when files are blocked
> file-block-page — Use scp to export file block comfort page
> filter-pcap — Use scp to export filter packet capture
    * from — pcap file name
> global-protect-portal-custom-help-page — Use scp to export global protect help page
    * name — Help page filename
> global-protect-portal-custom-login-page — Use scp to export global protect login page
    * name — Log in page filename
> global-protect-portal-custom-welcome-page — Use scp to export global protect welcome page
    * name — Welcome page filename
> high-availability-key — Use scp to export a high-availability peer encryption key
    * from — File name
> inbound-proxy-key — Use scp to export an inbound proxy key
    * from — Value (0-7)
> log — Use scp to export a log in comma-separated values (CSV) format (data, threat, traffic, or URL log)
    + max-log-count — Max number of logs to export (0-65535)
    + query — Query value, enclosed in quotation marks
    + unexported-only — Filter logs that are not previously exported (no or yes)
    * end-time — Date and time YYYY/MM/DD@hh:mm:ss (e.g. 2006/08/01@10:00:00)
    * start-time — Date and time YYYY/MM/DD@hh:mm:ss (e.g. 2006/08/01@10:00:00)
> log-file — Use scp to export log file
    > data-plane — Use scp to export data-plane core-file
    > management-plane — Use scp to export management-plane core-file
> logdb — Use scp to export a log database
> mgmt-pcap — Use scp to export packet capture from management interface
    * from — pcap file name
> pan-url-db — Use scp to export Palo Alto Networks URL database
> pdf-reports — Use scp to export PDF reports
    * from — File name
> ssl-cert-status-page — Use scp to export an SSL certificate status page
> ssl-optout-text — Use scp to export SSL optout text
> stats-dump — Use scp to export Application Visibility and Risk (AVR) Report data (default is last 7 days)
    + end-time — date and time YYYY/MM/DD@hh:mm:ss (e.g. 2006/08/01@10:00:00)
    + start-time — date and time YYYY/MM/DD@hh:mm:ss (e.g. 2006/08/01@10:00:00)
```

```
> tech-support — Use scp to export technical support information
> threat-pcap — Use scp to export threat packet capture
      * from — pcap file name
> url-block-page — Use scp to export a comfort page to be presented when files are blocked due to a blocked URL
> url-coach-text — Use scp to export text to be presented when files are blocked due to a blocked URL
> virus-block-page — Use scp to export a comfort page to be presented when files are blocked due to a virus
> web-interface-certificate — Use scp to export a web interface certificate
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

scp import

Uses SCP (secure copy) to download files to the device. Use this command to download a customizable HTML replacement message (comfort page) in place of a malware infected file.

Syntax

```
scp import <option> from <source> {remote-port <port_number> | source-ip
   <ip_address>}
   {
   anti-virus |
   application-block-page |
   captive-portal-text |
   certificate |
   configuration |
   content |
   device-state |
   file-block-continue-page |
   file-block-page |
   global-protect-client |
   global-protect-portal-custom-help-page profile <profile_name> |
   global-protect-portal-custom-login-page profile <profile_name> |
   global-protect-portal-custom-welcome-page profile <profile_name> |
   high-availability-key |
   keypair certificate-name <name> format {pem | pkcs12} passphrase <value> |
   license |
   logdb |
```

Because the file for the entire log database is too large for an import to be practical on the following platforms, they do not support the **`scp import logdb`** command: Panorama virtual appliance running Panorama 6.0 or later releases, Panorama M-Series appliances (all releases), and PA-7050 firewall (all releases).

```
   private-key certificate-name <name> format {pem | pkcs12} passphrase
     <value> |
   signed-url-database |
   software |
   ssl-cert-status-page |
   ssl-optout-text |
   ui-translation-mapping |
   url-block-page |
   url-coach-text |
   url-database |
   virus-block-page |
   wf-content |
   wildfire |
   wildfire-api-keys |
   wildfire-vm-image |
   }
```

Options

+ remote-port — SSH port number on remote host (1-65535)

+ source-ip — Set source address to specified interface address (x.x.x.x or IPv6)
* from — Source (username@host:path)
> anti-virus — Use scp to import anti-virus content
> application-block-page — Use scp to import application block comfort page
> captive-portal-text — Use scp to import text to be used in a captive portal
> certificate — Use scp to import an X.509 certificate
> configuration — Use scp to import a configuration file
> content — Use scp to import database content
> device-state — Use scp to import device state files for a GlobalProtect Portal
> file-block-continue-page — Use scp to import a blocked file continue page
> file-block-page — Use scp to import a file containing comfort pages to be presented when files are blocked
> global-protect-client — Use scp to import globalProtect client package
> global-protect-portal-custom-help-page — Use scp to import GlobalProtect portal custom help page
    * profile — For GlobalProtect portal profile
> global-protect-portal-custom-login-page — Use scp to import GlobalProtect portal custom login page
    * profile — For GlobalProtect portal profile
> global-protect-portal-custom-welcome-page — Use scp to import GlobalProtect portal custom welcome page
    * profile — For GlobalProtect portal profile
> high-availability-key — Use scp to import a high-availability peer encryption key
> keypair — Use scp to import an X.509 key pair
    * certificate-name — Name of the certificate object
    * format — Format of the keypair (PEM or PKCS12)
    * passphrase — Passphrase value
> license — Use scp to import a license file
> logdb — Use scp to import a log database
> private-key — Use scp to import an X.509 key
    * certificate-name — Name of the certificate object
    * format — Format of the keypair (PEM or PKCS12)
    * passphrase — Passphrase for private key
> signed-url-database — Use scp to import a signed url database package
> software — Use scp to import a software package
> ssl-cert-status-page — Use scp to import an SSL certificate status page
> ssl-optout-text — Use scp to import SSL optout text
> ui-translation-mapping — Use scp to import UI translation mapping
> url-block-page — Use scp to import a comfort page to be presented when a URL category is blocked in a security policy or URL filtering profile
> url-coach-text — Use scp to import coach text about possible actions on the URL comfort page
> url-database — Use scp to import a URL database package (for BrightCloud only)
> virus-block-page — Use scp to import a virus block comfort page
> wf-content — Import WF-500 appliance content updates
> wildfire — Use scp to import Wildfire content
> wildfire-api-keys — Import WildFire API keys to a WF-500 appliance
> wildfire-vm-image — Import Virtual Machine (VM) sandbox images to a WF-500 appliance

Sample Output

The following command imports a license file from a file in user1’s account on the machine with IP address 10.0.3.4.

```
username@hostname> scp import certificate from user1@10.0.3.4:/tmp/
   certificatefile
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set application

Configures parameters for system behavior when applications are blocked.

Syntax

```
set application
   {
   cache {no | yes} |
   dump |
      {
      off |
      on
         {
         application <name> |
         destination <ip_address> |
         destination-port <port_number> |
         destination-user <value> |
         from <zone> |
         limit <value> |
         protocol <value> |
         rule <name> |
         source <ip_address> |
         source-port <port_number> |
         source-user <value> |
         to <zone>
         }
      }
   dump-unknown {no | yes} |
   heuristics {no | yes} |
   notify-user {no | yes} |
   supernode {no | yes} |
   traceroute
      {
      enable {no |yes} |
      ttl-threshold <value>
   }
```

Options

> cache — Enables or disables the application cache
> dump — Enables or disables the application packet capture. The following options determine the contents of the dump:
+ application — Specified application
+ destination — Destination IP address of the session
+ destination-port — Destination port
+ destination-user — Destination user
+ from — Specified zone
+ limit — Maximum number of sessions to capture
+ protocol — Specified protocol
+ rule — Specified rule name
+ source — Source IP address for the session

+ source-port — Specified source port
+ source-user — Specified source user
+ to — Specified zone
> dump-unknown — Enables or disables capture of unknown applications
> heuristics — Enables or disables heuristics detection for applications
> notify-user — Enables or disables user notification when an application is blocked
> supernode — Enables or disables detection of super nodes for peer-to-peer applications that have designated supernodes on the Internet
> traceroute — Application identification for traceroute
+ enable — Enables/disables
+ ttl-threshold — Sets the TTL threshold value for traceroute identification

Sample Output

The following command turns packet capture for unknown applications off.

```
username@hostname> set application dump-unknown off

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set cli

Configures scripting and pager options for the PAN-OS CLI. Options are included to display configuration commands in default format, XML format, or as operational **set** commands.

Syntax

```
set cli
   {
   config-output-format {default | json | set | xml} |
   confirmation-prompt {off | on} |
   hide-ip |
   hide-user |
   pager {off | on} |
   scripting-mode {off | on} |
   terminal {height <value> | type <value> | width <value>} |
   timeout idle {never | value>}
   }
```

Options

> config-output-format — Sets the output format for the configuration file to the default, JSON, XML format, or **set** command format
> configuration-prompt — Enables or disables presentation of a confirmation prompt for some configuration commands
> hide-ip — Hides the last octet of the IP address in logs
> hide-user — Hides user names in logs
> scripting-mode — Toggles scripting mode (scripting mode will modify the CLI output such that special characters used for formatting are suppressed)
> pager — Enables or disables pagers
> terminal — Sets terminal parameters for CLI access
    > height — Sets terminal height (1-500)
    > type — Sets terminal type (press <tab> for list)
    > width — Sets terminal width (1-500)
> timeout — Sets administrative session timeout values
    + idle — Idle timeout (never or 0-1440 minutes; default = 60 minutes)

Sample Output

The following command sequence sets the configuration mode to use **set** command format for output and then displays the output of the **show system log-export-schedule** command in Configuration mode.

```
username@hostname> set cli config-output-format set
username@hostname> configure
Entering configuration mode
[edit]
username@hostname# edit deviceconfig
[edit deviceconfig]
username@hostname# show system log-export-schedule

set deviceconfig system log-export-schedule 10.16.0.97 description 10.16.0.97
set deviceconfig system log-export-schedule 10.16.0.97 enable yes
set deviceconfig system log-export-schedule 10.16.0.97 log-type threat
set deviceconfig system log-export-schedule 10.16.0.97 start-time 03:00
set deviceconfig system log-export-schedule 10.16.0.97 protocol ftp hostname
    10.16.0.97
set deviceconfig system log-export-schedule 10.16.0.97 protocol ftp port 21
set deviceconfig system log-export-schedule 10.16.0.97 protocol ftp passive-
    mode yes
set deviceconfig system log-export-schedule 10.16.0.97 protocol ftp username
    admin
set deviceconfig system log-export-schedule 10.16.0.97 protocol ftp password
    mZDB7rbW5y8=
username@hostname#
```

The following command sequence shows the same example after XML is specified as the command output format.

```
username@hostname> set cli config-output-format xml
username@hostname> configure
Entering configuration mode
[edit]
username@hostname# edit deviceconfig
[edit deviceconfig]
username@hostname# show system log-export-schedule

<log-export-schedule>
  <entry name="10.16.0.97">
    <description>10.16.0.97</description>
    <enable>yes</enable>
    <log-type>threat</log-type>
    <start-time>03:00</start-time>
    <protocol>
      <ftp>
        <hostname>10.16.0.97</hostname>
        <port>21</port>
        <passive-mode>yes</passive-mode>
        <username>admin</username>
        <password>mZDB7rbW5y8=</password>
      </ftp>
    </protocol>
  </entry>
</log-export-schedule>
[edit deviceconfig]
[edit deviceconfig]
username@hostname#
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set clock

Configures the system date and time.

Syntax

```
set clock {date <value> | time <value>}
```

Options

+ date — Specify the date in *yyyy/mm/dd* format
+ time — Specify the time in *hh:mm:ss* format (*hh*: 0-23, *mm*: 0-59, *ss*: 0-59)

Sample Output

The following command sets the system date and time.

```
username@hostname> set clock date 2009/03/20 time 14:32:00
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set data-access-password

Configures the access password for the data filtering logs. The data filtering log records information on the security policies that help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall.

Syntax

```
set data-access-password <pwd>
```

Options

<pwd> — Specifies the password for accessing data filtering logs

Sample Output

The following command sets the password for data filtering logs.

```
username@hostname> set data-access password 12345678
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set management-server

Configures parameters for the management server, which manages configuration, reports, and authentication for the firewall.

Syntax

```
set management-server
   {
   logging {import-end | import-start | off | on} |
   unlock admin <user_name>
   }
```

Options

> logging — Sets the following logging options:
   import-end — Exit import mode
   import-start — Enter import mode
   off — Disable logging
   on — Allow logging
> unlock — Unlocks locked administrators (specify username of administrator to unlock)

Sample Output

The following command enables logging on the management server.

```
username@hostname> set management-server logging on
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set panorama

Enables or disables the connection between the firewall and Panorama. For more information, refer to the *Panorama Administrator's Guide*.

Syntax

```
set panorama {off | on}
```

Options

on — Enables the connection between the firewall and Panorama
off — Disables the connection between the firewall and Panorama

Sample Output

The following command disables the connection between the firewall and Panorama.

```
username@hostname> set panorama off
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set password

Configures the firewall password. When you issue this command, the system prompts you to enter the old and new password and to confirm the new password.

Syntax

```
set password
```

Options

None

Sample Output

The following example shows how to reset the firewall password.

```
username@hostname> set password
Enter old password : (enter the old password)
Enter new password : (enter the new password0
Confirm password   : (reenter the new password)

Password changed

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set serial-number

(Panorama only) Configures the serial number of the Panorama machine. The serial number must be set for Panorama to connect to the update server.

Syntax

```
set serial-number <value>
```

Options

<value> — Specifies the serial number or software license key

Sample Output

The following command sets the Panorama serial number to 123456.

```
username@hostname> set serial-number 123456
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set session

Configures parameters for the networking session.

Syntax

```
set session
   {
   accelerated-aging-enable {no | yes} |
   accelerated-aging-scaling-factor <value> |
   accelerated-aging-threshold <value> |
   default |
   distribution-policy
   {
      fixed <value> |
      hash {destination | source} |
      ingress-slot |
      random |
      round-robin |
      session-load
   }
   offload {no | yes} |
   resource-limit-behavior {bypass | drop} |
   scan-scaling-factor <value> |
   scan-threshold <value> |
   tcp-reject-non-syn {no | yes} |
   timeout-captive-portal <value> |
   timeout-default <value> |
   timeout-discard-default <value> |
   timeout-discard-tcp <value> |
   timeout-discard-udp <value> |
   timeout-icmp <value> |
   timeout-scan <value> |
   timeout-tcp <value> |
   timeout-tcphandshake <value> |
   timeout-tcpinit <value> |
   timeout-tcpwait <value> |
   timeout-udp <value>
   }
```

Options

> accelerated-aging-enable — Enables or disables accelerated session aging
> accelerated-aging-scaling-factor — Sets the accelerated session aging scaling factor (power of 2, between 2-16)
> accelerated-aging-threshold — Sets the accelerated aging threshold as a percentage of session utilization (50-99)
> default — Restores all session settings to default values
> distribution-policy — The PA-7050 platform logically partitions security processing and I/O and in most cases, there is no set constraint that determines the slot or processor to which a given session is processed. Administrators can use this CLI command to define how sessions are handled.
   > fixed — Select a fixed dataplane. This is mainly used for debugging purposes.
   > hash — Sessions are distributed based on a hash of the source address or destination address. This option is recommended for environments that use large scale source NAT with Dynamic IP translation (DIP) and/or

Dynamic IP and Port translation (DIPP). This is accomplished by improving the efficiency of NAT resource management and by reducing the latency for NAT session setup due to potential IP/port conflicts. When using DIP, it is recommended to set the source address option and for DIPP, use the destination address option.

> ingress-slot — This option is the default setting for session distribution. In this case, I/O and security processing will be coupled on a per slot basis. Sessions will be distributed to the slot that contains the ingress interface of the first packet and processor selection is based on a hash of the source address and destination address. This option will attempt to reduce the number of times that a packet traverses the switch fabric when the ingress and egress interfaces reside on the same slot, or in environments without an asymmetric forwarding path. This option is recommended for latency-sensitive environments and because I/O and firewalling are coupled, when a hot-swap of a card is needed in an HA configuration, session migration may perform better.

> random — The dataplane will be randomly selected from a pool of active dataplanes.

> round-robin — This option will choose the dataplane based on round robin between active dataplanes; meaning that I/O and security processing will be shared among all active dataplanes.

> session-load — The dataplane is chosen based on the session count of each dataplane. The dataplane with the lowest count is selected for security processing. This option is recommended for environments where the I/O is distributed across multiple slots. For example, an inter-slot aggregate interface group or environments with asymmetric forwarding.

> offload — Enables or disables hardware session offload (Some firewall models have specialized hardware to manage TCP, UDP, and ICMP sessions. This option enables or disables this capability. If it is disabled, the sessions are managed by the firewall software.)

> resource-limit-behavior — Behavior when resource limit is reached (bypass or drop)

> scan-scaling-factor — Sets scan scaling factor (2-16)

> scan-threshold — Resource utilization threshold to trigger session scan (50-99)

> tcp-reject-non-syn — Rejects non-synchronized TCP packets for session setup (no or yes)

> timeout-captive-portal — Sets captive portal session timeout value, in seconds (1-15999999)

> timeout-default — Sets the session default timeout value, in seconds (1-604800)

> timeout-discard-default — Sets timeout of non-TCP/UDP session in discard state (1-604800)

> timeout-discard-tcp — Sets timeout of TCP session in discard state (1-604800)

> timeout-discard-udp — Sets timeout of UDP session in discard state (1-604800)

> timeout-icmp — Sets the session timeout value for ICMP commands (1-604800)

> timeout-scan — Application trickling timeout value, in seconds (5-30)

> timeout-tcp — Sets the session timeout value for TCP commands (1-5999999)

> timeout-tcphandshake — Sets session tcp handshake timeout value, in seconds (1-60)

> timeout-tcpinit — Sets the initial TCP timeout value, in seconds (1-60)

> timeout-tcpwait — Sets the session TCP wait timeout value, in seconds (1-60)

> timeout-udp — Sets the session timeout value for UDP commands (1-604800)

Sample Output

The following command sets the TCP timeout to 1 second.

```
username@hostname> set session timeout-tcpwait 1
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set ssh-authentication

Configures a public key for Secure Shell (SSH) authentication.

Syntax

```
set ssh-authentication {public-key <value>}
```

Options

+ public-key — Specifies the public key (RSA or DSA)

Sample Output

The following command configures the public key for SSH authentication.

```
username@hostname> set ssh-authentication public-key ssh-rsa AAAAB3N....
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

set system

Configures system operational parameters.

Syntax

```
set system
   {
   nfs dynamic-logging-partition threshold <value> |
   setting
     {
     ctd |
        {
        regex-stats-on {no | yes} |
        strip-x-fwd-for {no | yes} |
        x-forwarded-for {no | yes}
        }
     fan-mode {auto | on} |
     jumbo-frame {off | on} |
     logging |
        {
        default |
        default-policy-logging <value> |
        log-suppression {no | yes} |
        max-log-rate <value> |
        max-packet-rate <value>
        }
     mp-memory-monitor enable {no | yes}|
     packet-descriptor-monitor enable {no | yes}|
     packet-path-test enable {no | yes}|
     packet-path-test show |
     multi-vsys {off | on}|
     packet ip-frag-limit {no | yes} |
     pow |
        {
        wqe-inuse-check {no | yes} |
        wqe-swbuf-check {no | yes} |
        wqe-swbuf-ref {no | yes} |
        wqe-tag-check {no | yes}
        }
     shared-policy {disable | enable | import-and-disable} |
     ssl-decrypt |
        {
        answer-timeout <value> |
        notify-user {no | yes} |
        skip-ssl {no | yes} |
        skip-ssl-decrypt {no | yes}
        }
     target |
        {
        device-group <value> |
        none |
        template {name <value> | vsys <value>}
        }
     target-vsys {none | <vsystem>} |
     template {disable | enable | import-and-disable} |
     url-database <name> |
     url-filtering-feature {cache | filter} {false | true} |
     util assert-crash-once {no | yes} |
     wildfire interval
        {
        report-update-interval {default | <value>} |
        server-list-update-interval {default | <value>}
        }
     zip enable {yes | no}
     }
```

Options

>nfs
> setting — Sets system settings
    > ctd
        > regex-stats-on — Whether or not generate regular expression statistics
        > strip-x-fwd-for — Whether or not to strip x-forwarded-for from HTTP headers. When this option is selected, the firewall zeroes out the header value before forwarding the request, and the forwarded packets do not contain internal source IP information.
        > x-forwarded-for — Enables or disables parsing of the x-forwarded-for attribute
    >fan-mode — Sets fan to auto (fan turns on when needed) or on (always on); default = on
    > jumbo-frame — Sets jumbo frame mode
    > logging — Sets logging parameters
        > default — Restores logging parameters to the default settings
        > default-policy-logging — Sets the default log policy
        > log-suppression — Enables or disables log suppression (1-300)
        > max-packet-rate value — Sets the maximum packet rate for logging (0-50000)
        > max-log-rate value — Sets the maximum logging rate (0-2560)
    > multi-vsys — Enables or disables multiple virtual systems
    > packet — Enables or disables the IP fragmentation limit
    > mp-memory-monitor—Set monitoring of management memory
    > packet-descriptor-monitor—Set monitoring of packet descriptors
    > packet-path-test—Enable path test commands
    > packet-path-test show—Show which slots have path test enabled
    > pow — Enables or disables the Linux pow function Work Queue Entry (WQE) checks
        > wqe-inuse-check — Enable/disable WQE in-use check
        > wqe-swbuf-check — Enable/disable WQE software buffer trailer check
        > wqe-swbuf-ref — Enable/disable WQE software buffer ref in clone
        > wqe-tag-check — Enable/disable WQE session ID tag check
    > shared-policy — Enables, disables, or imports and disables shared policies
    > ssl-decrypt — Sets SSL decryption parameters
        > answer-timeout — Set ssl-decrypt answer timeout value (1-86400)
        > notify-user — Enable/disable notify user web page
        > skip-ssl — Enable/disable SSL decryption
        > skip-ssl-decrypt — Enable/disable ssl-decrypt
    > target — Target device group or template for operational commands
        > device-group — Target device group for operational commands
        > none — Unset target device group or template for operational commands
        > template — Target template for operational commands

+ name — Target template name for operational commands
+ vsys — Target template virtual system for operational commands
> target-vsys — Enables the specified virtual system for operational commands
> template — Template management via Panorama
- disable — Discard and disallow template to be pushed from Panorama
- enable — Allow template to be pushed from Panorama
- import-and-disable — Import and disallow template to be pushed from Panorama
> url-database — Sets the URL database
> url-filtering-feature — (BrightCloud only) Change URL filtering feature settings.

Note: These cache and filter options are not synchronized in an HA configuration, so you must configure them on both devices in the HA pair. After changing the setting, you must run the following command to activate: `debug software restart device-server`. Because these options take up management memory, it is recommended that you only enable them when high performance URL filtering is required. Both options are disabled by default.

> cache — Enable/disable the Base DB cache feature for URL filtering. This option caches the last one million queries stored in the on-device URL database and will keep them in the management plane memory to speed up URL lookups.
> filter — Enable/disable the Bloom filter feature for URL filtering. This option caches the MD5 hashes of the 20 million URLs stored in the on-device database and will keep them in the management plane memory to speed up URL lookups. With this option enabled, the system can quickly query the cache to check if the URL is present in the on-device database stored on disk; without having to actually access the disk.
> util — Sets the option to assert crash once
> wildfire — Sets the Wildfire intervals
+ report-update-interval — Sets the report update interval, in seconds (1-3600; default = 5 minutes (300 seconds))
+ server-list-update-interval — Sets the cloud server list update interval, in minutes (1-10080; default = one week (10080 minutes))
> zip — Enables or disables decompression of files within traffic for content scanning purposes

Sample Output

The following command enables logging suppression.

```
username@hostname> set system setting logging log-suppression yes
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show admins

Displays information about the active firewall administrators.

Syntax

```
show admins {all}
```

Options

+ all — Lists the names of all administrators

Sample Output

The following command displays administrator information for the 10.0.0.132 firewall.

```
username@hostname> show admins | match 10.0.0

Admin                           From     Type Session-start      Idle-for
--------------------------------------------------------------------------
admin                     10.0.0.132      Web 02/19 09:33:07     00:00:12s

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show arp

Displays current Address Resolution Protocol (ARP) entries.

Syntax

```
show arp <interface_name>
```

Options

<interface_name> — Specifies the interface for which the ARP table is displayed

- all — Displays information for all ARP tables
- ethernet*n/m* — Displays information for the specified interface
- loopback — Displays loopback information
- mgt — Displays host ARP information
- vlan — Displays VLAN information

Sample Output

The following command displays ARP information for the ethernet1/1 interface on a PA-200 firewall running PAN-OS 6.0.

```
username@hostname> show arp ethernet1/1

maximum of entries supported :      500
default timeout:                    1800 seconds
total ARP entries in table :        46
total ARP entries shown :           46
status: s - static, c - complete, i - incomplete

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show authentication

Displays authentication information.

Syntax

```
show authentication {allowlist | groupdb | groupnames}
```

Options

> allowlist — Displays the authentication allow list
> groupdb — Lists the group authentication databases
> groupnames — Lists the distinct group names

Sample Output

The following command shows the list of users that are allowed to access the firewall.

```
username@hostname> show authentication allowlist

vsysname    profilename  username
----------  -----------  ----------------------------
vsys1       SSLVPN       paloaltonetwork\domain users
vsys1       wtam-SSLVPN  group1

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show chassis-ready

Shows whether the data plane has a running policy.

Syntax

```
show chassis-ready
```

Options

None

Sample Output

The following command shows that the data plane has a currently running policy.

```
username@hostname> show chassis-ready
yes

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show chassis

Display chassis state and information.

Syntax

```
show chassis
{
    inventory |
    power |
    status {slot <value>}
}
```

Options

> inventory — Show chassis component information
> power — Show chassis power usage information
> status — Show chassis status information (can specify slot)

Sample Output

The following command shows chassis status.

```
username@hostname> show chassis status
Slot       Component          Card Status        Config Status   Disabled
1          PA-7000-20G-NPC    Up                 Success
2          PA-7000-20G-NPC    Up                 Success
3          empty
4          PA-7000-SMC        Up                 Success
5          PA-7000-20G-NPC    Up                 Success
6          empty
7          PA-7000-20G-NPC    Up                 Success
8          PA-7000-LPC        Up                 Success

----------------------------------------------------------------------------
    ----
Chassis autocommit ready : True
Inserted slots           : 1 2 4 5 7 8
Powered slots            : 1 2 4 5 7 8
Config ready slots       : 1 2 4 5 7 8
Config done slots        : 1 2 4 5 7 8
Traffic enabled slots    : 1 2 5 7


username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show cli

Displays information about the current CLI session.

Syntax

```
show cli {idle-timeout | info | permissions}
```

Options

> idle-timeout — Displays timeout information for this administrative session
> info — Displays various CLI information
> permissions — Displays the information about the user role

Sample Output

The following command shows information about the current CLI session.

```
username@hostname> show cli info
User                     : admin
Process ID               : 19510
Pager                    : enabled
Config Display Format    : default
Vsys configuration mode : enabled
Vsys                     : vsys1

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show clock

Shows the current time on the firewall.

Syntax

```
show clock {more}
```

Options

+ more — Displays dataplane time

Sample Output

The following command shows the current time.

```
username@hostname> show clock

Mon Jun 20 21:03:54 PDT 2011

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show collector-messages

(Panorama only) Displays log collector messages.

Syntax

```
show collector-messages collector <value> log-collector-group {default
   collector | <value>}
```

Options

* collector — Name of collector
* log-collector-group — Name of log collector group

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show commit-locks

Displays the list of administrators who hold commit locks.

Syntax

```
show commit-locks
```

Options

None

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show config

Displays the active configuration.

Syntax

```
show config
   {
   audit |
     {
     base-version <value> |
     base-version-no-deletes <value> |
     info |
     version <value>
     }
   candidate |
   diff |
   merged |
   pushed-shared-policy {vsys <value>} |
   pushed-template |
   running {xpath <value>} |
   saved <value> |
   synced
   }
```

Options

> audit — Displays config audit information
   > base-version — Base version to show
   > base-version-no-deletes — Version with no deletes to show
   > info — Audit information to show
   > version — Audit version to show
> candidate — Displays candidate configuration
> diff — Displays the differences between the running and candidate configurations
> merged — Displays pushed template and local config merge
> pushed-shared-policy — Displays shared policy pushed to the device
   + vsys — Virtual system to show
> pushed-template — Displays template pushed to the device
> running — Displays running configuration
   + xpath — XPath of the node to retrieve
> saved — Displays saved configuration
> synced — Displays configuration last synchronized with HA peer

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show config-locks

Displays the list of administrators who hold configuration locks.

Syntax

```
show config-locks
```

Options

None

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show counter

Displays system counter information.

Syntax

```
show counter
   {
   global |
      {
      filter |
         {
         aspect <value> |
         category <value> |
         delta {no | yes} |
         packet-filter {no | yes} |
         severity {drop | error | info | warn} |
         value {all | non-zero}
         }
      name
      }
   interface {all | management | <value>} |
   management-server
   }
```

Options

> global — Displays global system counter information
    > filter — Apply counter filters
        + aspect — Counter aspect
            aa — HA Active/Active mode
            arp — ARP processing
            dos — DoS protection
            forward — Packet forwarding
            ipfrag — IP fragment processing
            mgmt — Management-plane packet
            mld — MLD processing
            nd — ND processing
            offload — Hardware offload
            parse — Packet parsing
            pktproc — Packet processing
            qos — QoS enforcement
            resource — Resource management
            session — Session setup/teardown
            system — System function
            tunnel — Tunnel encryption/decryption
        + category — Counter category
            aho — AHO match engine
            appid — Application-Identification
            ctd — Content-Identification
            dfa — DFA match engine
            dlp — DLP

```
          flow — Packet processing
          fpga — FPGA
          ha — High-Availability
          log — Logging
          nat — Network Address Translation
          packet — Packet buffer
          proxy — TCP proxy
          session — Session management
          ssh — SSH termination
          ssl — SSL termination
          tcp — TCP reordering
          url — URL filtering
          zip — ZIP processing
       + delta — Difference from last read
       + packet-filter — Counters for packet that matches debug filter
       + severity — Counter severity
          drop — Drop
          error — Error
          info — Informational
          warn — Warning
       + value — value option
          all — All values
          non-zero — Non-zero only
    > name — Counter name (press <tab> for list)
> interface — Displays system counter information grouped by interface
    all — Show all interface counters
    management — Show management interface counter information
> management-server — Displays management server counter information
```

Sample Output

The following command displays all configuration counter information grouped according to interface.

```
username@hostname> show counter interface


hardware interface counters:
------------------------------------------------------------------------

interface: ethernet1/1
------------------------------------------------------------------------
bytes received                           0
bytes transmitted                        0
packets received                         0
packets transmitted                      0
receive errors                           0
packets dropped                          0
------------------------------------------------------------------------

...

username@hostname>
```

The following command displays all global counter information about the number of file forwards found.

```
username@hostname> show counter global name ctd_file_forward

Name:           ctd_file_forward
Value:          0
Severity:       Informational
Category:       ctd
Aspect:         pktproc
Description:     The number of file forward found

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show deployment-update-status

(Panorama only) Displays the deployment update schedule. For more information, refer to the *Panorama Administrator's Guide*.

Syntax

```
show deployment-update-schedule status name <value>
```

Options

> status — Indicates that status will be shown
>
> > name — Name of the dynamic update schedule (specify value)

Required Privilege Level

superuser, superuser (read only), Panorama admin

show device-messages

(Panorama only) Displays the policy messages for devices. For more information, refer to the *Panorama Administrator's Guide*.

Syntax

```
show device-messages device <value>
   {
   group <value> |
   template <value>
   }
```

Options

*device — Name of device
> group — Name of device group
> template — Name of temple

Sample Output

The following command shows the device messages for the device pan-mgmt2 and the group dg1.

```
username@hostname> show device-messages device pan-mgmt2 group dg1

username@hostname>
```

Required Privilege Level

superuser, superuser (read only), Panorama admin

show devicegroups

(Panorama only) Displays information about device groups. For more information, refer to the *Panorama Administrator’s Guide*.

Syntax

```
show devicegroups name <name>
```

Options

+ name — Displays the information for the specified device group

Sample Output

The following command shows information for the device group dg1.

```
username@hostname> show devicegroups name dg1
==========================================================================
Group: dg3 Shared policy md5sum:dfc61be308c23e54e5cde039689e9d46

Serial                   Hostname        IP              Connected
--------------------------------------------------------------------------
PA04070001               pan-mgmt2       10.1.7.2              yes
  last push state: push succeeded
  vsys3 shared policy md5sum:dfc61be308c23e54e5cde039689e9d46(In Sync)

username@hostname>
```

Required Privilege Level

superuser, superuser (read only), Panorama admin

show devices

(Panorama only) Shows the state of managed devices. For more information, refer to the *Panorama Administrator's Guide*.

Syntax

```
show device {all | connected}
```

Options

> all — Displays information for all managed devices
> connected — Displays information for all connected devices

Sample Output

The following command shows information for connected devices.

```
username@hostname> show devices connected

Serial                   Hostname        IP              Connected
--------------------------------------------------------------------------
PA04070001               pan-mgmt2       10.1.7.2              yes
  last push state:       none


username@hostname>
```

Required Privilege Level

superuser, superuser (read only), Panorama admin

show dhcp

Displays information about Dynamic Host Control Protocol (DHCP) leases.

Syntax

```
show dhcp
    {
    client state {all | <interface_name>} |
    server
      {
      lease {all | <interface_name>} |
      settings {all | <interface_name>}
      }
    }
```

Options

> client — Shows DHCP client runtime information
    all — Displays the client state information for all interfaces
    <interface_name> — Specifies an interface (ethernetn/m)
> server — Shows DHCP server runtime information
    > lease — Shows leases on one or all interfaces
    > settings — Shows settings on one or all interfaces

Sample Output

The following command shows the DHCP client state information for all interfaces.

```
username@hostname> show dhcp client state all

Interface       State        IP               Gateway          Leased-until
---------------------------------------------------------------------------
ethernet1/3     Selecting     0.0.0.0          0.0.0.0         0

username@hostname>
```

The following command shows the DHCP server settings for all interfaces.

```
username@hostname> show dhcp server settings all

Interface    GW            DNS1     DNS2     DNS-Suffix    Inherit source
---------------------------------------------------------------------------
ethernet1/11 10.100.1.1    0.0.0.0  0.0.0.0                ethernet1/3

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show dlc-query-state

(Panorama only) Displays the DLC query job state.

Syntax

```
show dlc-query-state id <value>
```

Options

<value> — Job ID value (1-4294967296)

Required Privilege Level

superuser, superuser (read only), Panorama admin

show dlc-query-ui

(Panorama only) Displays DLC query jobs.

Syntax

```
show dlc-query-ui id <value> skip <value>
```

Options

* id — Job ID (1-4294967296)
* skip — Skip logs for paging (0-1000)

Required Privilege Level

superuser, superuser (read only), Panorama admin

show dns-proxy

Displays information about the Domain Name Server (DNS) proxy.

Syntax

```
show dns-proxy
   {
   cache {all | name <value>} |
   settings {all | name <value>} |
   static-entries {all | name <value>} |
   statistics {all | name <value>}
   }
```

Options

> cache — DNS proxy cache
   > all — Displays all DNS proxy cache information
   > name — Displays cache information for the specified DNS proxy object
> settings — DNS proxy settings
   > all — Displays all DNS proxy settings
   > name — Displays settings for the specified DNS proxy object
> static-entries — DNS proxy static entries
   > all — Displays all DNS proxy static entries
   > name — Displays static entries for the specified DNS proxy object
> statistics — DNS proxy statistics
   > all — Displays all DNS proxy statistics
   > name — Displays statistics for the specified DNS proxy object

Sample Output

The following command displays all of the DNS proxy settings in the current session.

```
username@hostname> show dns-proxy settings all

Name: Nicks Proxy
Interfaces: ethernet1/10.1 ethernet1/10.2
Default name servers:  68.87.76.182  68.87.78.134
Status: Enabled
Match Rules:
backhaul to corporate dns:
  engineering.paloaltonetworks.com *.paloaltonetworks.local *.local
   10.0.0.2  10.0.0.3
My Company:
  *.mycompany.*
   11.11.11.253
--------------------------------------

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show dos-protection

Displays information about the Denial of Service (DoS) protection.

Syntax

```
show dos-protection
   {
   rule <name> |
     {
     settings |
     statistics
     }
   zone <name> blocked source
   }
```

Options

> rule — Displays settings and statistics about the specified rule
>
> > settings — Show settings
> >
> > statistics — Show statistics
>
> zone — Displays information about the specified zone

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show global-protect

Show GlobalProtect agent software download redirect setting.

Syntax

```
show global-protect redirect
```

Options

None

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show global-protect-gateway

Displays GlobalProtect gateway run-time objects.

Syntax

```
show global-protect-gateway
   {
   current-satellite {gateway <value> | satellite <value>} |
   current-user |
      {
      domain <value> |
      gateway <value> |
      user <value>
      }
   flow {name <value> | tunnel-id <value>} |
   flow-site-to-site {name <value> | tunnel-id <value>} |
   gateway {name <value> | type {remote-user | satellite}} |
   previous-satellite {gateway <value> | satellite <value>} |
   previous-user
      {
      domain <value> |
      gateway <value> |
      user <value>
      }
   }
```

Options

> current-satellite — Displays current GlobalProtect gateway satellites
    + gateway — Displays the given GlobalProtect gateway
    + satellite — Displays the satellites for which the satellite serial number starts with the string
> current-user — Displays current GlobalProtect gateway users
    + domain — Displays users for which the domain name starts with the string
    + gateway — Displays the given GlobalProtect gateway
    + user — Displays users for which the user name starts with the string
> flow — Displays data plane GlobalProtect gateway tunnel information
    > name — Displays the given GlobalProtect gateway tunnel
    > tunnel-id — Displays specific tunnel information (1-65535)
> flow-site-to-site — Displays dataplane GlobalProtect site-to-site gateway tunnel information
    > name — Displays the given GlobalProtect site-to-site gateway tunnel
    > tunnel-id — Displays specific tunnel information (1-65535)
> gateway — Displays list of GlobalProtect gateway configurations
    + name — Displays the given GlobalProtect gateway
    + type — Displays remote user or satellite
        - remote-user — Show only remote user gateway configuration
        - satellite — Show only satellite gateway configuration
> previous-satellite — Displays previous GlobalProtect gateway satellites
    + gateway — Displays the given GlobalProtect gateway
    + satellite — Displays the satellites for which the satellite serial number starts with the string
> previous-user — Displays previous user session for GlobalProtect gateway users
    + domain — Displays users which domain name start with the string

+ gateway — Displays the given GlobalProtect gateway
+ user — Displays the users for which the user name starts with the string

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show global-protect-mdm

Displays options for GlobalProtect Mobile Security Manager.

Syntax

```
show global-protect-mdm
   {
   state {all | <value>} |
   statistics
   }
```

Options

> state— Displays state of GlobalProtect servers
> statistics — Displays GlobalProtect statistics

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show global-protect-satellite

Displays GlobalProtect satellite run-time objects.

Syntax

```
show global-protect-satellite
   {
   current-gateway {gateway <value> | satellite <value>} |
   satellite name <value>
   }
```

Options

> current-gateway — Displays current GlobalProtect gateway connection infos
   + gateway — Displays gateway info for specified gateway (FQDN/IP address)
   + satellite — Displays for given GlobalProtect satellite instance
> satellite — Displays list of GlobalProtect satellite configuration
   + name — Displays for given GlobalProtect satellite

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show high-availability

Displays runtime information about the high availability subsystem.

Syntax

```
show high-availability
    {
    all |
    control-link statistics |
    dataplane-status |
    flap_statistics |
    ha2_keepalive |
    interface <interface_name> |
    link-monitoring |
    path-monitoring |
    slots |
    state |
    state-synchronization |
    transitions |
    virtual-address
    }
```

Options

> all — Displays high availability information
> control-link — Displays control link statistic information
> dataplane-status — Displays data plane runtime status
> flap-statistics — Displays high availability preemptive/non-functional flap statistics
> ha2_keepalive — Displays HA2 Keep-Alive statistics
> interface — Displays high availability interface information
> link-monitoring — Displays link monitoring state
> path-monitoring — Displays path monitoring statistics
> slots — Displays high availability slot information
> state — Displays high availability state information
> state-synchronization — Displays state synchronization statistics
> transitions — Displays high availability transition statistic information
> virtual-address — Displays the virtual addresses configured on the firewall in active-active high availability mode, summarizing the virtual IPs and virtual MACs according to the interface on which they are configured

Sample Output

The following command shows information for the high availability subsystem.

```
username@hostname> show high-availability path-monitoring

----------------------------------------------------------------------------
path monitoring:                                disabled
total paths monitored:                          0
----------------------------------------------------------------------------

username@hostname>
```

show hsm

Displays hardware security module (HSM) information.

Syntax

```
show hsm
   {
   client-address |
   ha-status |
   info |
   is-priv-key-on-hsm certificate-name <value> |
   nshield-connect-rfs |
   servers |
   slots |
   state
   }
```

Options

> client-address — Show HSM client ip address
> ha-status — Show HSM HA setting and members. Only valid for Luna SA
> info — Show HSM info
> is-priv-key-on-hsm— Query whether private key for a specified certificate is on HSM
> nshield-connect-rfs — Show nshield-connect RFS info. Only valid for nShield Connect
> servers — Show HSM registered servers
> slots — Show HSM slots
> state — Show HSM connection state

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show interface

Displays information about system interfaces.

Syntax

```
show interface <interface_name>
```

Options

all — Displays information for all ARP tables
ethernet*n/m* — Displays information for the specified interface
hardware — Displays all hardware interface information
logical — Displays all logical interface information
loopback — Displays loopback information
management — Displays management interface information
tunnel — Displays tunnel information
vlan — Displays VLAN information

Sample Output

The following command displays information about an aggregate Ethernet interface named ae3.

```
username@hostname> show interface ae3
----------------------------------------------------------------------------
Name: ae3, ID: 50
Link status:
  Runtime link speed/duplex/state: unknown/unknown/down
  Configured link speed/duplex/state: auto/auto/auto
MAC address:
  Port MAC address 00:1b:17:0b:de:32
Aggregate group members: 2
  ethernet1/5 ethernet1/6
Operation mode: layer3
Untagged sub-interface support: no
----------------------------------------------------------------------------
Name: ae3, ID: 50
Operation mode: layer3
Virtual router default
Interface MTU 1500
Interface IP address: 23.23.23.31/24
Interface management profile: ping
  ping: yes  telnet: no  ssh: no  http: no  https: no
  snmp: no  response-pages: no  userid-service: no
Service configured: LACP
Zone: trust, virtual system: vsys1
Adjust TCP MSS: no
----------------------------------------------------------------------------

Hardware interface counters read from CPU:
----------------------------------------------------------------------------
bytes received                           0
bytes transmitted                        0
packets received                         0
packets transmitted                      0
receive errors                           0
packets dropped                          0
----------------------------------------------------------------------------

Logical interface counters read from CPU:
----------------------------------------------------------------------------
bytes received                           0
bytes transmitted                        0
packets received                         0
packets transmitted                      0
receive errors                           0
packets dropped                          0
packets dropped by flow state check      0
forwarding errors                        0
no route                                 0
arp not found                            0
neighbor not found                       0
neighbor info pending                    0
mac not found                            0
packets routed to different zone         0
land attacks                             0
ping-of-death attacks                    0
teardrop attacks                         0
ip spoof attacks                         0
mac spoof attacks                        0
ICMP fragment                            0
layer2 encapsulated packets              0
layer2 decapsulated packets              0
----------------------------------------------------------------------------
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show jobs

Displays information about current system processes.

Syntax

```
show jobs {all | id <value> | pending | processed}
```

Options

> all — Displays information for all jobs
> id number — Identifies the process by number (1-4294967296)
> pending — Displays recent jobs that are waiting to be executed
> processed — Displays recent jobs that have been processed

Sample Output

The following command lists jobs that have been processed in the current session.

```
username@hostname> show jobs processed

Enqueued                   ID     Type Status Result Completed
--------------------------------------------------------------------------
2007/02/18 09:34:39         2  AutoCom    FIN     OK 2007/02/18 09:34:40
2007/02/18 09:33:00         1  AutoCom    FIN   FAIL 2007/02/18 09:33:54

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show lacp aggregate-ethernet

Shows the Link Aggregation Control Protocol (LACP) settings of an aggregate Ethernet group that has LACP enabled.

> ***Note:*** *To see information about the interfaces assigned to an aggregate Ethernet group, including whether LACP is enabled on the group, use the command "show interface" on page 489.*

Syntax

```
show lacp aggregate-ethernet <ae-group-name>
```

Options

<ae-group-name> — Specifies the name of the aggregate Ethernet group.

Sample Output

The following command shows information for an aggregate Ethernet group named ae1.

```
username@hostname> show lacp aggregate-ethernet ae1
LACP:
AE Group: ae1
Members :         bndl  rx state   mux state  sel state
   ethernet1/18  yes   Current    Tx_Rx       Selected
   ethernet1/19  yes   Current    Tx_Rx       Selected
   ethernet1/20  no    Defaulted  Detached   Unselected (cannot detect peer)

Status  : Enabled
Mode    : Active
Rate    : Fast
Local   : System Priority: 32768
          System MAC     : AC-DE-48-03-67-80
          Key            : 0001
Partner : System Priority: 00001
          System MAC     : AC-DE-48-03-FF-FF
          Key            : 0005
Port State   :
----------------------------------------------------------------------------

Interface      Port

            Number   Priority      Mode   Rate   Key   State

----------------------------------------------------------------------------

ethernet1/18    33     127      Active    Fast    49     0x3D
Partner         12     200      Passive   Slow     5     0x3C

ethernet1/19    34     127      Active    Fast    49     0x3D
Partner         13     201      Active    Fast     5     0x3D
```

```
ethernet1/20    35     127      Active    Fast    50     0x45
Partner          0       0      Passive   Slow     0     0x00

----------------------------------------------------------------------------

port Counters

----------------------------------------------------------------------------

Interface      LACPDUs   Marker   Marker response   Error

               Sent   Recv   Sent   Recv   Sent    Recv      Unknown Illegal
Ethernet1/18   2082   2189      0      0      0       0            0       0
Ethernet1/19     31     33      0      3      3       0            0       0
Ethernet1/20     22      0      0      0      0       0           15       2
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show location

Shows the geographic location of a firewall.

Syntax

```
show location ip <ip_address>
```

Options

<ip_address> — Specifies the IP address of the firewall (x.x.x.x or IPv6)

Sample Output

The following command shows location information for the firewall 10.1.1.1.

```
username@hostname> show location ip 10.1.1.1
show location ip 201.52.0.0
201.52.0.0

Brazil
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show log

Displays system logs.

Syntax

```
show log
   {
   alarm |
     {
     ack_admin equal <value> |
     admin equal <value> |
     csv-output equal {no | yes} |
     direction equal {backward | forward} |
     dport equal <port_number> |
     dst equal <ip/netmask> |
     end-time equal <value> |
     opaque contains <value> |
     receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
        days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
        day | last-calendar-month | last-hour} |
     rulegroup equal <value> |
     sport equal <port_number> |
     src equal <ip/netmask> |
     start-time equal <value> |
     time_acknowledged equal <value> |
     vsys equal <value> |
     }
   appstat |
     {
     csv-output equal {no | yes} |
     direction equal {backward | forward} |
     end-time equal <value> |
     name {equal | not-equal} <value> |
     query equal <value> |
     receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
        days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
        day | last-calendar-month | last-hour} |
     risk {equal | greater-than-or equal | less-than-or-equal | not-equal}
        {1 | 2 | 3 | 4 | 5} |
     start-time equal <value> |
     type {equal | not-equal} <value>
     }
   config |
     {
     client {equal | not-equal} {cli | web} |
     cmd {equal | not-equal} {add | clone | commit | create | delete | edit
        | get | load-from-disk | move | rename | save-to-diak | set}|
     csv-output equal {no | yes} |
     direction equal {backward | forward} |
     end-time equal <value> |
     query equal <value> |
     receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
        days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
        day | last-calendar-month | last-hour} |
     result {equal | not-equal} {failed | succeeded | unauthorized} |
     start-time equal <value>
     }
   dailythsum |
     {
     app {equal | not-equal} <value> |
     csv-output equal {no | yes} |
     direction equal {backward | forward} |
     dst in <value> |
     dstloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
        <value> |
     dstuser {equal | not-equal} <value> |
     end-time equal <value> |
     query equal <value> |
     receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
        days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
        day | last-calendar-month | last-hour} |
     rule {equal | not-equal} <value> |
     src in <value> |
     srcloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
        <value> |
     srcuser {equal | not-equal} <value> |
     start-time equal <value> |
     subtype {equal | not-equal} <value> |
     threatid {equal | greater-than-or-equal | less-than-or-equal | not-
        equal} <value>
     }
   dailytrsum |
     {
     app {equal | not-equal} <value> |
     csv-output equal {no | yes} |
     direction equal {backward | forward} |
     dst in <value> |
     dstloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
        <value> |
     dstuser {equal | not-equal} <value> |
     end-time equal <value> |
     query equal <value> |
     receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
        days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
        day | last-calendar-month | last-hour} |
     rule {equal | not-equal} <value> |
     src in <value> |
     srcloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
        <value> |
     srcuser {equal | not-equal} <value> |
     start-time equal <value>
     }
   data |
     {
     action {equal | not-equal} {alert | allow | block-url | deny | drop |
        drop-all-packets | reset-both | reset-client | reset-server |
        wildfire-upload-fail | wildfire-upload-skip | wildfire-upload-
        success} |
     app {equal | not-equal} <value> |
     category {equal | not-equal} <value> |
     csv-output equal {no | yes} |
     direction equal {backward | forward} |
     dport {equal | not-equal} <port_number> |
     dst {in | not-in} <ip/netmask> |
     dstuser equal <user_name> |
     end-time equal <value> |
     from {equal | not-equal} <value>
     query equal <value> |
     receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
        days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
        day | last-calendar-month | last-hour} |
     rule {equal | not-equal} <value> |
     sport {equal | not-equal} <port_number> |
     src {in | not-in} <ip/netmask> |
     srcuser equal <user_name> |
     start-time equal <value> |
     suppress-threatid-mapping equal {no | yes} |
     to {equal | not-equal} <value>
     }
  hipmatch |
     {
     direction equal {backward | forward} |
     machinename {equal | not-equal} <name> |
     matchname {equal | not-equal} <name> |
     matchtype {equal | not-equal} {object | profile} |
     query equal <value> |
     receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
        days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
        day | last-calendar-month | last-hour} |
     src {in | not-in} <ip/netmask> |
     srcuser equal <user_name>
     }
  hourlythsum |
     {
     app {equal | not-equal} <value> |
     csv-output equal {no | yes} |
     direction equal {backward | forward} |
     dst in <value> |
     dstloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
        <value> |
     dstuser {equal | not-equal} <value> |
     end-time equal <value> |
     query equal <value> |
     receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
        days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
        day | last-calendar-month | last-hour} |
     rule {equal | not-equal} <value> |
     src in <value> |
     srcloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
```

```
    <value> |
  srcuser {equal | not-equal} <value> |
  start-time equal <value> |
  subtype {equal | not-equal} <value> |
  threatid {equal | greater-than-or-equal | less-than-or-equal | not-
    equal} <value>
  }
hourlytrsum |
  {
  app {equal | not-equal} <value> |
  csv-output equal {no | yes} |
  direction equal {backward | forward} |
  dst in <value> |
  dstloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
    <value> |
  dstuser {equal | not-equal} <value> |
  end-time equal <value> |
  query equal <value> |
  receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
    days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
    day | last-calendar-month | last-hour} |
  rule {equal | not-equal} <value> |
  src in <value> |
  srcloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
    <value> |
  srcuser {equal | not-equal} <value> |
  start-time equal <value>
  }
iptag |
  {
  datasource_subtype {equal | not-equal} <value> |
  datasource_type {equal | not-equal} <value> |
  datasourcename {equal | not-equal} <value> |
  event_id {equal | not-equal} <value> |
  ip {in | not-in} <ip/netmask> |
  receive_time in <value> |
  tag_name {equal | not-equal} <value> |
  vsys equal <id> |
  }
mdm receive_time in <value> ||
system |
  {
  csv-output equal {no | yes} |
  direction equal {backward | forward} |
  end-time equal <value> |
  eventid {equal | not-equal} <value>
  id {equal | not-equal} <value>
  object {equal | not-equal} <value>
  opaque contains <value> |
  query equal <value> |
  receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
    days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
    day | last-calendar-month | last-hour} |
  severity {equal | greater-than-or equal | less-than-or-equal | not-
```

```
                  equal} {critical | high | informational | low | medium} |
               start-time equal <value> |
               subtype {equal | not-equal} <value>
               }
            threat |
               {
               action {equal | not-equal} {alert | allow | block-url | deny | drop |
                  drop-all-packets | reset-both | reset-client | reset-server} |
               app {equal | not-equal} <value> |
               category {equal | not-equal} <value> |
               csv-output equal {no | yes} |
               direction equal {backward | forward} |
               dport {equal | not-equal} <port_number> |
               dst {in | not-in} <ip/netmask> |
               dstuser equal <user_name> |
               end-time equal <value> |
               from {equal | not-equal} <value>
               query equal <value> |
               receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
                  days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
                  day | last-calendar-month | last-hour} |
               rule {equal | not-equal} <value> |
               sport {equal | not-equal} <port_number> |
               src {in | not-in} <ip/netmask> |
               srcuser equal <user_name> |
               start-time equal <value> |
               suppress-threatid-mapping equal {no | yes} |
               to {equal | not-equal} <value>
               }
            thsum |
               {
               app {equal | not-equal} <value> |
               csv-output equal {no | yes} |
               direction equal {backward | forward} |
               dst in <value> |
               dstloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
                  <value> |
               dstuser {equal | not-equal} <value> |
               end-time equal <value> |
               query equal <value> |
               receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
                  days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
                  day | last-calendar-month | last-hour} |
               rule {equal | not-equal} <value> |
               src in <value> |
               srcloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
                  <value> |
               srcuser {equal | not-equal} <value> |
               start-time equal <value> |
               subtype {equal | not-equal} <value> |
               threatid {equal | greater-than-or-equal | less-than-or-equal | not-
                  equal} <value>
               }
            traffic |
               {
               action {equal | not-equal} {allow | deny | drop} |
               app {equal | not-equal} <value> |
               csv-output equal {no | yes} |
               direction equal {backward | forward} |
               dport {equal | not-equal} <port_number> |
               dst {in | not-in} <ip/netmask> |
               dstuser equal <user_name> |
               end-reason equal {aged-out | decoder | tcp-fin | tcp-reuse | tcp-rst-
                  from-client | tcp-rst-from-server | policy-deny | threat |
                  resources-unavailable | unknown} |
               end-time equal <value> |
               from {equal | not-equal} <value>
               query equal <value> |
               receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
                  days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
                  day | last-calendar-month | last-hour} |
               rule {equal | not-equal} <value> |
               sport {equal | not-equal} <port_number> |
               src {in | not-in} <ip/netmask> |
               srcuser equal <user_name> |
               start-time equal <value> |
               to {equal | not-equal} <value>
               }
            trsum |
               {
               app {equal | not-equal} <value> |
               csv-output equal {no | yes} |
               direction equal {backward | forward} |
               dst in <value> |
               dstloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
                  <value> |
               dstuser {equal | not-equal} <value> |
               end-time equal <value> |
               query equal <value> |
               receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
                  days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
                  day | last-calendar-month | last-hour} |
               rule {equal | not-equal} <value> |
               src in <value> |
               srcloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
                  <value> |
               srcuser {equal | not-equal} <value> |
               start-time equal <value>
               }
            url |
               {
               action {equal | not-equal} {alert | allow | block-url | deny | drop |
                  drop-all-packets | reset-both | reset-client | reset-server} |
               app {equal | not-equal} <value> |
               category {equal | not-equal} <value> |
               csv-output equal {no | yes} |
               direction equal {backward | forward} |
               dport {equal | not-equal} <port_number> |
               dst {in | not-in} <ip/netmask> |
               dstuser equal <user_name> |
               end-time equal <value> |
               from {equal | not-equal} <value>
               query equal <value> |
               receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
                  days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
                  day | last-calendar-month | last-hour} |
               rule {equal | not-equal} <value> |
               sport {equal | not-equal} <port_number> |
               src {in | not-in} <ip/netmask> |
               srcuser equal <user_name> |
               start-time equal <value> |
               suppress-threatid-mapping equal {no | yes} |
               to {equal | not-equal} <value>
               }
            userid |
               {
               beginport {equal | not-equal} <value> |
               datasource equal {agent | captive-portal | event-log | ha | probing |
                  server-session-monitor | ts-agent | unknown | vpn-client | xml-api}
                  |
               datasourcename equal <value> |
               datasourcetype equal {authenticate | client-cert | directory-server |
                  exchange-server | globalprotect | kerberos | netbios-probing | ntlm
                  | unknown | vpn-client | wmi-probing} |
               direction equal {backward | forward} |
               endport {equal | not-equal} <value> |
               ip {in | not-in} <ip/netmask> |
               query equal <value> |
               receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
                  days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
                  day | last-calendar-month | last-hour} |
               user equal <user_name> |
               vsys equal <value>
               }
            weeklythsum |
               {
               app {equal | not-equal} <value> |
               csv-output equal {no | yes} |
               direction equal {backward | forward} |
               dst in <value> |
               dstloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
                  <value> |
               dstuser {equal | not-equal} <value> |
               end-time equal <value> |
               query equal <value> |
               receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
                  days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
                  day | last-calendar-month | last-hour} |
               rule {equal | not-equal} <value> |
               src in <value> |
               srcloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
                  <value> |
               srcuser {equal | not-equal} <value> |
               start-time equal <value> |
               subtype {equal | not-equal} <value> |
               threatid {equal | greater-than-or-equal | less-than-or-equal | not-
                  equal} <value>
               }
            weeklytrsum
               {
               app {equal | not-equal} <value> |
               csv-output equal {no | yes} |
               direction equal {backward | forward} |
               dst in <value> |
               dstloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
                  <value> |
               dstuser {equal | not-equal} <value> |
               end-time equal <value> |
               query equal <value> |
               receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
                  days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
                  day | last-calendar-month | last-hour} |
               rule {equal | not-equal} <value> |
               src in <value> |
               srcloc {equal | greater-than-or-equal | less-than-or-equal | not-equal}
                  <value> |
               srcuser {equal | not-equal} <value> |
               start-time equal <value>
               }
            wildfire |
               {
               action {equal | not-equal} {alert | allow | block-url | deny | drop |
                  drop-all-packets | reset-both | reset-client | reset-server} |
               app {equal | not-equal} <value> |
               category {equal | not-equal} <value> |
               csv-output equal {no | yes} |
               direction equal {backward | forward} |
               dport {equal | not-equal} <port_number> |
               dst {in | not-in} <ip/netmask> |
               dstuser equal <user_name> |
               end-time equal <value> |
               from {equal | not-equal} <value>
               query equal <value> |
               receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
                  days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
                  day | last-calendar-month | last-hour} |
               rule {equal | not-equal} <value> |
               sport {equal | not-equal} <port_number> |
               src {in | not-in} <ip/netmask> |
               srcuser equal <user_name> |
               start-time equal <value> |
               suppress-threatid-mapping equal {no | yes} |
               to {equal | not-equal} <value>
               }
            }
```

Options

> alarm — Displays alarm logs
  + ack_admin — Acknowledging admin name (alphanumeric string)
  + admin — Admin name (alphanumeric string)
  + csv-output — Equals CSV output (no or yes)
  + direction — Backward or forward direction
  + dport — Destination port (0-65535)
  + dst — Destination IP address (x.x.x.x/y or IPv6/netmask)
  + end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
  + opaque — Opaque contains substring value
  + receive_time — Receive time in the last specified time period (press <tab> for list)
  + rulegroup — Rule group equals rule value
  + sport — Source port (0-65535)
  + src — Source IP address (x.x.x.x/y or IPv6/netmask)
  + start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
  + time_acknowledged — Acknowledgement date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
  + vsys — Virtual system name
> appstat — Displays appstat logs
  + csv-output — Equals CSV output (no or yes)
  + direction — Backward or forward direction
  + end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
  + name — Equal or not equal to name value
  + query — Equal to query value
  + receive_time — Receive time in the last specified time period (press <tab> for list)
  + risk — Risk equal to, greater than or equal to, less than or equal to, or not equal to (1-5)
  + start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
  + type — Type equal to or not equal to value
> config — Displays config logs
  + client — Client equals or does not equal CLI or Web
  + cmd — Command equals or does not equal (press <tab> for list for commands)
  + csv-output — Equals CSV output (no or yes)
  + direction — Backward or forward direction
  + end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
  + query — Equal to query value
  + receive_time — Receive time in the last specified time period (press <tab> for list)
  + result — Result equals or does not equal failed, succeeded, or unauthorized
  + start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
> dailythsum — Displays daily thsum logs
  + app — Equals or does not equal value
  + csv-output — Equals CSV output (no or yes)
  + direction — Backward or forward direction
  + dst — Destination in value
  + dstloc — Destination equal to, greater than or equal to, less than or equal to, or not equal to value
  + dstuser — Equals or does not equal the value of the complete destination username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter **`abccorp\"mktnguser1`** as the value.
  + end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
  + query — Equal to query value
  + receive_time — Receive time in the last specified time period (press <tab> for list)
  + rule — Equals or does not equal rule value
  + src — Source in value

+ srcloc — Source equal to, greater than or equal to, less than or equal to, or not equal to value
+ srcuser — Equals or does not equal the value of the complete source username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter **`abccorp\"mktnguser1`** as the value.
+ start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
+ subtype — Equals or does not equal value
+ threatid — Equal to, greater than or equal to, less than or equal to, or not equal to value value

> dailytrsum — Displays daily trsum logs
+ app — Equals or does not equal value
+ csv-output — Equals CSV output (no or yes)
+ direction — Backward or forward direction
+ dst — Destination in value
+ dstloc — Destination equal to, greater than or equal to, less than or equal to, or not equal to value
+ dstuser — Equals or does not equal the value of the complete destination username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter **`abccorp\"mktnguser1`** as the value.
+ end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
+ query — Equal to query value
+ receive_time — Receive time in the last specified time period (press <tab> for list)
+ rule — Equals or does not equal rule value
+ src — Source in value
+ srcloc — Source equal to, greater than or equal to, less than or equal to, or not equal to value
+ srcuser + srcuser — Equals or does not equal valueEquals or does not equal the value of the complete source username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter **`abccorp\"mktnguser1`** as the value.
— Equals or does not equal value
+ start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)

> data — Displays data logs
+ action — Action equals or does not equal (press <tab> for list of actions)
+ app — Equals or does not equal value
+ category — URL category equals or does not equal (press <tab> for list of categories)
+ csv-output — Equals CSV output (no or yes)
+ direction — Backward or forward direction
+ dport — Destination port equals or does not equal (0-65535)
+ dst — Destination IP address in or not in (x.x.x.x/y or IPv6/netmask)
+ dstuser — Equals or does not equal the value of the complete destination username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter **`abccorp\"mktnguser1`** as the value.
+ end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
+ from — Equals or does not equal value
+ query — Equal to query value
+ receive_time — Receive time in the last specified time period (press <tab> for list)
+ rule — Equals or does not equal rule value
+ sport — Source port equals or does not equal (0-65535)
+ src — Source IP address in or not in (x.x.x.x/y or IPv6/netmask)
+ srcuser — Equals or does not equal the value of the complete source username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter **`abccorp\"mktnguser1`** as the value.
+ start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)

```
      + suppress-threatid-mapping — Suppress threat ID mapping (no or yes)
      + to — Equals or does not equal value
  > hipmatch — Displays host IP match logs
      + csv-output — Equals CSV output (no or yes)
      + machinename — Equals or does not equal machine name
      + matchname — Equals or does not equal match name
      + matchtype — Equals or does not equal object or profile
      + query — Equal to query value
      + receive_time — Receive time in the last specified time period (press <tab> for list)
      + src — Source IP address in or not in (x.x.x.x/y or IPv6/netmask)
      + srcuser — Equals or does not equal the value of the complete source username, including any specified
         domain name (the command doesn’t match partial username strings). If the username contains a double-
         quote character (“), you must escape the character. For example, if the username is
         abccorp"mktnguser1, enter abccorp\"mktnguser1 as the value.
  > hourlythsum — Displays hourly thsum logs
      + app — Equals or does not equal value
      + csv-output — Equals CSV output (no or yes)
      + direction — Backward or forward direction
      + dst — Destination in value
      + dstloc — Destination equal to, greater than or equal to, less than or equal to, or not equal to value
      + dstuser — Equals or does not equal the value of the complete destination username, including any specified
         domain name (the command doesn’t match partial username strings). If the username contains a double-
         quote character (“), you must escape the character. For example, if the username is
         abccorp"mktnguser1, enter abccorp\"mktnguser1 as the value.
      + end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
      + query — Equal to query value
      + receive_time — Receive time in the last specified time period (press <tab> for list)
      + rule — Equals or does not equal rule value
      + src — Source in value
      + srcloc — Source equal to, greater than or equal to, less than or equal to, or not equal to value
      + srcuser — Equals or does not equal the value of the complete source username, including any specified
         domain name (the command doesn’t match partial username strings). If the username contains a double-
         quote character (“), you must escape the character. For example, if the username is
         abccorp"mktnguser1, enter abccorp\"mktnguser1 as the value.
      + start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
      + subtype — Equals or does not equal value
      + threatid — Equal to, greater than or equal to, less than or equal to, or not equal to value value
  > hourlytrsum — Displays hourly trsum logs
      + app — Equals or does not equal value
      + csv-output — Equals CSV output (no or yes)
      + direction — Backward or forward direction
      + dst — Destination in value
      + dstloc — Destination equal to, greater than or equal to, less than or equal to, or not equal to value
      + dstuser — Equals or does not equal the value of the complete destination username, including any specified
         domain name (the command doesn’t match partial username strings). If the username contains a double-
         quote character (“), you must escape the character. For example, if the username is
         abccorp"mktnguser1, enter abccorp\"mktnguser1 as the value.
      + end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
      + query — Equal to query value
      + receive_time — Receive time in the last specified time period (press <tab> for list)
      + rule — Equals or does not equal rule value
      + src — Source in value
      + srcloc — Source equal to, greater than or equal to, less than or equal to, or not equal to value
      + srcuser — Equals or does not equal the value of the complete source username, including any specified
```

```
        domain name (the command doesn’t match partial username strings). If the username contains a double-
        quote character (“), you must escape the character. For example, if the username is
        abccorp"mktnguser1, enter abccorp\"mktnguser1 as the value.
    + start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
> iptag
    + datasource_subtype — Type of the datasource (equal or not equal to specified value)
    + datasource_type — Type of the datasource (equal or not equal to specified value)
    + datasourcename — Type of the datasource (equal or not equal to specified value)
    + event_id — Event ID (equal or not equal to specified value)
    + ip - IP subnet (in or not in specified subnet)
    + receive_time — Receive time (in the specified time period)
    + tag_name — Tag name (equal or not equal to the specified value)
    + vsys — Vsys ID (equal or equal to specified value)
> mdm receive_time —Displays log information for the specified time period.
> system — Displays system logs
    + csv-output — Equals CSV output (no or yes)
    + direction — Backward or forward direction
    + end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
    + eventid — Equals or does not equal value
    + id — Equals or does not equal value
    + object — Equals or does not equal value
    + opaque — Opaque contains substring value
    + query — Equal to query value
    + receive_time — Receive time in the last specified time period (press <tab> for list)
    + severity — Equal to, greater than or equal to, less than or equal to, or not equal to critical, high,
        informational, low, or medium
    + start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
    + subtype — Equal to subtype value
> threat — Displays threat logs
    + action — Action equals or does not equal (press <tab> for list of actions)
    + app — Equals or does not equal value
    + category — URL category equals or does not equal (press <tab> for list of categories)
    + csv-output — Equals CSV output (no or yes)
    + direction — Backward or forward direction
    + dport — Destination port equals or does not equal (0-65535)
    + dst — Destination IP address in or not in (x.x.x.x/y or IPv6/netmask)
    + dstuser — Equals or does not equal the value of the complete destination username, including any specified
        domain name (the command doesn’t match partial username strings). If the username contains a double-
        quote character (“), you must escape the character. For example, if the username is
        abccorp"mktnguser1, enter abccorp\"mktnguser1 as the value.
    + end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
    + from — Equals or does not equal value
    + query — Equal to query value
    + receive_time — Receive time in the last specified time period (press <tab> for list)
    + rule — Equals or does not equal rule value
    + sport — Source port equals or does not equal (0-65535)
    + src — Source IP address in or not in (x.x.x.x/y or IPv6/netmask)
    + srcuser — Equals or does not equal the value of the complete source username, including any specified
        domain name (the command doesn’t match partial username strings). If the username contains a double-
        quote character (“), you must escape the character. For example, if the username is
        abccorp"mktnguser1, enter abccorp\"mktnguser1 as the value.
    + start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
    + suppress-threatid-mapping — Suppress threat ID mapping (no or yes)
    + to — Equals or does not equal value
```

> thsum — Displays thsum logs
    + app — Equals or does not equal value
    + csv-output — Equals CSV output (no or yes)
    + direction — Backward or forward direction
    + dst — Destination in value
    + dstloc — Destination equal to, greater than or equal to, less than or equal to, or not equal to value
    + dstuser — Equals or does not equal the value of the complete destination username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter **`abccorp\"mktnguser1`** as the value.
    + end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
    + query — Equal to query value
    + receive_time — Receive time in the last specified time period (press <tab> for list)
    + rule — Equals or does not equal rule value
    + src — Source in value
    + srcloc — Source equal to, greater than or equal to, less than or equal to, or not equal to value
    + srcuser — Equals or does not equal the value of the complete source username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter **`abccorp\"mktnguser1`** as the value.
    + start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
    + subtype — Equals or does not equal value
    + threatid — Equal to, greater than or equal to, less than or equal to, or not equal to value value
> traffic — Displays traffic logs
    + action — Action equals or does not equal allow, deny, or drop
    + app — Equals or does not equal value
    + csv-output — Equals CSV output (no or yes)
    + direction — Backward or forward direction
    + dport — Destination port equals or does not equal (0-65535)
    + dst — Destination IP address in or not in (x.x.x.x/y or IPv6/netmask)
    + dstuser — Equals or does not equal the value of the complete destination username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter **`abccorp\"mktnguser1`** as the value.
    + end-reason — Session end reason (e.g., TCP FIN)
    + end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
    + from — Equals or does not equal value
    + query — Equal to query value
    + receive_time — Receive time in the last specified time period (press <tab> for list)
    + rule — Equals or does not equal rule value
    + sport — Source port equals or does not equal (0-65535)
    + src — Source IP address in or not in (x.x.x.x/y or IPv6/netmask)
    + srcuser — Equals or does not equal the value of the complete source username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter **`abccorp\"mktnguser1`** as the value.
    + start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
    + to — Equals or does not equal value
> trsum — Displays trsum logs
    + app — Equals or does not equal value
    + csv-output — Equals CSV output (no or yes)
    + direction — Backward or forward direction
    + dst — Destination in value
    + dstloc — Destination equal to, greater than or equal to, less than or equal to, or not equal to value

+ dstuser — Equals or does not equal the value of the complete destination username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter **`abccorp\"mktnguser1`** as the value.
+ end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
+ query — Equal to query value
+ receive_time — Receive time in the last specified time period (press <tab> for list)
+ rule — Equals or does not equal rule value
+ src — Source in value
+ srcloc — Source equal to, greater than or equal to, less than or equal to, or not equal to value
+ srcuser — Equals or does not equal the value of the complete source username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter **`abccorp\"mktnguser1`** as the value.
+ start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)

> url — Displays URL logs

+ action — Action equals or does not equal (press <tab> for list of actions)
+ app — Equals or does not equal value
+ category — URL category equals or does not equal (press <tab> for list of categories)
+ csv-output — Equals CSV output (no or yes)
+ direction — Backward or forward direction
+ dport — Destination port equals or does not equal (0-65535)
+ dst — Destination IP address in or not in (x.x.x.x/y or IPv6/netmask)
+ dstuser — Equals or does not equal the value of the complete destination username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter **`abccorp\"mktnguser1`** as the value.
+ end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
+ from — Equals or does not equal value
+ query — Equal to query value
+ receive_time — Receive time in the last specified time period (press <tab> for list)
+ rule — Equals or does not equal rule value
+ sport — Source port equals or does not equal (0-65535)
+ src — Source IP address in or not in (x.x.x.x/y or IPv6/netmask)
+ srcuser — Equals or does not equal the value of the complete source username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter **`abccorp\"mktnguser1`** as the value.
+ start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
+ suppress-threatid-mapping — Suppress threat ID mapping (no or yes)
+ to — Equals or does not equal value

> userid — Displays user ID logs

+ beginport — Source port equals or does not equal (1-65535)
+ datasource — Source of data (press <tab> for list)
+ datasourcename — Data source name
+ datasourcetype — Type of data source (press <tab> for list)
+ direction — Backward or forward direction
+ endport — Destination port equals or does not equal (0-65535)
+ ip — IP address in or not in (x.x.x.x/y or IPv6/netmask)
+ query — Equal to query value
+ receive_time — Receive time in the last specified time period (press <tab> for list)
+ user — Equals or does not equal the value of the complete username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter

abccorp\"mktnguser1 as the value.
+ vsys — Equals virtual system ID
> weeklythsum — Displays weekly thsum logs
+ app — Equals or does not equal value
+ csv-output — Equals CSV output (no or yes)
+ direction — Backward or forward direction
+ dst — Destination in value
+ dstloc — Destination equal to, greater than or equal to, less than or equal to, or not equal to value
+ dstuser — Equals or does not equal value
+ end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
+ query — Equal to query value
+ receive_time — Receive time in the last specified time period (press <tab> for list)
+ rule — Equals or does not equal rule value
+ src — Source in value
+ srcloc — Source equal to, greater than or equal to, less than or equal to, or not equal to value
+ srcuser — Equals or does not equal value
+ start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
+ subtype — Equals or does not equal value
+ threatid — Equal to, greater than or equal to, less than or equal to, or not equal to value value
> weeklytrsum — Displays weekly trsum logs
+ app — Equals or does not equal value
+ csv-output — Equals CSV output (no or yes)
+ direction — Backward or forward direction
+ dst — Destination in value
+ dstloc — Destination equal to, greater than or equal to, less than or equal to, or not equal to value
+ dstuser — Equals or does not equal the value of the complete destination username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **abccorp"mktnguser1**, enter **abccorp\"mktnguser1** as the value.
+ end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
+ query — Equal to query value
+ receive_time — Receive time in the last specified time period (press <tab> for list)
+ rule — Equals or does not equal rule value
+ src — Source in value
+ srcloc — Source equal to, greater than or equal to, less than or equal to, or not equal to value
+ srcuser — Equals or does not equal the value of the complete source username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **abccorp"mktnguser1**, enter **abccorp\"mktnguser1** as the value.
+ start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
> wildfire — Displays Wildfire logs
+ action — Action equals or does not equal (press <tab> for list of actions)
+ app — Equals or does not equal value
+ category — URL category equals or does not equal (press <tab> for list of categories)
+ csv-output — Equals CSV output (no or yes)
+ direction — Backward or forward direction
+ dport — Destination port equals or does not equal (0-65535)
+ dst — Destination IP address in or not in (x.x.x.x/y or IPv6/netmask)
+ dstuser — Equals or does not equal the value of the complete destination username, including any specified domain name (the command doesn't match partial username strings). If the username contains a double-quote character ("), you must escape the character. For example, if the username is **abccorp"mktnguser1**, enter **abccorp\"mktnguser1** as the value.
destination user name
+ end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)

+ from — Equals or does not equal value
+ query — Equal to query value
+ receive_time — Receive time in the last specified time period (press <tab> for list)
+ rule — Equals or does not equal rule value
+ sport — Source port equals or does not equal (0-65535)
+ src — Source IP address in or not in (x.x.x.x/y or IPv6/netmask)
+ srcuser — Equals or does not equal the value of the complete source username, including any specified domain name (the command doesn’t match partial username strings). If the username contains a double-quote character (“), you must escape the character. For example, if the username is **`abccorp"mktnguser1`**, enter **`abccorp\"mktnguser1`** as the value.
+ start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
+ suppress-threatid-mapping — Suppress threat ID mapping (no or yes)
+ to — Equals or does not equal value

Sample Output

The following command shows the configuration log.

```
username@hostname> show log config
Time                Host            Command   Admin      Client Result
============================================================================
03/05 22:04:16 10.0.0.135      edit      admin     Web     Succeeded
03/05 22:03:22 10.0.0.135      edit      admin     Web     Succeeded
03/05 22:03:22 10.0.0.135      create    admin     Web     Succeeded
03/05 21:56:58 10.0.0.135      edit      admin     Web     Succeeded
...

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show log-collector

Displays information about the device log collector.

Syntax

```
show log-collector
   {
   all |
   connected |
   detail |
   hints |
   serial-number <value> |
   stats
     {
     runtime interval-type <value> ld <value> segment <value> {active-
        segments {no | yes}} |
     storage ld <value> segment <value> {active-segments {no | yes}}
     }
   }
```

Options

> all — All managed log collectors
> connected — All connected log collectors
> detail — Log collector details
> hints — Show the hints stored on this Log collector
> serial-number — Log collector serial number
> stats — Log collector statistics
   > runtime — Show runtime statistics
      + active-segments — Only display active segments
      * interval-type — Interval for the statistics, in minutes
      * ld — Logical disk number (1-4)
      * segment — Segment ID (all or 0-25)
   > storage — Show Storage statistics
      + active-segments — Only display active segments
      * ld — Logical disk number (1-4)
      * segment — Segment ID (all or 0-25)

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show log-collector-group

Displays information about log collector groups.

Syntax

```
show log-collector-group
    {
    all |
    from ring-name {default | <name>} |
    name {default | <name>}
    }
```

Options

> all — All managed log Collector Groups
> from ring-name — Displays the following information about the Log Collectors in the named Collector Group: serial number, IPv4 address, IPv6 address, disk size, number of segments, and identifiers for the RAID disk pairs (Vld Id).
> name — Log Collector Group name

Sample Output

The following command displays information about the default log collector group.

```
username@hostname> show log-collector-group name default

Group: default
     Ring version 4  updated at 2012/04/25 18:07:12
     Sent to log collectors at ?
     Last pushed ring version 4
     Min retention period 30
     Total disk capacity 1863 GB
     Last commit-all:       none updated at ?
     Devices in the group:
          Device 001606000100
               Log collector pref list 003001000017
          Device 001606000112
               Log collector pref list 003001000014
          Device 0008C100105
               Log collector pref list 003001000014


Log collectors in the group:

Serial           Hostname             IP              Connected    sw version
----------------------------------------------------------------------------
003001000014     AviaryPanorama       12.3.45.670     yes          5.0

Last commit-all: commit succeeded, current ring version 4
md5sum 1945b1f04eef6d29045648a8075b6e49 updated at ?


Serial           Hostname             IP              Connected    sw version
```

```
----------------------------------------------------------------------------
003001000017     M-100                12.3.456.70     yes          5.0

Last commit-all: commit succeeded, current ring version 4
md5sum 1262fa4e81e3ded4a1fe7ed4997c400a updated at ?
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show logging-status

Displays information about log forwarding for each CMS.

Syntax

```
show logging-status
```

Options

None

Sample Output

The following command reports all available log forwarding statistics.

```
username@hostname> show logging-status

Type        Last Log fwded        Last SeqNo. fwded     Last Log Received
CMS 0
    config        Not Available                       0         Not Available
    system        Not Available                       0         Not Available
    threat   2011/06/20 18:03:44                1606507   2011/06/20 18:03:17
   traffic   2011/06/20 23:23:46                6020338   2011/06/20 23:23:19
  hipmatch        Not Available                       0         Not Available

CMS 1
        Not Sending to CMS 1

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show mac

Displays MAC address information.

Syntax

```
show mac {all | <value>}
```

Options

all — Displays all MAC information
<value> — Displays specified VLAN MAC information (dot1q-vlan name)

Sample Output

The following command lists all currently MAC address information.

```
username@hostname> show mac all

maximum of entries supported :      8192
default timeout :                   1800 seconds
total MAC entries in table :        4
total MAC entries shown :           4
status: s - static, c - complete, i - incomplete
vlan                hw address        interface         status   ttl
---------------------------------------------------------------------------
Vlan56              0:0:1:0:0:3       ethernet1/5         c      1087
Vlan56              0:0:1:0:0:4       ethernet1/6         c      1087
Vlan11-12           0:0:1:0:0:9       ethernet1/12        c      487
Vlan11-12           0:0:1:0:0:10      ethernet1/11        c      487

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show management-clients

Shows information about internal management server clients.

Syntax

```
show management-clients
```

Options

None

Sample Output

The following command shows information about the internal management server clients.

```
username@hostname> show management-clients

              Client PRI    State Progress
-------------------------------------------------------------------------
              routed 30    P2-ok      100
              device 20    P2-ok      100
              ikemgr 10    P2-ok      100
              keymgr 10     init        0    (op cmds only)
               dhcpd 10    P2-ok      100
            ha_agent 10    P2-ok      100
             npagent 10    P2-ok      100
            exampled 10     init        0    (op cmds only)

Overall status: P2-ok. Progress: 0
Warnings:
Errors:
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show migration-log

Shows the migration log file.

Syntax

```
show migration-log
```

Options

None

Sample Output

The following command displays the migration log file.

```
username@hostname> show migration-log
```

```
[TBS]
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show neighbor

Displays IPv6 neighbor information.

Syntax

```
show neighbor {all | mgt | <interface_name>}
```

Options

all — Displays all IPv6 neighbor information
mgt — Displays host IPv6 neighbor information
<interface_name> — Displays IPv6 neighbor information for the specified interface

Sample Output

The following command displays all of the IPv6 neighbor information.

```
username@hostname> show neighbor all

maximum of entries supported :      1000
default base reachable time:        30 seconds
total neighbor entries in table :   0
total neighbor entries shown :      0

interface         ip address        hw address        status
----------------------------------------------------------------------------

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show ntp

Displays the Network Time Protocol (NTP) synchronization state.

Syntax

```
show ntp
```

Options

None

Sample Output

The following command displays the NTP synchronization state.

```
username@hostname> show ntp

NTP state:
    NTP synched to LOCAL

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show object

Shows the name of an address object with an IP address that exactly matches the address specified in the filter.

Syntax

```
show object
   {
   dynamic-address-group {all | name <value>} |
   registered-address {all option {count | file} | ip <ip/netmask> | tag
     <value>} |
   static ip <address> {vsys <name>}
   }
```

Options

> dynamic-address-group — Dynamic address object
   > all — Shows all dynamic address objects
   > name — Shows the dynamic address objects for the specified name
> registered-address — Lists registered IP addresses
   > all — Shows all registered addresses
   > ip — Shows the registered address that matches the specific IP address
   > tag — Shows the register address that matches the specified tag
> static — IP to object name
   + vsys — Specifies the virtual system
   * ip — Specifies the IP address (x.x.x.x or IPv6)

Sample Output

The following command shows the name of an address object, “one-more,” with IP address 3.3.3.3 that exists in virtual system “vsys1.”

```
username@hostname> show object static vsys vsys1 ip 3.3.3.3

one-more
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show operational-mode

Displays the device operational mode (normal, fips, or cc).

Syntax

```
show operational-mode
```

Options

None

Sample Output

The following command shows the device operational mode.

```
username@hostname> show operational-mode

normal
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show panorama-certificates

Lists certificate information for connection between the firewall and Panorama. Primarily used for debugging purposes.

Syntax

```
show panorama-certificates
```

Options

None

Sample Output

The following command shows that the firewall has a Panorama certificate key file “client.pem.”

```
username@hostname> show panorama-certificates
-rw-r--r-- 1 root root 5.8K Oct 15  2010 client.pem

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show panorama-status

Shows the Panorama connection status.

Syntax

```
show panorama-status
```

Options

None

Sample Output

The following command shows information about the Panorama connection.

```
username@hostname> show panorama-status

Panorama Server 1 : 10.1.7.90
State : Unknown

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show pbf

Displays runtime statistics for policy-based forwarding (PBF).

Syntax

```
show pbf
    {
    return-mac {all | name <name>} |
    rule {all | name <rule_name>}
    }
```

Options

> return-mac — PBF return MAC info
    all — Displays all current return MAC information
    > name — Displays the runtime statistics for a specified return MAC
> rule — PBF rule status
    > all — Displays information about all current policy-based forwarding rules
    > name — Displays the runtime statistics for a specified policy-based forwarding rule

Sample Output

The following command shows the current PBF settings.

```
username@hostname> show pbf rule all

Rule       ID    State    R-Action Egress IF    NextHop          Interval
    Threshold Status M-Action  KA sent KA got Packets Matched
========== ===== ======== ======== ============ ================ ========
    ========= ====== ========= ======= ====== ===============
r1        4    Normal  Discard            0.0.0.0        0       0       UP
    Monitor  0      0      0
to-host    7    Normal  Forward  ethernet1/1  100.1.1.254      2       3
    UP    Fail-Over 1270    1270  0
to-tunnel  8    Normal  Forward  ethernet1/3  201.1.1.254      2       3
    DOWN  Fail-Over 23      23    2
r5         9    Normal  Forward  ethernet1/9  0.0.0.0         2       3
    UP    Fail-Over 0      0      3

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show pppoe

Displays statistics about the Point-to-Point Protocol over Ethernet (PPPoE) connections. The firewall can be configured to be a PPPoE termination point to support connectivity in a Digital Subscriber Line (DSL) environment where there is a DSL modem but no other PPPoE device to terminate the connection.

Syntax

```
show pppoe interface {all | <interface_name>}
```

Options

all — Displays PPPoE information for all interfaces
<interface_name> — Displays PPPoE information for the specified firewall interface

Sample Output

The following command shows PPPoE information for the ethernet1/4 interface.

```
username@hostname> show pppoe interface ethernet1/4
Interface   PPPoE      PPP State    Username Access Concentrator MAC IP
ethernet1/4 Initiating Disconnected pa4020   Access Concentrator 00:11:22:33:44:55 10.0.2.2
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show qos

Shows Quality of Service (QoS) runtime information.

Syntax

```
show qos
   {
   interface <interface> |
   counter |
   match-rule |
   throughput <value> |
   tunnel-throughput <value>
   }
```

Options

+ interface — Specifies the QoS interface
> counter — Displays software-based QoS counters
> match-rule — Displays members of regular traffic configuration
> throughput — Displays throughput (last 3 seconds) of all classes under the specified node-ID ((0-65535)
> tunnel-throughput — Displays throughput (last 3 seconds) of all classes under the specified tunnel interface

Sample Output

The following command shows the QoS throughput for interface ethernet1/2, node default-group (ID 0):

```
username@hostname> show qos interface ethernet1/2 throughput 0
QoS throughput for interface ethernet1/2, node default-group (Qid 0):
class 4:      362 kbps
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show query

Displays information about query jobs.

Syntax

```
show query {id <value> | jobs}
```

Options

> id — Displays job information for the specified ID (1-4294967296)
> jobs — Displays all job information

Sample Output

The following command shows information about all current query jobs.

```
username@hostname> show query jobs
Enqueued          ID Last Upd
--------------------------------------------------------------------------
13:58:19          16 13:58:19

    Type         ID Dequeued?
-----------------------------------------------------
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show report

Displays information about process jobs.

Syntax

```
show report
   {
   custom |
     {
     aggregate-fields equal <value> |
     database equal {appstat | threat | thsum | traffic | trsum} |
     query equal <value> |
     receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
        days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
        day | last-calendar-month | last-hour} |
     topn equal <value> |
     value-fields equal <value>
     }
   directory-listing |
   id <value> |
   jobs |
   predefined name equal {top-applications | top-attackers | top-attackers-
     by-countries | top-attacks | top-connections | top-denied-applications
     | top-denied-destinations | top-denied-sources | top-destination-
     countries | top-destinations | top-egress-interfaces | top-egress-zones
     | top-http-applications | top-ingress-interfaces | top-ingress-zones |
     top-rules | top-source-countries | top-sources | top-spyware-threats |
     top-url-categories | top-url-user-behavior | top-url-users | top-
     victims | top-victims-by-countries | top-viruses | top-vulnerabilities
     | top-websites | unknown-tcp-connections | unknown-udp-connections}
     {
     end-time <value> |
     start-time <value> |
     }
   }
```

Options

> custom — Displays custom reports
  + aggregate-fields — Report with comma-separated aggregate field names
  + database — Data base report (appstat, threat, thsum, traffic, or trsum)
  + query — Report formulated with the query string value
  + receive_time — Report with the receive time in the specified time period (press <tab> for list)
  + topn — Report of TopN return results
  + value-fields — Report with comma-separated value field names
> directory-listing — Displays report of directory listings
> id — Displays reports by ID (1-4294967296)
> jobs — Reports all jobs
> predefined — Displays predefined reports
  + end-time — End date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
  + start-time — Start date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)

* name — Predefined report of the specified name (press <tab> for list)

Sample Output

The following command shows the pre-defined report “top-applications.”

```
username@hostname> show report predefined name equal top-applications
<?xml version="1.0"?>
<report reportname="top-applications" logtype="appstat">
  <result name="Top applications" logtype="appstat" start="2011/01/01 0
0:00:00" start-epoch="1293868800" end="2011/01/01 23:59:59" end-epoch="
1293955199" generated-at="2011/01/02 17:22:47" generated-at-epoch="1294
017767" range="Saturday, January 01, 2011">
    <entry>
      <name>icmp</name>
      <nbytes>0</nbytes>
      <nsess>480</nsess>
    </entry>
    <entry>
      <name>ospf</name>
      <nbytes>3920</nbytes>
      <nsess>20</nsess>
    </entry>
    <entry>
      <name>ping</name>
      <nbytes>172</nbytes>
      <nsess>2</nsess>
    </entry>
  </result>
</report>

username@hostname>
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show resource

Displays resource limits for policies, sessions, SSL VPN tunnels, and VPN tunnels.

Syntax

```
show resource limit {policies | session | ssl-vpn | vpn}
```

Options

> policies — Displays the resource limit for policies
> session — Displays the resource limit of the session
> ssl-vpn — Displays the resource limit for SSL VPN tunnels
> vpn — Displays the resource limit for site-to-site VPN tunnels

Sample Output

The following command shows the session resource limit.

```
username@hostname> show resource limit session

current session   max session
----------------- -----------------
3044              262143

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show routing

Displays routing run-time objects.

Syntax

```
show routing
   {
   fib {virtual-router <name>} |
   interface |
   multicast |
     {
     fib |
        {
        group <ip/netmask> |
        interface <value> |
        source <ip/netmask> |
        virtual-router <value>
        }
     group-permission |
        {
        interface <value> |
        virtual-router <value>
        }
     igmp |
        {
        interface {virtual-router <value>} |
        membership {interface <value> | virtual-router <value>} |
        statistics {interface <value>}
        }
     pim |
        {
        elected-bsr |
        group-mapping {group <ip/netmask> | virtual-router <value>} |
        interface {virtual-router <value>} |
        neighbor {virtual-router <value>} |
        state |
           {
           group <ip/netmask> |
           interface <value> |
           rpt-only {no | yes} |
           source {any | <ip/netmask>} |
           virtual-router <value>
           }
        statistics {interface <value> | neighbor <ip/netmask>}
        }
     route
        {
        group <ip/netmask> |
        interface <value> |
        source <ip/netmask> |
        virtual-router <value>
```

```
      }
   }
protocol |
   {
   bgp |
      {
      loc-rib {nexthop <ip/netmask> | peer <value> | prefix <ip/netmask> |
         virtual-router <value>} |
      loc-rib-detail {nexthop <ip/netmask> | peer <value> | prefix <ip/
         netmask> | virtual-router <value>} |
      peer {peer-name <value> | virtual-router <value>} |
      peer-group {group-name <value> | virtual-router <value>} |
      policy {aggregate | cond-adv | export | import} {virtual-router
         <value>} |
      rib-out {nexthop <ip/netmask> | peer <value> | prefix <ip/netmask> |
         virtual-router <value>} |
      rib-out-detail {nexthop <ip/netmask> | peer <value> | prefix <ip/
         netmask> | virtual-router <value>} |
      summary {virtual-router <value>}
      }
   ospf |
      {
      area {virtual-router <value>} |
      dumplsdb {virtual-router <value>} |
      graceful-restart {virtual-router <value>} |
      interface {virtual-router <value>} |
      lsdb {virtual-router <value>} |
      neighbor {virtual-router <value>} |
      summary {virtual-router <value>} |
      virt-link {virtual-router <value>} |
      virt-neighbor {virtual-router <value>}
      }
   ospfv3 |
      {
      area {virtual-router <value>} |
      dumplsdb {virtual-router <value>} |
      graceful-restart {virtual-router <value>} |
      interface {virtual-router <value>} |
      lsdb {virtual-router <value>} |
      neighbor {virtual-router <value>} |
      summary {virtual-router <value>} |
      virt-link {virtual-router <value>} |
      virt-neighbor {virtual-router <value>}
      }
   redist |
      {
      all {virtual-router <value>} |
      bgp {virtual-router <value>} |
      ospf {virtual-router <value>} |
      rip {virtual-router <value>}
      }
   rip
      {
      database {virtual-router <value>} |
      interface {virtual-router <value>} |
      peer {virtual-router <value>} |
      summary {virtual-router <value>}
      }
   }
resource |
route |
   {
   destination <ip/netmask>|
   interface <interface_name> |
   nexthop <ip/netmask> |
   type {bgp | connect | ospf | rip | static} |
   virtual-router <name>
   }
summary {virtual-router <name>}
}
```

Options

> fib — Displays Forwarding Information Base (FIB) entries (option to filter result by virtual router)
> interface — Displays interface status
> multicast — Displays multicast routing protocol information
    > fib — Displays multicast Forwarding Information Base (FIB) entries
        + group — Filters result by multicast group address (IP address and network mask)
        + interface — Filters result by incoming interface (interface name)
        + source — Filters result by multicast source address (IP address and network mask)
        + virtual-router — Filters result by virtual-router (router name)
    > group-permission — Displays multicast group permission
        + interface — Filters result by incoming interface (interface name)
        + virtual-router — Filters result by virtual-router (router name)
    > igmp — Displays Internet Group Management Protocol (IGMP) information
        > interface — Displays IGMP enabled interface status (option to filter result by virtual router)
        > membership — Displays IGMP membership information (options to filter result by interface or virtual router)
        > statistics — Displays IGMP statistics (option to display statistics for specified IGMP interfaces)
    > pim — Displays Protocol Independent Multicast (PIM) information
        > elected-bsr — Displays address of elected bootstrap router (BSR)
        > group-mapping — Displays PIM group-rp mapping (options to filter result by group or virtual router)
        > interface — Displays PIM enabled interface status (option to filter result by virtual router)
        > neighbor — Displays PIM neighbor information (option to filter result by virtual router)
        > state — Displays current PIM multicast tree state
            + group — Filters result by multicast group address
            + interface — Displays interface specific states
            + rpt-only — Displays only RPT states
            + source — Displays (S, G) or (S, G, ...) states
            + virtual-router — Filters result by virtual-router
        > statistics — Displays PIM statistics (options to filter result by interface or neighbor)
    > route — Displays multicast route entries
        + group — Filters result by multicast group address (IP address and network mask)
        + interface — Filters result by incoming interface (interface name)
        + source — Filters result by multicast source address (IP address and network mask)
        + virtual-router — Filters result by virtual-router (router name)
> protocol — Displays dynamic routing protocol information
    > bgp — Displays Border Gateway Protocol (BGP) information

```
  > loc-rib — Displays BGP Local Routing Information Base (Loc-RIB)
    + nexthop — Filters result by nexthop (x.x.x.x/y or IPv6/netmask)
    + peer — Displays for given BGP peer
    + prefix — Filters result by prefix (x.x.x.x/y or IPv6/netmask)
    + virtual-router — Filters result by virtual router
  > loc-rib-detail — Displays BGP Local Routing Information Base (Loc-RIB) details
    + nexthop — Filters result by nexthop (x.x.x.x/y or IPv6/netmask)
    + peer — Displays for given BGP peer
    + prefix — Filters result by prefix (x.x.x.x/y or IPv6/netmask)
    + virtual-router — Filters result by virtual router
  > peer — Displays BGP peer status
    + peer-name — Displays for given BGP peer
    + virtual-router — Filters result by virtual router
  > peer-group — Displays BGP peer group status
    + group-name — Displays for given BGP peer group
    + virtual-router — Filters result by virtual router
  > policy — Displays BGP route-map status
    + virtual-router — Filters result by virtual router
    > aggregate — Displays BGP aggregate policy
    > cond-adv — Displays BGP conditional advertisement policy
    > export — Displays BGP export policy
    > import — Displays BGP import policy
  > rib-out — Displays BGP routes sent to BGP peer
    + nexthop — Filters result by nexthop (x.x.x.x/y or IPv6/netmask)
    + peer — Displays for given BGP peer
    + prefix — Filters result by prefix (x.x.x.x/y or IPv6/netmask)
    + virtual-router — Filters result by virtual router
  > rib-out-detail — Displays BGP routes sent to BGP peer
    + nexthop — Filters result by nexthop (x.x.x.x/y or IPv6/netmask)
    + peer — Displays for given BGP peer
    + prefix — Filters result by prefix (x.x.x.x/y or IPv6/netmask)
    + virtual-router — Filters result by virtual router
  > summary — Displays BGP summary information
    + virtual-router — Filters result by virtual router
> ospf — Displays Open Shortest Path First (OSPF) information
  > area — Displays OSPF area status
    + virtual-router — Filters result by virtual router
  > dumplsdb — Displays OSPF LS database status with all details
    + virtual-router — Filters result by virtual router
  > interface — Displays OSPF interface status
    + virtual-router — Filters result by virtual router
  > lsdb — Displays OSPF LS database status
    + virtual-router — Filters result by virtual router
  > neighbor — Displays OSPF neighbor status
    + virtual-router — Filters result by virtual router
  > summary — Displays OSPF summary information
    + virtual-router — Filters result by virtual router
  > virt-link — Displays OSPF virtual link status
    + virtual-router — Filters result by virtual router
  > virt-neighbor — Displays OSPF virtual neighbor status
    + virtual-router — Filters result by virtual router
> ospfv3 — Displays OSPFv3 information
  > area — Displays OSPFv3 area status
    + virtual-router — Filters result by virtual router
```

```
            > dumplsdb — Displays OSPFv3 LS database status with all details
               + virtual-router — Filters result by virtual router
            > graceful-restart — Displays OSPFv3 graceful restart status
               + virtual-router — Filters result by virtual router
            > interface — Displays OSPFv3 interface status
               + virtual-router — Filters result by virtual router
            > lsdb — Displays OSPFv3 LS database status
               + virtual-router — Filters result by virtual router
            > neighbor — Displays OSPFv3 neighbor status
               + virtual-router — Filters result by virtual router
            > summary — Displays OSPFv3 summary information
               + virtual-router — Filters result by virtual router
            > virt-link — Displays OSPFv3 virtual link status
               + virtual-router — Filters result by virtual router
            > virt-neighbor — Displays OSPF virtual neighbor status
               + virtual-router — Filters result by virtual router
         > redist — Displays redistribution rule entries
            > all — Displays all redist rules
               + virtual-router — Filters result by virtual router
            > bgp — Displays only BGP redist rules
               + virtual-router — Filters result by virtual router
            > ospf — Displays only OSPF redist rules
               + virtual-router — Filters result by virtual router
            > rip — Displays only RIP redist rules
               + virtual-router — Filters result by virtual router
         > rip — Displays Routing Information Protocol (RIP) information
            > database — Displays RIP route database
               + virtual-router — Filters result by virtual router
            > interface — Displays RIP interface status
               + virtual-router — Filters result by virtual router
            > peer — Displays RIP peer status
               + virtual-router — Filters result by virtual router
            > summary — Displays RIP summary information
               + virtual-router — Filters result by virtual router
      > resource — Displays resource usage
      > route — Displays route entries
         + destination — Filters result by destination network and mask (x.x.x.x/y or IPv6/netmask)
         + interface — Filters result by network interface
         + nexthop — Filters result by nexthop network and mask (x.x.x.x/y or IPv6/netmask)
         + type — Filters result by type of routes (BGP, connect and host, OSPF, RIP, or static)
         + virtual-router — Filters result by virtual router
      > summary — Displays summary information
         + virtual-router — Filters result by virtual router
```

Sample Output

The following command shows summary routing information for the virtual router vrl.

```
username@hostname> show routing summary virtual-router vr1

VIRTUAL ROUTER: vr1 (id 1)
==========
OSPF
area id:                     0.0.0.0
```

```
interface:                 192.168.6.254
interface:                 200.1.1.2
dynamic neighbors:
IP 200.1.1.1 ID 200.1.1.1
area id:                     1.1.1.1
interface:                 1.1.1.1
interface:                 1.1.2.1
interface:                 1.1.3.1
interface:                 2.1.1.1
static neighbor:         IP 65.54.5.33 ID *down*
static neighbor:         IP 65.54.77.88 ID *down*
interface:                 22.22.22.22
interface:                 35.1.15.40
interface:                 192.168.7.254
dynamic neighbors:
IP 35.1.15.1 ID 35.35.35.35
==========
RIP
interface:                   2.1.1.1
interface:                   22.22.22.22
interface:                   35.1.15.40
interface:                   192.168.6.254
interface:                   200.1.1.2
==========
INTERFACE
==========
interface name:                ethernet1/1
interface index:               16
virtual router:                vr1
operation status:              up
IPv4 address:                  22.22.22.22/24
IPv4 address:                  35.1.15.40/24
==========
interface name:                ethernet1/3
interface index:               18
virtual router:                vr1
operation status:              up
IPv4 address:                  200.1.1.2/24
==========
interface name:                ethernet1/7
interface index:               22
virtual router:                vr1
operation status:              up
IPv4 address:                  1.1.1.1/24
IPv4 address:                  1.1.2.1/24
IPv4 address:                  1.1.3.1/24
==========
interface name:                ethernet1/15
interface index:               30
virtual router:                vr1
operation status:              up
IPv4 address:                  192.168.6.254/24
==========
interface name:                ethernet1/16
interface index:               31
virtual router:                vr1
operation status:              up
IPv4 address:                  192.168.7.254/24
==========
interface name:                ethernet1/18
interface index:               33
virtual router:                vr1
operation status:              down
IPv4 address:                  2.1.1.1/24

username@hostname>
```

The following command shows dynamic routing protocol information for RIP.

```
username@hostname> show routing protocol rip summary

==========
virtual router:                vr1
reject default route:          yes
interval seconds:              1
update intervals:              30
expire intervals:              180
delete intervals:              120
interface:                   2.1.1.1
interface:                   22.22.22.22
interface:                   35.1.15.40
interface:                   192.168.6.254
interface:                   200.1.1.2
==========
virtual router:                newr
reject default route:          yes
interval seconds:              1
update intervals:              30
expire intervals:              180
delete intervals:              120
interface:                   0.0.0.0
interface:                   30.30.30.31
interface:                   151.152.153.154
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show rule-use

Displays used and non-used policy rules.

Syntax

```
show rule-use
   {
   device-group <value> |
   rule-base {app-override | cp | decryption | nat | pbf | qos | security} |
   type used
   }
```

Options

* device-group — Displays information for the specified device group
* rule-base — Rule base category
   app-override — Application override policy
   cp — Captive portal policy
   decryption — SSL decryption policy
   nat — Network Address Translation (NAT) policy
   pbf — Policy based forwarding (PBF) policy
   qos — Quality of service (QOS) policy
   security — Security policy
* type — Rule use type (used)

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show running

Displays running operational parameters.

Syntax

```
show running
   {
   appinfo2ip |
   application {cache | setting | statistics} |
   application-override-policy |
   application-signature statistics |
   captive-portal-policy |
   decryption-policy |
   dos-policy |
   global-ippool |
   ippool |
   ipv6 {address} |
   logging |
   nat-policy |
   nat-rule-cache |
   nat-rule-ippool rule <name> {show-cache {no | yes} | show-freelist {no |
     yes}} |
   pbf-policy |
   qos-policy |
   resource-monitor {day | hour | minute | second | week} {last <value>} |
   rule-use rule-base {app-override | cp | decryption | dos | nat | pbf | qos
     | security} type {unused | used} vsys <name> |
   security-policy |
   ssl-cert-cn |
   tcp state |
   top-urls {category <value> | top <value>} |
   ts-agent-data {all | ip <ip/netmask> | source-user <value>} |
   tunnel flow |
     {
     all |
        {
        filter state {active | inactive | init} |
        filter type {ipsec | sslvpn}
        }
     context <value> |
     info |
     lookup |
     name <tunnel_name> |
     nexthop |
     operation-stats |
     tunnel-id <value>
     }
   url <value> |
   url-cache {all | statistics} |
   url-info <value> |
   url-license
```

```
      }
```

Options

```
> appinfo2ip — Displays application-specific IP mapping information
> application — Displays application info (cache, setting, or statistics)
> application-override-policy — Displays currently deployed application override policy
> application-signature — Displays application signature statistics
> captive-portal-policy — Displays currently deployed captive-portal policy
> decryption-policy — Displays currently deployed decryption policy
> dos-policy — Displays currently deployed DoS policy
> global-ippool — Displays global IP pool status
> ippool — Displays IP pool usage
> ipv6 — Displays IPv6 information (option to show IPv6 addresses)
> logging — Displays log and packet logging rate
> nat-policy — Displays currently deployed Network Address Translation (NAT) policy
> nat-rule-cache — Displays all NAT rules of all versions in cache
> nat-rule-ippool — Displays specified NAT rule ippool usage
    + show-cache — Displays reserve time cache
    + show-freelist — Displays free list
    * rule — Specifies NAT rule name
> pbf-policy — Displays currently deployed Policy-Based Forwarding policy
> qos-policy — Displays currently deployed QoS policy
> resource-monitor — Displays resource monitoring statistics
    > day — Per-day monitoring statistics (last 1-7 days)
    > hour — Per-hour monitoring statistics (last 1-24 hours)
    > minute — Per-minute monitoring statistics (last 1-60 minutes)
    > second — Per-second monitoring statistics (last 1-60 seconds)
    > week — Per-week monitoring statistics (last 1-13 weeks)
> rule-use — Displays used/non-used policy rules
    * rule-base — Rule base name
        app-override — Application override policy
        cp — Captive portal policy
        decryption — SSL decryption policy
        dos — DoS protection policy
        nat — NAT policy
        pbf — Policy-based Forwarding policy
        qos — QoS policy
        security — Security policy
    * type — Rule use type (unused or used)
    * vsys — Virtual system name
> security-policy — Displays currently deployed security policy
> ssl-cert-cn — Displays SSL certificate common name cache
> tcp — Displays TCP reassembly setup
> top-urls — Displays top URLs statistics (for BrightCloud only)
    + category — Specify the URL category
    + top — First top elements (1-10000)
> ts-agent-data — Displays terminal server agent data
    > all — Displays all terminal server agents data
    > ip — Displays terminal server agent data for IP address (x.x.x.x/y or IPv6/netmask)
    > source-user — Displays terminal server agent data for user
> tunnel — Displays runtime tunnel states
    > all — Displays all tunnels
        + filter — Specifies filters
            + state — Tunnel state (active, inactive, initial state)
            + type — Tunnel type (IPSec or SSL-VPN tunnel)
```

> context — Displays encap/decap context (1-65535)
> info — Displays runtime statistics
> lookup — Displays runtime lookup structures
> name — Displays tunnel name
> nexthop — Displays nexthop resolution structures
> operation-stats — Displays tunnel setup/teardown/update operation statistics
> tunnel-id — Displays tunnel id (1-65535)
> url — Displays the category of the URL in the URL cache (for the Palo Alto Networks URL filtering database only)
> url-cache — Displays all URLs in the URL cache (for the Palo Alto Networks URL filtering database only)
> all — Displays all URLs in the URL cache
> statistics — Displays URL cache statistics
> url-info — Displays categorization details of the URL as in the URL cache
> url-license — Displays URL license information

Sample Output

The following command shows statistics for running applications.

```
username@hostname> show running application statistics

Time: Wed Feb 17 15:16:30 2010
Vsys: 1
Number of apps: 31
App (report-as) sessions   packets    bytes        app changed threats
--------------- ---------- ---------- ------------ ----------- -------
15              495        188516     99646149     0           0
16              11         1803       1319859      0           0
32              464        467        51055        0           3
36              518        16395      1921997      0           0
37              2          2574       273600       0           0
42              1888       4101       454433       0           0
44              1          1          422          1           0
48              29         686        225194       0           0
50              2          7          2741         0           0
79              2          185        97363        2           0
86              9          115        25843        8           0
109             1604       75513      55339483     0           0
147             155        374        33660        0           0
193             0          3          1018         1           0
225             12         272        71706        12          0
280             77         217        44906        0           0
318             48         85         30161        0           0
452             2          139        109886       2           0
453             1          9          1914         1           0
491             21         1293       812870       21          0
518             128        98192      96499118     128         0
658             6          70         18944        6           0
674             53         1487       1122891      53          0
735             8          8446       8385474      8           0
796             1          16         4215         1           0
852             1          117        87965        1           0
872             49         2852       2296433      49          0
900             24         2206       1179538      24          0
980             32         573        233308       32          0
1019            412        2679       200506       0           0
1024            913        6971       549052       0           0
```

```
--------------- ---------- ---------- ------------ ----------- -------
Total           6968       416364     271041704    350         3

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show session

Displays session information.

Syntax

```
show session
   {
   all |
     {
     filter
        {
        application <name> |
        count {no | yes} |
        destination  <ip_address> |
        destination-port  <port_number> |
        destination-user {known-user | unknown | <value>} |
        egress-interface  <value> |
        from <zone> |
        hw-interface <value> |
        ingress-interface <value> |
        min-kb <value> |
        nat {both | destination | none | source} |
        nat-rule <rule_name> |
        pbf-rule <rule_name> |
        protocol <value> |
        qos-class <value> |
        qos-node-id <value> |
        qos-rule <rule_name> |
        rematch security-policy |
        rule <rule_name> |
        source <ip_address> |
        source-port <port_number> |
        source-user {known-user | unknown | <value>} |
        ssl-decrypt {no | yes} |
        start-at <value> |
        state {active | closed | closing | discard | initial | opening} |
        to <zone> |
        type {flow | predict} |
        vsys-name <name>
        }
     start-at <value>
     }
   id <number> |
   info |
   meter
   rematch
   }
```

Options

> all — Displays active sessions

+ filter — Apply show session filter
    + application — Application name (press <tab> for list)
    + count — Count number of sessions only (no or yes)
    + destination — Destination IP address (x.x.x.x or IPv6)
    + destination-port — Destination port (1-65535)
    + destination-user — Destination user (known-user, unknown, or enter a value)
    + egress-interface — Egress interface
    + from — From zone
    + hw-interface — Hardware interface
    + ingress-interface — Ingress interface
    + min-kb — Minimum KB of byte count (1-1048576)
    + nat — If session is NAT (both, destination, none, or source)
    + nat-rule — NAT rule name
    + pbf-rule — Policy-based Forwarding rule name
    + protocol — IP protocol value (1-255)
    + qos-class — QoS class (1-8)
    + qos-node-id — QoS node ID value (0-5000; -2 = bypass mode)
    + qos-rule — QoS rule name
    + rematch — Rematch sessions (security policy)
    + rule — Security rule name
    + source — Source IP address (x.x.x.x or IPv6)
    + source-port — Source port (1-65535)
    + source-user — Source user (known-user, unknown, or enter a value)
    + ssl-decrypt — Session is decrypted (no or yes)
    + start-at — Show next 1K sessions (1-2097152)
    + state — Flow state (active, closed, closing, discard, initial, or opening)
    + to — To zone
    + type — Flow type (regular flow or predict)
    + vsys-name — Virtual system name
+ start-at   Show next 1K sessions (1-2097152)

> id — Displays specific session information (1-2147483648), such as the session end reason. Note that the PA-4000 Series platforms will show a “0” value in the `total byte count (s2c)` and `layer 7 packet count (s2c)` fields due to a platform limitation.

> info — Displays session statistics

> meter — Displays session metering statistics

> rematch — Used to show the statistics of the most recent session rematch processes when session rematch is enabled (set device config setting config rematch yes). The rematch process rematches all existing sessions against the updated policy rulebase when a new configuration is committed. The purpose of this option is to make sure that if a policy is changed to remove access to a given application, all current sessions will be ended.

Sample Output

The following command displays session statistics.

```
username@hostname> show session info
--------------------------------------------------------------------------------
number of sessions supported:                   524287
number of active sessions:                      498520
number of active TCP sessions:                  0
number of active UDP sessions:                  498518
number of active ICMP sessions:                 0
number of active BCAST sessions:                0
number of active MCAST sessions:                0
number of predict sessions:                     0
```

```
session table utilization:                      95%
number of sessions created since system bootup: 3072041
Packet rate:                                    0/s
Throughput:                                     0 Kbps
New connection establish rate:                  0 cps
-------------------------------------------------------------------------------
session timeout
  TCP default timeout:                          3600 seconds
  TCP session timeout before 3-way handshaking:    5 seconds
  TCP session timeout after FIN/RST:              30 seconds
  UDP default timeout:                          3600 seconds
  ICMP default timeout:                            6 seconds
  other IP default timeout:                       30 seconds
  Session timeout in discard state:
    TCP: 90 seconds, UDP: 60 seconds, other IP protocols: 60 seconds
-------------------------------------------------------------------------------
session accelerated aging:                      enabled
  accelerated aging threshold:                  80% of utilization
  scaling factor:                               2 X
-------------------------------------------------------------------------------
session setup
  TCP - reject non-SYN first packet:            yes
  hardware session offloading:                  yes
  IPv6 firewalling:                             no
-------------------------------------------------------------------------------
application trickling scan parameters:
  timeout to determine application trickling:   10 seconds
  resource utilization threshold to start scan: 80%
  scan scaling factor over regular aging:       8
-------------------------------------------------------------------------------
```

The following command lists statistics for the specified session.

```
username@hostname> show session id 371731
session     371731
        c2s flow:
                source:   172.16.40.20[L3Intranet]
                dst:      84.72.62.7
                sport:    49230         dport:    31162
                proto:    17            dir:      c2s
                state:    ACTIVE        type:     FLOW
                ipver:    4
                src-user: qa2003domain-b\kwisdom
                dst-user: unknown
                PBF rule: rule4(2)
                qos node: ethernet1/14, qos member N/A Qid 0
                ez fid:   0x0d208003(13, 0, 0, 3)
        s2c flow:
                source:   84.72.62.7[L3Extranet]
                dst:      172.16.40.20
                sport:    31162         dport:    49230
                proto:    17            dir:      s2c
                state:    ACTIVE        type:     FLOW
                ipver:    4
                src-user: unknown
                dst-user: qa2003domain-b\kwisdom
                ez fid:   0x0ca0703f(12, 2, 3, 63)
        start time            : Fri Jan 15 15:55:56 2010
        timeout               : 1200 sec
```

```
time to live          : 1076 sec
total byte count      : 145
layer7 packet count   : 0
vsys                  : vsys1
application           : bittorrent
rule                  : rule23
session to be logged at end      : yes
session in session ager          : yes
session sync'ed from HA peer     : yes
layer7 processing                : completed
URL filtering enabled            : yes
URL category                     : any
ingress interface                : ethernet1/13
egress interface                 : ethernet1/14
session QoS rule                 : default (class 4)
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show sslmgr-store

Displays the store for the Secure Socket Layer (SSL) manager that validates certificates for the Certificate Revocation List (CRL) and the Online Certificate Status Protocol (OCSP). Each trusted certificate authority (CA) maintains CRLs to determine if an SSL certificate is valid (not revoked) for SSL decryption. The OCSP can also be used to dynamically check the revocation status of a certificate.

Syntax

```
show sslmgr-store
   {
   certificate-info |
      {
      issuer <value> |
      portal {db-serialno <value> | name <value> | serialno <value>}
      }
   config-ca-certificate |
      {
      publickey-hash <value> |
      subjectname-hash <value>
      }
   config-certificate-info |
         {
         db-serialno <value> |
         issuer-subjectname-hash <value>
         }
   satellite-info |
      {
      portal
         {
         name <value> |
         serialno <value> |
         state {assigned | unassigned}
         }
   serialno-certificate-info {db-serialno <value>}
   }
```

Options

> certificate-info — Displays list of certificate status
    > issuer — Show all certificate status information signed by issuing entity
    > portal — GlobalProtect portal
        + db-serialno — Certificate serial number
        + name — shows certificate status for given GlobalProtect portal
        + serialno — GlobalProtect satellite serial number
> config-ca-certificate — Displays list of config CA certificate
    + publickey-hash — Certificate public key hash (sha1)
    + subjectname-hash — Certificate subject name hash (sha1)
> config-certificate-info — Displays list of config certificate status
    + db-serialno — Certificate serial number
    + issuer-subjectname-hash — Issuer subject name hash (sha1)
> satellite-info — Displays list of registered satellites

```
    + portal — GlobalProtect portal
        + name — Shows satellite info for given GlobalProtect portal
        + serialno — GlobalProtect satellite serial number
        + state — Satellite info assigned or unassigned
            - assigned — Satellite info assigned
            - unassigned — Satellite info unassigned
> serialno-certificate-info — Displays list of certificate status from certificate serial number
    > db-serialno — Certificate serial number
```

Required Privilege Level

superuser, vsysadmin

show statistics

Displays firewall statistics.

Syntax

```
show statistics
```

Options

None

Sample Output

The following command displays firewall statistics.

```
username@hostname> show statistics

  TASK   PID N_PACKETS  CONTINUE     ERROR      DROP    BYPASS TERMINATE
     0     0         0         0         0         0         0         0
     1   806   6180587   6179536        39         0         0      1012
     2   807     39312     37511         0         0         0      1801
     3   808 176054840 173273080      2289   2777524         0      1947
     4   809 112733251 111536151      1744   1194906         0       450
     5   810  66052142  65225559      1271    825010         0       302
     6   811  49682445  49028991       909    652227         0       318
     7   812  43618777  43030638       712    587129         0       298
     8   813  41255949  40706957       708    548031         0       253
     9   814  42570163  42010404       714    558773         0       272
    10   815   7332493   7332494         0         0         0         0
task  1(pid:    806) flow_mgmt
task  2(pid:    807) flow_ctrl flow_host
task  3(pid:    808) flow_lookup flow_fastpath flow_slowpath flow_forwarding
    flow_np
task  4(pid:    809) flow_lookup flow_fastpath flow_slowpath flow_forwarding
    flow_np
task  5(pid:    810) flow_lookup flow_fastpath flow_slowpath flow_forwarding
    flow_np
task  6(pid:    811) flow_lookup flow_fastpath flow_slowpath flow_forwarding
    flow_np
task  7(pid:    812) flow_lookup flow_fastpath flow_slowpath flow_forwarding
    flow_np
task  8(pid:    813) flow_lookup flow_fastpath flow_slowpath flow_forwarding
    flow_np
task  9(pid:    814) flow_lookup flow_fastpath flow_slowpath flow_forwarding
    flow_np
task 10(pid:    815) appid_result
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show system

Displays system-related information.

Syntax

```
show system
   {
   disk-space |
   environmentals {fans | fan-tray | power | power-supply | slot <value> |
     thermal} |
   files |
   info |
   logdb-quota |
   masterkey-properties |
   packet-path-test status {slot <value>} |
   raid detail |
   resources {follow} |
   services |
   setting |
     {
     ctd |
        {
        state |
        threat {application <value> | id <value> | profile <value>} |
        url-block-cache
        }
     jumbo-frame |
     logging |
     multi-vsys |
     packet |
     pow |
     shared-policy |
     ssl-decrypt {certificate | certificate-cache | exclude-cache | memory
        {detail} | notify-cache | setting} |
     target-vsys |
     template |
     url-cache {all | statistics} |
     url-database |
     url-filtering-feature |
     util |
     zip
     }
   software status {slot <value>}|
   state {browser | filter | filter-pretty} |
   statistics {application vsys <name> | session}
   }
```

Options

> disk-space — Reports file system disk space usage
> environmentals — Displays system environment state (fan-tray, fans, power, power-supply, slot, thermal)

> files — Lists important files in the system
> info — Displays system information
> log-summary status — Reports time of last generated thsum and trsum logs
> logdb-quota — Reports log data base quotas
> masterkey-properties — Displays Master key expiry and reminders times
> packet-path-test — Displays packet path monitoring information
>> resources — Displays system resources
> services — Displays system services
> setting — Displays system settings
  > ctd — Displays ctd settings
    > state — Displays ctd configure state
    > threat — Displays threat stats (application, id, or profile) (0-4294967295)
    > url-block-cache — Displays url block cache
  > jumbo-frame — Displays Jumbo-Frame mode
  > logging — Displays log and packet logging rate
  > multi-vsys — Displays multiple virtual system mode
  > packet — Displays system packet settings
  > pow — Displays pow (verifies if wqe inuse is enabled)
  > shared-policy — Displays shared policy status
  > ssl-decrypt — Displays SSL decryption
    > certificate — Displays SSL decryption certificate
    > certificate-cache — Displays SSL decryption certificate cache
    > exclude-cache — Displays SSL decryption exclude cache
    > memory — Displays SSL decryption memory usage (option to show detail)
    > notify-cache — Displays SSL decryption notify cache
    > setting — Displays SSL decryption settings
  > target-vsys — Displays target virtual system for operational commands
  > template — Displays template status
  > url-cache — Displays URL cache statistics
  > url-database — Displays URL database
  > url-filtering-feature — Displays URL filtering feature settings
  > util — Displays utility settings
  > zip — Shows whether the firewall is configured to decompress files within traffic for content scanning purposes
> software — Displays software information
> state — Displays system state
  > browser — Navigate in a text-mode browser
  > filter — Filter by subtree/wildcard
  > filter-pretty — Filter by subtree/wildcard with pretty printing
> statistics — Displays system statistics
  > application — Displays application statistics for the specified virtual system
  > session — Displays statistics for the session

Sample Output

The following command displays system information.

```
username@hostname> show system info

hostname: thunder
ip-address: 10.1.7.1
netmask: 255.255.0.0
default-gateway: 10.1.0.1
ipv6-address:
ipv6-default-gateway:
```

```
mac-address: 00:13:72:3c:c9:e3

time: Tue Feb  9 10:02:57 2010

uptime: 0 days, 0:00:00
family: 4000
model: thunder
serial: 06081420000021
sw-version: 4.0.0-c758.dev
vpnclient-package-version: 1.0.0-c10
app-version: 158-450
av-version: 0
threat-version: 0
url-filtering-version: 2216
logdb-version: 3.0.0

username@hostname>
```

The following command shows an example with the default threat action.

```
username@hostname> show system setting ctd threat 100000 application 109
    profile 1
Profile 1 appid 109 , action 0
action 0 means “default” action.
username@hostname>
```

The following command displays log database quotas and disk usage.

```
username@hostname> show system logdb-quota
Quotas:
             traffic: 32.00%, 14.650 GB
              threat: 16.00%, 7.325 GB
              system: 4.00%, 1.831 GB
              config: 4.00%, 1.831 GB
               alarm: 3.00%, 1.373 GB
               trsum: 12.00%, 5.494 GB
         hourlytrsum: 2.00%, 0.916 GB
          dailytrsum: 2.00%, 0.916 GB
         weeklytrsum: 2.00%, 0.916 GB
               thsum: 4.00%, 1.831 GB
        hourlythsum: 2.00%, 0.916 GB
          dailythsum: 2.00%, 0.916 GB
         weeklythsum: 2.00%, 0.916 GB
             appstat: 12.00%, 5.494 GB
   application-pcaps: 1.00%, 0.458 GB
        threat-pcaps: 1.00%, 0.458 GB
  debug-filter-pcaps: 1.00%, 0.458 GB
            dlp-logs: 1.00%, 0.458 GB
Disk usage:
traffic: Logs: 12G, Index: 2.9G
threat: Logs: 21M, Index: 560K
system: Logs: 90M, Index: 11M
config: Logs: 112K, Index: 512K
alarm: Logs: 8.0K, Index: 8.0K
trsum: Logs: 379M, Index: 57M
hourlytrsum: Logs: 379M, Index: 57M
```

```
dailytrsum: Logs: 379M, Index: 57M
weeklytrsum: Logs: 379M, Index: 57M
thsum: Logs: 76K, Index: 252K
hourlythsum: Logs: 76K, Index: 252K
dailythsum: Logs: 76K, Index: 252K
weeklythsum: Logs: 76K, Index: 252K
appstatdb: Logs: 11M, Index: 5.5M
application-pcaps: 670M
threat-pcaps: 5.7M
debug-filter-pcaps: 4.0M
dlp-logs: 5.0M
```

The following command displays the times of the last generated thsum and trsum logs.

```
username@hostname> show system log-summary status
hourlytrsum: last generated 2011/01/23 12:00:10
dailytrsum: last generated 2011/01/23 00:00:20
weeklytrsum: last generated 2011/01/23 00:00:30

hourlythsum: last generated 2011/01/23 12:00:12
dailythsum: last generated 2011/01/23 00:00:23
weeklythsum: last generated 2011/01/23 00:00:35
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show templates

(Panorama only) Displays defined templates.

Syntax

```
show templates name <value>
```

Options

name — Specifies the template name

Sample Output

The following command shows template configurations.

```
username@hostname> show template name name

[TBS]


username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show threat

Displays threat ID descriptions.

Syntax

```
show threat id <value>
```

Options

<value> — Specifies the threat ID (1-4294967296)

Sample Output

The following command shows threat ID descriptions for ID 11172.

```
username@hostname> show threat id 11172
This signature detects the runtime behavior of the spyware MiniBug. MiniBug,
    also known as Weatherbug, installs other spyware, such as WeatherBug, and
    My Web Search Bar. It is also adware program that displays advertisements
    in its application window.

medium

http://www.spywareguide.com/product_show.php?id=2178

http://www.spyany.com/program/article_spw_rm_Minibug.htm

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show url-cloud

Displays the URL cloud status.

Syntax

```
show url-cloud status
```

Options

None

Sample Output

The following command displays the status for the URL cloud.

```
username@hostname> show url-cloud status

PAN-DB URL Filtering
License :                          valid
Current cloud server :             s0200.urlcloud.paloaltonetworks.com
Cloud connection :                 connected
URL database version - device :    2012.03.22.182
URL database version - cloud :    2012.03.22.182  ( last update time 2012/03/
    23 11:2
0:22 )
URL database status :              good
URL protocol version - device :    pan/0.0.2
URL protocol version - cloud :     pan/0.0.2
Protocol compatibility status :    compatible

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show user

Displays user identification information. You can show information for a specified IP address, user, or all.

Syntax

```
show user
   group |
     {
     list |
        + xmlapi
        | {except <value>| match <value>}
     name <value>}
     }
   group-mapping |
     {
     naming-context server {<ip/netmask> | <host_name>} |
        {
        is-active-directory {no | yes} |
        proxy-agent {<ip/netmask> | <host_name>} |
        proxy-agent-port <value> |
        server-port <value> |
        use-ssl {no | yes}
        }
     state {all | <value>} |
     statistics
     }
   group-mapping-service |
     {
     query {all | local | remote} |
     status
     }
   group-selection server {<ip/netmask> | <host_name>} |
     {
     base <value> |
     bind-dn <value> |
     bind-password <value> |
     container-object <value> |
     filter <value> |
     force {no | yes} |
     group-object <value> |
     name-attribute <value> |
     proxy-agent {<ip/netmask> | <host_name>} |
     proxy-agent-port <value> |
     search-scope {one | subtree} |
     server-port <value> |
     use-ssl {no | yes}
     }
   ip-port-user-mapping {all | ip <ip/netmask> | source-user <value>} |
   ip-user-mapping |
        {
     option {count | detail} |
     type { AD | CP | EDIR | GP | NTLM | SSL/VPN | UIA | UNKNOWN | XMLAPI} |
     all |
     ip <ip/netmask>
     }
   ip-user-mapping-mp |
     {
     no-group-only {no | yes} |
     option {count | detail} |
     type { AD | CP | EDIR | GP | NTLM | SSL/VPN | UIA | UNKNOWN | XMLAPI} |
     all |
     ip <ip/netmask>
     }
   local-user-db |
     {
     disabled {no |yes} |
     username <name> |
     vsys <name>
     }
   server monitor |
     {
     auto-discover {domain | except <value>| match <value>} |
     state {all | <name>}|
     statistics | {except | match}
     }
   ts-agent statistics |
     {
     state {all | <value>} |
     statistics
     }
   user-IDs {match-user <value>} |
   user-id-agent |
     {
     config name <value> |
     state {all | <name>} |
     statistics
     }
   user-id-service
     {
     client {all | <ip/port>} |
     status
     }
   xml-api multiusersystem
   }
```

Options

> group — Displays user groups data
    > list — Lists all groups
        +xml_api— Lists groups from XML API
    > name — Displays group's members
> group-mapping — Displays group mapping states
    > naming-context — Displays naming context for directory server

```
        + is-active-directory — Server is active directory
        + proxy-agent — Agent IP address or host name
        + proxy-agent-port — User ID agent listening port (1-65535, default is 5007)
        + server-port — LDAP server listening port (1-65535)
        + use-ssl — Use SSL
        * server — LDAP server IP address (x.x.x.x/y) or host name
    > state — Displays state of one or all group mapping data
    > statistics — Displays group mapping statistics
> group-mapping-service — Displays group-mapping service info
    > query — Displays group-mapping queries
        - all — Displays all group-mapping queries
        - local — Displays group-mapping queries added by local requests
        - remote — Displays group-mapping queries added by remote requests
    > status — Displays group-mapping service status
> group-selection — Show members under one container
    + base — Default base distinguished name (DN) to use for searches
    + bind-dn — Bind distinguished name
    + bind-password — Bind password
    + container-object — Container object class (comma-separated)
    + filter — Search filter
    + force — Whether to force
    + group-object — Group object class (comma-separated)
    + name-attribute — Name attribute
    + proxy-agent — Agent IP address/network mask or host name
    + proxy-agent-port — user-id agent listening port (1-65535; default = 5007)
    + search-scope — Search scope (one or subtree)
    + server-port — LDAP server listening port (1-65535)
    + use-ssl — Whether to use SSL
    * server — LDAP server IP address/network mask or host name
> ip-port-user-mapping — Displays terminal server agent data
    > all — Displays all terminal server agents data
    > ip — Displays terminal server agent data for IP address (x.x.x.x/y or IPv6/netmask)
    > source-user — Displays terminal server agent data for user
> ip-user-mapping — Displays the data plane ip-user-mapping
    + option — Displays option (count or detail)
    + type — Displays type (AD, CP, EDIR, GP, NTLM, SSL/VPN, UIA, unknown, or XMLAPI)
    > all — Displays all user/groups
    > ip — Displays user/group info for IP address (x.x.x.x/y or IPv6/netmask)
> ip-user-mapping-mp — Displays the management plane ip-user-mapping
    + no-group-only — Displays no group only
    + option — Displays option (count or detail)
    + type — Displays type (AD, CP, EDIR, GP, NTLM, SSL/VPN, UIA, unknown, or XMLAPI)
    > all — Displays all user/groups
    > ip — Displays user/group info for IP address (x.x.x.x/y or IPv6/netmask)
> local-user-db — Displays the local user database
    + disabled — Filters by disabled/enabled
    + username — Specifies user name
    + vsys — Specifies virtual system name
>server-monitor — Displays server monitor information
    +auto-discover   Discovers AD domain controllers
    +state           Shows state of one or all server monitored
    +statistics      Shows server monitor statistics
> ts-agent — Displays statistics for the terminal services agent
    > state — Shows state of one or all agents
```

    > statistics — Shows terminal server agent statistics
> user-IDs — Displays user names, virtual systems, and groups
    + match-user — Shows only the user(s) that match the string
> user-id-agent — Displays user information for the user-id agent
    > config — Shows specified client config
    > state — Shows state of one or all agents
    > statistics — Shows user-id-agent statistics
> user-id-service — Displays user-id service info
    > client — Displays user-id service clients (all or IP address/port number)
    > status — Displays user-id service status
> xml-api multiusersystem — Show multiuser system statistics

Sample Output

The following command displays user ID information for a specified user (in this case, the root user).

```
username@hostname> show user-IDs match-user paloaltonetwork\root

User Name                       Vsys    Groups
------------------------------------------------------------------
paloaltonetwork\root            vsys1   paloaltonetwork\domain users
                                        paloaltonetwork\users

username@hostname>
```

The following command displays statistics for the user-id agent.

```
username@hostname> show user-id-agent statistics

Name             Host            Port  Vsys    State             Ver Usage
---------------------------------------------------------------------------
agent            10.31.3.249     2010  vsys1   conn:idle         3     N

Usage: 'P': LDAP Proxy, 'N': NTLM AUTH, '*' Currently Used

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show virtual-wire

Displays information about virtual wire interfaces.

Syntax

```
show virtual-wire {all | default-vwire | <value>}
```

Options

all — Displays all virtual wire information
default-vwire — Displays information about the default virtual wire
<value> — Specifies a virtual wire interface

Sample Output

The following command displays information for the default virtual wire interface.

```
username@hostname> show virtual-wire default-vwire


total virtual-wire shown :            1

name                interface1        interface2
----------------------------------------------------------------------------
    ---
default-vwire       ethernet1/1       ethernet1/2

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show vlan

Displays VLAN information.

Syntax

```
show vlan {all | <value>}
```

Options

all — Shows information for all VLANs
<value> — Specifies a VLAN name

Sample Output

The following command displays information for all VLANs.

```
username@hostname> show vlan all

total vlan shown :                    2

name                interface         virtual interface   layer3 forwarding
----------------------------------------------------------------------------
TheTenOne           ethernet1/1.1001  vlan.1001           enabled
                    ethernet1/10.1001
                    ethernet1/2.1001
                    ethernet1/5.1001
                    ethernet1/6.1001
                    ethernet1/7.1001
                    ethernet1/8.1001
                    ethernet1/9.1001
                    ethernet1/4.1001
                    ae1
                    ethernet1/13.1001
TheTenTwo           ethernet1/1.1002  vlan.1002           enabled
                    ethernet1/2.1002
                    ethernet1/5.1002
                    ethernet1/6.1002
                    ethernet1/7.1002
                    ethernet1/8.1002
                    ethernet1/9.1002
                    ethernet1/10.1002
                    ethernet1/14
                    ethernet1/13.1002

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show vm-monitor

Displays VM monitoring information.

Syntax

```
show vm-monitor{ source [state (all | <name>) | statistics ]  | vms [ summary
    | ref-id <value>  | source-name <value> | summary ] }
```

Options

<value> — Specifies a value for the specified parameter

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show vpn

Displays Virtual Private Network (VPN) information.

Syntax

```
show vpn
    {
    flow {name <name> | tunnel-id <value>} |
    gateway {name <name>} |
    ike-sa {gateway <value>} |
    ipsec-sa {tunnel <value>} |
    tunnel {name <name>}
    }
```

Options

> flow — Displays information about the IPSec VPN tunnel on the data plane
    > name — Specifies VPN tunnel name
    > tunnel-id — Specifies VPN tunnel ID (1-65535)
> gateway — Displays Internet Key Exchange (IKE) gateway configuration
    + name — Specifies IKE gateway
> ike-sa — Displays information about the active IKE Security Association (SA)
    + gateway — Specifies IKE gateway
> ipsec-sa — Displays information about IPsec SA tunnels
    + tunnel — Specifies VPN tunnel
> tunnel — Displays auto-key IPSec tunnel configuration
    + name — Specifies VPN tunnel

Sample Output

The following command shows VPN information for the auto key IPsec tunnel k1.

```
username@hostname> show vpn tunnel name k1

TnID Name(Gateway)                 Local Proxy IP     Ptl:Port  Remote Proxy
    IP    Ptl:Port  Proposals
---- -------------                  --------------     --------- ------------
    ---    --------- ---------
   2 t-5(ike5)                  0.0.0.0/0          0:0    0.0.0.0/0
    0:0     ESP tunl [DH2][AES128,3DES][SHA1] 3600-sec
   3 t-6(ike6)                  0.0.0.0/0          0:0    0.0.0.0/0
    0:0     ESP tunl [DH2][AES128,3DES][SHA1] 3600-sec
   6 myBlue72Tunnel(to_100)       0.0.0.0/0          0:0    0.0.0.0/0
    0:0     ESP tunl [DH2][AES128,3DES][SHA1] 3600-sec

Show IPSec tunnel config: Total 3 tunnels found.

username@hostname>
```

The following command shows VPN information for the IKE gateway **g2**.

```
username@hostname> show vpn tunnel name g2

GwID Name            Peer Address/ID   Local Address/ID   Protocol   Proposals
---- ----            ---------------   ----------------   --------   ---------
   3 falcon-kestrel   35.1.15.1          35.1.15.40         Auto(main)
    [PSK][DH2][AES128,3DES][SHA1] 28800-sec

Total 1 gateways found, 0 ike sa found, 0 error.

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show wildfire

Displays Wildfire disk usage, statistics, and status.

Syntax

```
show wildfire
   {last-device-registration all |
   {latest {analysis | samples | sessions | uploads}
     {days <value> | filter column <name> value <value>} | limit <value> |
        sort-by <value> | sort-direction {asc | desc}} |
   sample-status sha256 equal <value> |
   cloud-info
   disk-usage
   statistics {days <value>} |
   status
   vm-images
```

Options

> last-device-registration — Show list of latest registration activities
> latest — Show latest 30 activities (analysis, samples, sessions, upload)
   + days — Set number of days to look back, default is 1
   + filter — Filter output based on column and value
   + limit — Set number of rows to display, default is 30
   + sort-by — Set field to sort on
   + sort-direction — Set sort direction (ascending [asc] or descending [desc])
> sample-status — Show wildfire sample status
> cloud-info— Show cloud information
> disk-usage — Show disk usage information
> statistics — Show basic wildfire statistics
> status — Show status
> vm-images — Show VM images

Sample Output

The following command displays Wildfire status

```
username@hostname> show wildfire status

Connection info:
  Wildfire cloud:                dev4.wildfire.paloaltonetworks.com
  Status:                        Idle
  Auto-Submit:                   enabled
  Selected VM:                   vm-2
  VM internet connection:        enabled
  VM network using Tor:          disabled
  Best server:                   dev4.wildfire.paloaltonetworks.com
  Device registered:             yes
  Service route IP address:      10.5.164.238
  Signature verification:        enable
  Server selection:              enable
  Through a proxy:               no
```

```
username@hostname>
```

The following command displays Wildfire statistics for the past 12 days.

```
username@hostname> show wildfire statistics days 12

Last one hour statistics :
Total sessions submitted :            0
Samples submitted        :            0
  analyzed               :            0
  pending                :            0
  malicious              :            0
  benign                 :            0
  error                  :            0
  uploaded               :            0

Last 12 days statistics  :
Total sessions submitted :           37
Samples submitted        :            7
  analyzed               :            7
  pending                :            0
  malicious              :            1
  benign                 :            6
  error                  :            0
  uploaded               :            1
```

```
username@hostname>
```

The following command displays Wildfire status.

```
username@hostname> show wildfire status

Connection info:
        Wildfire cloud:                default cloud
        Best server:
        Device registered:             no
        Service route IP address:      10.16.3.223
        Signature verification:        enable
        Through a proxy:               no

Forwarding info:
        file size limit (MB):                       5
        file idle time out (minute):                3
        total file forwarded:                       0
        forwarding rate (per minute):               0
        concurrent files:                           0

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

show zone-protection

Displays the running configuration status and run time statistics for zone protection elements.

Syntax

```
show zone-protection {zone <zone_name>}
```

Options

<zone_name> — Specifies the name of a zone

Sample Output

The following command shows statistics for the trust zone.

```
username@hostname> show zone-protection zone trust

---------------------------------------------------------------------------
Zone trust, vsys vsys1, profile custom-zone-protection
----------------------------------------------------------------------------
    tcp-syn              enabled: no
----------------------------------------------------------------------------
    udp                  RED enabled: no
----------------------------------------------------------------------------
    icmp                 RED enabled: no
----------------------------------------------------------------------------
    other-ip             RED enabled: no
----------------------------------------------------------------------------
    packet filter:
discard-ip-spoof:                enabled: no
discard-ip-frag:                 enabled: no
discard-icmp-ping-zero-id:       enabled: no
discard-icmp-frag:               enabled: no
discard-icmp-large-packet:       enabled: no
reply-icmp-timeexceeded:         enabled: no

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin, superreader, vsysreader

ssh

Opens a secure shell (SSH) connection to another host.

Syntax

```
ssh host <value>
   {
   inet {no | yes} |
   port <port_number> |
   source <ip_address> |
   v1 {no | yes} |
   v2 {no | yes}
   }
```

Options

+ inet — Force to IPv4 destination
+ port — Port to connect to on the remote host (1-65535; default = 22))
+ source — Source address for SSH session
+ v1 — Force SSH to try protocol version 1 only (default = version 2)
+ v2 — Force SSH to try protocol version 2 only
* host — Host name or IP address of remote host

Sample Output

The following command opens an SSH connection to host 10.0.0.250 using SSH version 2.

```
username@hostname> ssh v2 user@10.0.0.250
user@10.0.0.250's password:

#
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

tail

Prints the last 10 lines of a debug file.

Note: The `dp-log` option will not be available on devices that do not have a dataplane, such as the PA-200.

Syntax

```
tail
   {
   follow {no | yes} |
   lines <value> |
   agent-log <value> |
   dp-log <file> |
   mp-log <file> |
   webserver-log <file>
   }
```

Options

+ follow — Outputs appended data as the file grows
+ lines — Outputs the last N lines, instead of the last 10 (1-65535)
> agent-log — Agent log file to display (press <tab> for a list of numbers)
> dp-log — Data plane log file to display (press <tab> for list of files)
> mp-log — Management plane log file to display (press <tab> for list of files)
> webserver-log — Web server log file to display (press <tab> for list of files)

Sample Output

The following command displays the last 10 lines of the */var/log/pan/masterd.log* file.

```
username@hostname> tail /var/log/pan/masterd.log
[09:32:46] Successfully started process 'mgmtsrvr' instance '1'
[09:32:47] Successfully started process 'appWeb' instance '1'
[09:32:47] Started group 'pan' start script 'octeon' with options 'start'
[09:32:48] Process 'appWeb' instance '1' exited normally with status '7'
[09:32:48] Process 'appWeb' instance '1' has no further exit rules
[09:32:53] Successfully started process 'pan-ez-agent' instance '1'
[09:32:53] Process 'pan-ez-agent' instance '1' exited normally with status
   '0'
[09:32:53] Process 'pan-ez-agent' instance '1' has no further exit rules
[09:32:54] Successfully started process 'pan_netconfig_agent' instance '1'
[09:32:54] Finished initial start of all processes

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

target

Configures and shows a management session target.

Syntax

```
target {set <value> | show}
```

Options

> set — Sets the target device
> show — Shows the management session target

Sample Output

The following command displays the management session target.

```
username@hostname> target show

TBS

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

tcpdump

Captures packets on the management interface.

Syntax

Use this command to performs packet captures on the management interface (MGT). This can be useful to verify that traffic is traversing the interface and to analyze the traffic. Because this command defaults to the MGT interface, there is no need to specify an interface.

Press ctrl-c to stop the capture. To view the capture results, run `view-pcap mgmt-pcap mgmt.pcap`.

Syntax

```
tcpdump
   {
   filter “value” |
   snaplen <value> |
   {
```

Options

+ filter — Apply TCP dump filters. The filter must be enclosed in quotes. For example, `tcpdump filter “src net 67.207.148.0/24 and not port 22”`.
+ snaplen — Define the packet capture snap length (0-65535). For example, to set 1500 bytes, run `tcpdump filter “not port 22” snaplen 1500`. Setting the snaplen to 0 will cause the firewall to use the required length to capture whole packets. It is recommended to set the snaplen to the smallest value possible to capture the protocol or packet.

Required Privilege Level

superuser, vsysadmin, deviceadmin

test

Runs tests based on installed security policies.

Syntax

```
test
   {
   arp gratuitous {interface <interface_name> | ip <ip/netmask>} |
   botnet domain <value> |
   cp-policy-match {category <name> | destination <ip_address> | from <zone>
     | source <ip_address> | to <zone>} |
   custom-url rule <rule_name> url <value> |
   data-filtering {ccn <value> | pattern <value> | ssn <value>} |
   decryption-policy-match {application <name> | category <name> |
     destination <ip_address> | from <zone> | source <ip_address> | to
     <zone>} |
   deployment-update-schedule refresh name <value> |
   dns-proxy query name <name> source <ip_address> {domain-name <name> | ip
     <ip_address>} |
   dos-policy-match {destination <ip_address> | destination-port
     <port_number> | from <zone> | from-interface <value> | protocol <value>
     | source <ip_address> | source-user <value> | to <zone> | to-interface
     <value>} |
   global-protect-satellite {gateway-connect | gateway-disconnect | gateway-
     reconnect} gateway-address <value> method {activation | registration}
     satellite <value> |
   nat-policy-match {destination <ip_address> | destination-port
     <port_number> | from <zone> | ha-device-id <value> | protocol <value> |
     source <ip_address> | source-port <port_number> | to <zone> | to-
     interface <value>} |
   nfs dynamic-logging-partition {port <port_number> | protocol {tcp | udp} |
     readsize <value> | writesize <value> | logdirectory <value> | server
     <ip/netmask>}
   nd router-advertisement interface <value> |
   pbf-policy-match {application <name> | destination <ip_address> |
     destination-port <port_number> | from <zone> | from-interface <value> |
     ha-device-id <value> | protocol <value> | source <ip_address> | source-
     user <value>} |
   pppoe interface <interface_name> |
   qos-policy-match {application <name> | destination <ip_address> |
     destination-port <port_number> | from <zone> | protocol <value> |
     source <ip_address> | source-user <value> | to <zone>} |
   routing |
     {
     bgp virtual-router <name>
        {
        refresh peer <value> |
        restart {peer <value> | self}
        }
     fib-lookup ip <ip_address> virtual-router <value>}
     mfig-lookup group <ip/netmask> virtual-router <value> {source
```

```
            <ip_address>} |
          }
        scp-server-connection |
          {
          confirm hostname <value> key <value> |
          initiate hostname <value> password <value> username <value> {path
            <value> | port <value>}
          }
        security-policy-match {application <name> | category <name> | destination
          <ip_address> | destination-port <port_number> | from <zone> | protocol
          <value> | show-all {no | yes} | source <ip_address> | source-user
          <value> | to <zone>} |
        stats-service |
        tag-filter <value> |
        url <value> |
        url-cloud-traffic |
        url-info-cloud <value> |
        url-info-host <value> |
        vpn |
          {
          ike-sa {gateway <value>} |
          ipsec {tunnel <value>}
          }
        wildfire registration
        }
```

Options

> arp — Tests the Address Resolution Protocol (ARP) for the specified interface
    * interface — Sends gratuitous ARP for specific interface
    * ip — Sends gratuitous ARP to interface IP address (x.x.x.x/y or IPv6/netmask)
> botnet — Tests botnet domain categorization
> cp-policy-match — Tests captive portal policy matches
    + category — URL category name (press <tab> for a list of category names)
    + destination — Specifies the destination IP address (x.x.x.x or IPv6)
    + from — Specifies the From zone
    + source — Specifies the source IP address (x.x.x.x or IPv6)
    + to — Specifies the To zone
> custom-url — Tests custom URL categorization
    * rule — Specifies a security rule name
    * url — Specifies the URL value
> data-filtering — Tests credit card number (CCN), social security number (SSN), or pattern matches
    > ccn — Specifies a credit card number
    > pattern — Specifies a pattern
    > ssn — Specifies a social security number
> decryption-policy-match — Tests Secure Socket Layer (SSL) policy matches
    + application — Specifies the application name to match (press <tab> for list)
    + category — Specifies the category name to match (press <tab> for list)
    + destination — Specifies the destination IP address (x.x.x.x or IPv6)
    + from — Specifies the From zone
    + source — Specifies the source IP address (x.x.x.x or IPv6)
    + to — Specifies the To zone
> deployment-update-schedule— Tests deployment update schedule operations
    > refresh — Runs the test

```
        * name — Specifies the deployment update schedule (specify value)
> dns-proxy — Tests Domain Name Server (DNS) queries
    * source — Specifies a source IP from the object's assigned interfaces to use (x.x.x.x or IPv6)
    > domain-name — Specifies a fully qualified domain name
    > ip — Specifies an IP address to reverse query (x.x.x.x or IPv6)
> dos-policy-match — Tests Denial of Service (DoS) policy matches
    + destination — Specifies a destination IP address (x.x.x.x or IPv6)
    + destination-port — Specifies a destination port number (1-65535)
    + from — Specifies a From zone
    + from-interface — Specifies a From interface value
    + protocol — Specifies an IP protocol value (1-255)
    + source — Specifies a source IP address (x.x.x.x or IPv6)
    + source-user — Specifies a source user value
    + to — Specifies a To zone
    + to-interface — Specifies a To interface value
> global-protect-satellite — Tests GlobalProtect satellite
    > gateway-connect — Trigger GlobalProtect satellite connects to gateways
    > gateway-disconnect — Trigger GlobalProtect satellite disconnects from gateways
    > gateway-reconnect — Trigger GlobalProtect satellite reconnects to gateways
    * gateway-address — Gateway address
    * method — Activation or registration method
    * satellite — GlobalProtect satellite
> nat-policy-match — Tests Network address Translation (NAT) policy matching
    + destination — Specifies a destination IP address (x.x.x.x or IPv6)
    + destination-port — Specifies a destination port number (1-65535)
    + from — Specifies a From zone
    + ha-device-id — Specifies the HA Active-Active device ID (0-1)
    + protocol — Specifies an IP protocol value (1-255)
    + source — Specifies a source IP address (x.x.x.x or IPv6)
    + source-port — Specifies a source port number (1-65535)
    + to — Specifies a To zone
    + to-interface — Specifies an egress interface value
> nfs — Tests NFS mounts
    + port — Port number (0-65535)
    + protocol — Protocol (TCP or UDP)
    + readsize — readsize (256-32768)
    + writesize — writesize (256-32768)
    * logdirectory — Directory to mount
    * server — Server IP and network mask or FQDN
> nd — Tests IPv6 Neighbor Discovery by sending router advertisement for specified interface
> pbf-policy-match — Tests Policy-based Forwarding (PBF) matching
    + application — Specifies the application name to match (press <tab> for list)
    + destination — Specifies a destination IP address (x.x.x.x or IPv6)
    + destination-port — Specifies a destination port number (1-65535)
    + from — Specifies a From zone
    + from-interface — Specifies a From interface value
    + ha-device-id — Specifies the HA Active-Active device ID (0-1)
    + protocol — Specifies an IP protocol value (1-255)
    + source — Specifies a source IP address (x.x.x.x or IPv6)
    + source-user — Specifies a source user value
> pppoe — Tests Point-to-Point Protocol over Ethernet (PPPoE) connections
> qos-policy-match — Tests Quality of Service (QoS) policy matching
    + application — Specifies the application name to match (press <tab> for list)
    + category — URL category name (press <tab> for a list of category names)
    + destination — Specifies a destination IP address (x.x.x.x or IPv6)
    + destination-port — Specifies a destination port number (1-65535)
    + from — Specifies a From zone
    + protocol — Specifies an IP protocol value (1-255)
    + source — Specifies a source IP address (x.x.x.x or IPv6)
    + source-user — Specifies a source user value
    + to — Specifies a To zone
> routing — Tests routing. Options include:
    > bgp — Restarts the Border Gateway Protocol (BGP) connections with the peer, or refreshes to trigger a
        resending of all routes
        > refresh — Triggers specified BGP peer to resend all routes
        > restart — Restarts BGP connection
            > peer — Restarts the BGP connection with the specified peer
            > self — Restarts the virtual router itself
    > fib-lookup — Performs route lookup within the active route table (FIB)
        * ip — Specifies a destination IP address (x.x.x.x or IPv6)
        * virtual-router — Performs route lookup within specified virtual-router
    > mfib-lookup — Performs multicast route lookup within the active multicast route table (MFIB)
        + source — Specifies a multicast source IP address
        * group — Specifies a multicast group address (IP address and network mask)
        * virtual-router — Performs the multicast route lookup within the specified virtual router
> scp-server-connection — Tests SCP server connection
    > confirm — Confirms SCP server connection
        * hostname — Specifies an SCP hostname
        * key — Specifies an RSA key
    > initiate — Initiates SCP server connection
        + path — Specifies an SCP path
        + port — Specifies an SCP port (1-65535)
        * hostname — Specifies an SCP hostname
        * password — Specifies an SCP password
        * username — Specifies an SCP username
> security-policy-match — Tests security policy matching
    + application — Specifies the application name to match (press <tab> for list)
    + category — URL category name (press <tab> for a list of category names)
    + destination — Specifies a destination IP address (x.x.x.x or IPv6)
    + destination-port — Specifies a destination port number (1-65535)
    + from — Specifies a From zone
    + protocol — Specifies an IP protocol value (1-255)
    + show-all — Displays all potential match rules (no or yes)
    + source — Specifies a source IP address (x.x.x.x or IPv6)
    + source-user — Specifies a source user value
    + to — Specifies a To zone
> stats-service — Tests statistics service
> tag-filter — test a tag-filter by listing information that matches the filter based on running configuration.
> url — Tests URL categorization
> url-cloud-traffic — Tests traffic to the cloud
> url-info-cloud — Returns detailed information about the URL in the cloud
> url-info-host — Returns detailed information about the URL in the management plane
> vpn — Verifies Internet Key Exchange (IKE) and IP Security (IPSec) settings
    > ike-sa — Performs the tests only for the negotiated IKE security association (SA)
        + gateway — Specifies an IKE gateway to test
    > ipsec-sa — Performs the tests for IPsec SA (and IKE SA if necessary)
        + tunnel — Specifies a VPN tunnel to test
> url — Tests Wildfire registration
```

Sample Output

The following command tests whether the set of criteria matches any of the existing rules in the security rule base.

```
username@hostname> test security-policy-match from trust to untrust
    application google-talk source 10.0.0.1 destination 192.168.0.1 protocol
    6 destination-port 80 source-user known-user

Matched rule: 'rule1' action: allow

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

tftp export

Uses Trivial File Transfer Protocol (TFTP) to export files from the firewall to another host. TFTP export actions must specify the management interface IP as the source IP address. TFTP export actions are not supported on in-band management ports.

Syntax

```
tftp export <option> {remote-port <port_number> | source-ip <ip_address>} to
   <host>
   {
   application-block-page |
   application-pcap from <file_name> |
   captive-portal-text |
   config-bundle |
   configuration from <file_name> |
   core-file {data-plane | management-plane} from <file_name> |
   crl from <file_name> |
   debug-pcap from <file_name> |
   device-state |
   file-block-continue-page |
   file-block-page |
   filter-pcap from <file_name> |
   global-protect-portal-custom-help-page name <file_name> |
   global-protect-portal-custom-login-page name <file_name> |
   global-protect-portal-custom-welcome-page name <file_name> |
   high-availability-key from <file_name> |
   inbound-proxy-key from <value> |
   log-file {data-plane | management-plane} |
   mgmt-pcap from <file_name> |
   ssl-cert-status-page |
   ssl-optout-text |
   stats-dump |
   tech-support |
   threat-pcap from <file_name> |
   url-block-page |
   url-coach-text |
   virus-block-page |
   web-interface-certificate
   }
```

Options

+ remote-port — TFTP server port number on remote host(1-65535)
+ source-ip — Set source address to specified interface address (x.x.x.x or IPv6)
* to — TFTP host
> application-block-page — Exports application block comfort page
> application-pcap — Exports application packet capture
> captive-portal-text — Exports captive portal text
> config-bundle — Exports configuration bundle
> configuration — Exports configuration
> core-file — Exports core file
> crl — Exports crl.tgz

> debug-pcap — Exports packet capture generated for purpose of debugging daemons
> device-state — Exports device state files from a GlobalProtect Portal
> file-block-continue-page — Exports file block continue comfort page
> file-block-page — Exports file block comfort page
> filter-pcap — Exports filter packet capture
> global-protect-portal-custom-help-page — Exports GlobalProtect help page
> global-protect-portal-custom-login-page — Exports GlobalProtect login page
> global-protect-portal-custom-welcome-page — Exports GlobalProtect welcome page
> high-availability-key — Exports High Availability peer encryption key
> inbound-proxy-key — Exports inbound proxy key
> log-file — Exports log- file
> mgmt-pcap — Exports packet capture from management interface
> ssl-cert-status-page — Exports SSL certificate revoked notification page
> ssl-optout-text — Exports SSL optout text
> stats-dump — Exports log data base in CSV format
> tech-support — Exports tech support info
> threat-pcap — Exports threat packet capture
> url-block-page — Exports URL block comfort page
> url-coach-text — Exports URL coach text
> virus-block-page — Exports virus block comfort page
> web-interface-certificate — Exports web interface certificate

Required Privilege Level

superuser, vsysadmin, deviceadmin

tftp import

Uses Trivial File Transfer Protocol (TFTP) to import files to the firewall from another host. TFTP import actions must specify the management interface IP as the destination IP address. TFTP import actions are not supported on in-band management ports.

Syntax

```
tftp import <option> {remote-port <port_number> | source-ip <ip_address>}
   file <source_path> from <host>
   {
   anti-virus |
   application-block-page |
   captive-portal-text |
   certificate certificate-name <certificate_name> format {pem | pkcs12}
     {passphrase <value>} |
   configuration |
   content |
   device-state
   file-block-continue-page |
   file-block-page |
   global-protect-client |
   global-protect-portal-custom-help-page profile <profile_name> |
   global-protect-portal-custom-login-page profile <profile_name> |
   global-protect-portal-custom-welcome-page profile <profile_name> |
   high-availability-key |
   keypair certificate-name <certificate_name> format {pem | pkcs12}
     passphrase <value> |
   license |
   private-key certificate-name <certificate_name> format {pem | pkcs12}
     passphrase <value> |
   signed-url-database |
   software |
   ssl-cert-status-page |
   ssl-optout-text |
   url-block-page |
   url-coach-text |
   url-database |
   virus-block-page |
   wildfire
   }
```

Options

+ remote-port — TFTP server port number on remote host(1-65535)
+ source-ip — Set source address to specified interface address (x.x.x.x or IPv6)
* file — Source path
* from — TFTP host
> anti-virus — Imports anti-virus content
> application-block-page — Imports application block comfort page
> captive-portal-text — Imports captive portal text
> certificate — Imports X.509 certificate

> configuration — Imports configuration
> content — Imports database content
> device-state — Imports device state files for a GlobalProtect Portal
> file-block-continue-page — Imports file block continue comfort page
> file-block-page — Imports file block comfort page
> global-protect-client — Imports GlobalProtect client package
> global-protect-portal-custom-help-page — Imports GlobalProtect portal custom help page
> global-protect-portal-custom-login-page — Imports GlobalProtect portal custom login page
> global-protect-portal-custom-welcome-page — Imports GlobalProtect portal custom welcome page
> high-availability-key — Imports High Availability peer encryption key
> keypair — Imports X.509 keys (PEM or PKCS12 format)
> license — Imports license file
> private-key — Imports SSL private key
> signed-url-database — Imports signed URL database package
> software — Imports software package
> ssl-cert-status-page — Imports SSL certificate revoked notification page
> ssl-optout-text — Imports SSL optout text
> url-block-page — Imports URL block comfort page
> url-coach-text — Imports URL coach text
> url-database — Imports URL database package
> virus-block-page — Imports virus block comfort page
> wildfire — Imports wildfire content

Sample Output

The following command imports a license file from a file in user1’s account on the machine with IP address **10.0.3.4**.

```
username@hostname> tftp import ssl-certificate from user1@10.0.3.4:/tmp/
    certificatefile
username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

traceroute

Displays information about the route packets take to another host.

Syntax

```
traceroute host <value>
   {
   bypass-routing {no | yes} |
   debug-socket {no | yes} |
   do-not-fragment {no | yes} |
   first-ttl <value> |
   gateway <value> |
   ipv4 {no | yes} |
   ipv6 {no | yes} |
   max-ttl <value> |
   no-resolve {no | yes} |
   pause <value> |
   port <value> |
   source <ip_address> |
   tos <value> {verbose} |
   wait <value>
   }
```

Options

+ bypass-routing — Sends the request directly to the host on a direct attached network, bypassing usual routing table
+ debug-socket — Enables socket-level debugging
+ do-not-fragment — Sets the do-not-fragment bit
+ first-ttl — Sets the time-to-live (in number of hops) in the first outgoing probe packet
+ gateway — Specifies a loose source router gateway (maximum = 8)
+ ipv4 — Specifies that IPv4 is used
+ ipv6 — Specifies that IPv6 is used
+ max-ttl — Sets the maximum time-to-live in number of hops
+ no-resolve — Does not attempt to print resolved domain names
+ pause — Sets the time to pause between probes (in milliseconds)
+ port — Sets the base port number used in probes (default for UDP = 33434; for TCP = 80; for ICMP = 1)
+ source — Specifies the source IP address in outgoing probe packets
+ tos — Specifies the type of service (TOS) treatment for the packets by way of the TOS bit for the IP header in the ping packet (0-255)
+ wait — Specifies a delay in transmission of the traceroute request (in seconds)
* host — Specifies the IP address or name of the remote host (required)

Sample Output

The following command displays information about the route from the firewall to www.google.com.

```
username@hostname> traceroute www.paloaltonetworks.com
traceroute to www.paloaltonetworks.com (72.32.199.53), 30 hops max, 38 byte
    packets
1  10.1.0.1 (10.1.0.1)  0.399 ms  1.288 ms  0.437 ms
2  64.0.27.225.ptr.us.xo.net (64.0.27.225)  1.910 ms dsl027-186-
    189.sfo1.dsl.speakeasy.net (216.27.186.189)  1.012 ms
    64.0.27.225.ptr.us.xo.net (64.0.27.225)  1.865 ms
3  dsl027-182-001.sfo1.dsl.speakeasy.net (216.27.182.1)  16.768 ms  581.420
    ms 64.3.142.37.ptr.us.xo.net (64.3.142.37)  219.190 ms
4  ge5-0-0.mar2.fremont-ca.us.xo.net (207.88.80.21)  228.551 ms 110.ge-0-0-
    0.cr1.sfo1.speakeasy.net (69.17.83.189)  12.352 ms ge5-0-0.mar2.fremont-
    ca.us.xo.net (207.88.80.21)  218.547 ms
5  ge-5-3-0.mpr3.pao1.us.above.net (209.249.11.177)  13.212 ms p4-0-
    0.rar2.sanjose-ca.us.xo.net (65.106.5.137)  273.935 ms  221.313 ms
6  p1-0.ir1.paloalto-ca.us.xo.net (65.106.5.178)  139.212 ms so-1-2-
    1.mpr1.sjc2.us.above.net (64.125.28.141)  13.348 ms p1-0.ir1.paloalto-
    ca.us.xo.net (65.106.5.178)  92.795 ms
7  so-0-0-0.mpr2.sjc2.us.above.net (64.125.27.246)  12.069 ms
    206.111.12.146.ptr.us.xo.net (206.111.12.146)  93.278 ms so-0-0-
    0.mpr2.sjc2.us.above.net (64.125.27.246)  556.033 ms
8  tbr1p013201.sffca.ip.att.net (12.123.13.66)  52.726 ms so-3-2-
    0.cr1.dfw2.us.above.net (64.125.29.54)  61.875 ms
    tbr1p013201.sffca.ip.att.net (12.123.13.66)  58.462 ms

     MPLS Label=32537 CoS=0 TTL=1 S=1

 9  64.124.12.6.available.above.net (64.124.12.6)  74.828 ms
    tbr1cl3.la2ca.ip.att.net (12.122.10.26)  62.533 ms
    64.124.12.6.available.above.net (64.124.12.6)  60.537 ms
10  tbr1cl20.dlstx.ip.att.net (12.122.10.49)  60.617 ms
    vlan901.core1.dfw1.rackspace.com (72.3.128.21)  59.881 ms  60.429 ms
11  gar1p360.dlrtx.ip.att.net (12.123.16.169)  108.713 ms
    aggr5a.dfw1.rackspace.net (72.3.129.19)  58.049 ms
    gar1p360.dlrtx.ip.att.net (12.123.16.169)  173.102 ms
12  72.32.199.53 (72.32.199.53)  342.977 ms  557.097 ms  60.899 ms

username@hostname>
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

view-pcap

Displays the contents of packet capture files.

Syntax

```
view-pcap {application-pcap | debug-pcap | filter-pcap | threat-pcap}
   <file_name>
   {
   absolute-seq {no | yes} |
   delta {no | yes} |
   follow {no | yes} |
   hex {no | yes} |
   hex-ascii {no | yes} |
   hex-ascii-link {no | yes} |
   hex-link {no | yes} |
   link-header {no | yes} |
   no-dns-lookup {no | yes} |
   no-port-lookup {no | yes} |
   no-qualification {no | yes} |
   no-timestamp {no | yes} |
   timestamp {no | yes} |
   undecoded-NFS {no | yes} |
   unformatted-timestamp {no | yes} |
   verbose {no | yes} |
   verbose+ {no | yes} |
   verbose++ {no | yes}
   }
```

Options

+ absolute-seq — Display the absolute TCP sequence numbers
+ delta — Display a delta (in micro-seconds) between the current and previous lines
+ follow — Monitor a pcap file in real time
+ hex — Display each packet (minus link header) in hex
+ hex-ascii — Display each packet (minus link header) in hex and ASCII
+ hex-ascii-link — Display each packet (including link header) in hex and ASCII
+ hex-link — Display each packet (including link header) in hex
+ link-header — Display the link-level header on each dump line
+ no-dns-lookup — Do not convert host addresses to names
+ no-port-lookup — Do not convert protocol and port numbers to names
+ no-qualification — Do not print domain name qualification of host names
+ no-timestamp — Do not print a timestamp
+ timestamp — Print a timestamp proceeded by date
+ undecoded-NFS — Print undecoded NFS handles
+ unformatted-timestamp — Print an unformatted timestamp
+ verbose — Display verbose output
+ verbose+ — Display more verbose output
+ verbose++ — Display the maximum output details
> application-pcap — Display application packet capture file specified by name
> debug-pcap — Display debug packet capture file specified by name
> filter-pcap — Display filter packet capture file specified by name
> threat-pcap — Display threat packet capture file specified by name

Sample Output

The following command displays the contents of the packet capture file */var/session/pan/filters/syslog.pcap* in ASCII and hex formats.

```
username@hostname> view-pcap hex-ascii /var/session/pan/filters/syslog.pcap
reading from file /var/session/pan/filters/syslog.pcap, link-type EN10MB
    (Ethernet)
08:34:31.922899 IP 10.0.0.244.32884 > jdoe.paloaltonetworks.local.syslog:
    UDP, length 314
         0x0000:  4500 0156 0000 4000 4011 2438 0a00 00f4  E..V..@.@.$8....
         0x0010:  0a00 006c 8074 0202 0142 d163 3c31 3137  ...l.t...B.c<117
         0x0020:  3e41 7072 2020 3233 2030 383a 3334 3a33  >Apr..23.08:34:3
         0x0030:  3420 312c 3034 2f32 3320 3038 3a33 343a  4.1,04/23.08:34:
         0x0040:  3334 2c54 4852 4541 542c 7572 6c2c 312c  34,THREAT,url,1,
         0x0050:  3034 2f32 3320 3038 3a33 343a 3235 2c31  04/23.08:34:25,1
         0x0060:  302e 302e 302e 3838 2c32 3039 2e31 3331  0.0.0.88,209.131
         0x0070:  2e33 362e 3135 382c 302e 302e 302e 302c  .36.158,0.0.0.0,
         0x0080:  302e 302e 302e 302c 6c32 2d6c 616e 2d6f  0.0.0.0,l2-lan-o
         0x0090:  7574 2c77 6562 2d62 726f 7773 696e 672c  ut,web-browsing,
         0x00a0:  7673 7973 312c 6c32 2d6c 616e 2d74 7275  vsys1,l2-lan-tru
         0x00b0:  7374 2c6c 322d 6c61 6e2d 756e 7472 7573  st,l2-lan-untrus
         0x00c0:  742c 6574 6865 726e 6574 312f 3132 2c65  t,ethernet1/12,e
         0x00d0:  7468 6572 6e65 7431 2f31 312c 466f 7277  thernet1/11,Forw
         0x00e0:  6172 6420 746f 204d 696b 652c 3034 2f32  ard.to.Mike,04/2
         0x00f0:  3320 3038 3a33 343a 3334 2c38 3336 3435  3.08:34:34,83645
         0x0100:  372c 322c 3438 3632 2c38 302c 302c 302c  7,2,4862,80,0,0,
         0x0110:  3078 302c 7463 7028 3629 2c61 6c65 7274  0x0,tcp(6),alert
         0x0120:  2c77 7777 2e79 6168 6f6f 2e63 6f6d 2f70  ,www.yahoo.com/p
         0x0130:  2e67 6966 3f2c 2c73 6561 7263 682d 656e  .gif?,,search-en
         0x0140:  6769 6e65 732c 696e 666f 726d 6174 696f  gines,informatio
         0x0150:  6e61 6c2c 3000                           nal,0.
```

Required Privilege Level

superuser, vsysadmin, deviceadmin

Chapter 5
GP-100 GlobalProtect Mobile Security Manager Commands

This chapter contains command reference pages for the GP-100 GlobalProtect Mobile Security Manager appliance. For more information, refer to the *GlobalProtect Administrator's Guide*..

Configuration Mode Commands

The following Configuration Mode commands are described in the following sections. For Operational Mode commands, see “GP-100 GlobalProtect Mobile Security Manager Operation Mode Commands” on page 671

- “set deviceconfig setting” on page 604
- “set deviceconfig system” on page 607
- “set directory-integration” on page 615
- “set global-protect-mdm” on page 616
- “set icon” on page 618
- “set mgt-config” on page 621
- “set policy” on page 624
- “set profiles” on page 625
- “set setting” on page 644
- “set shared admin-role” on page 645
- “set shared authentication-profile” on page 650
- “set shared authentication-sequence” on page 652
- “set shared certificate” on page 653
- “set shared certificate-profile” on page 654
- “set shared email-scheduler” on page 655
- “set shared icon” on page 656
- “set shared local-user-database” on page 657
- “set shared log-settings” on page 658
- “set shared pdf-summary-report” on page 661
- “set shared report-group” on page 662
- “set shared reports” on page 663
- “set shared server-profile” on page 665
- “set shared tags” on page 667
- “show” on page 668
- “top” on page 669
- “up” on page 670

Note: *Changes in the configuration are retained, until overwritten, while the firewall is powered. To save a candidate configuration in non-volatile storage, use the* ***save*** *command. To make a candidate configuration active, use the* ***commit*** *command.*

check

Displays the current configuration status.

Syntax

```
check
   {
   data-access-passwd {system} |
   pending-changes
   }
```

Options

> data-access-passwd — Check data access authentication status for this session
   + system — Check whether data access password exists for the system
> pending-changes — Check for uncommitted changes

Sample Output

The following command shows that there are currently no uncommitted changes.

```
username@hostname# check pending-changes
no
[edit]
username@hostname#
```

Required Privilege Level

superuser, deviceadmin

commit

Makes the current candidate configuration the active configuration on the firewall.

> ***Note:*** *When you change a configuration setting, the current "candidate" configuration is updated, not the active configuration. The* ***commit*** *command applies the candidate configuration to the active configuration, which activates all configuration changes since the last commit.*

Syntax

```
commit
   {
   force
   partial {
     device-and-network excluded |
     policy-and-objects excluded |
   validate
   }
```

Options

> force — Forces the commit command in the event of a conflict
> partial — Commits the specified part of the configuration
   + device-and-network — Excludes device and network configurations from the commit (configurations under config/mgt-config, config/devices/platform, config/devices/deviceconfig, and config/devices/network)
   + policy-and-object — Excludes policy and object configurations from the commit (configurations under (config/shared; also excludes config/devices/vsys if in single vsys mode)
> validate — Validates the command prior to commit.

Sample Output

The following command updates the active configuration with the contents of the candidate configuration.

```
username@hostname# commit
```

Required Privilege Level

superuser, deviceadmin

copy

Makes a copy of a node in the hierarchy along with its children, and adds the copy to the same hierarchy level.

Syntax

```
copy <node1> to <node2>
```

Options

<node1> — Specifies the node to be copied
<node2> — Specifies the name of the copy

Sample Output

The following command, copies policy1 to policy2.

```
username@hostname# copy policy policy1 to policy2
```

Required Privilege Level

superuser, deviceadmin

delete

Removes a node from the candidate configuration along with all its children.

> ***Note:*** *No confirmation is requested when this command is entered.*

Syntax

```
delete <node>
```

Options

<node> — Specifies the node to be deleted. For available nodes of the hierarchy, press <tab>.

Sample Output

The following command deletes the icon **`label1`** from the candidate configuration.

```
username@hostname# delete icon label1
[edit]
  username@hostname#
```

Required Privilege Level

superuser, deviceadmin

edit

Changes context to a lower level in the configuration hierarchy.

Syntax

```
edit <context>
```

Options

<context> — Specifies a path through the hierarchy. For available contexts in the hierarchy, press <tab>.

Sample Output

The following command changes context from the top level to the **mgt-config** level of the hierarchy.

```
[edit]
   username@hostname# edit mgt-config

[edit mgt-config]
   username@hostname#
```

Required Privilege Level

superuser, deviceadmin

exit

Exits from the current PAN-OS CLI level.

- From Operational mode — Exits the PAN-OS CLI.
- From Configuration mode, top hierarchy level — Exits Configuration mode, returning to Operational mode.
- From Configuration mode, lower hierarchy levels — Changes context to one level up in the hierarchy. Provides the same result as the **up** command.

***Note:** The **exit** command is the same as the **quit** command.*

Syntax

```
exit
```

Options

None

Sample Output

The following command changes to the profiles level and then changes context back to the top level.

```
username@hostname# edit profiles
[edit profiles]
username@hostname# exit
username@hostname#
```

The following command changes from Configuration mode to Operational mode.

```
[edit]
   username@hostname# exit
Exiting configuration mode

username@hostname>
```

Required Privilege Level

All

find

Lists CLI commands containing the specified keyword.

Syntax

```
find command keyword <value>
```

Options

<value> — Specifies a keyword.

Sample Output

The following command lists all CLI commands containing the keyword hsm.

```
username@hostname# find command keyword hsm
show deviceconfig system hsm-settings
show deviceconfig system hsm-settings provider
show deviceconfig system hsm-settings provider
show deviceconfig system hsm-settings provider safenet-luna-sa
show deviceconfig system hsm-settings provider safenet-luna-sa hsm-server
show deviceconfig system hsm-settings provider safenet-luna-sa hsm-server
   <name>
show deviceconfig system hsm-settings provider safenet-luna-sa ha
...
username@hostname#
```

Required Privilege Level

All

load

Assigns the last saved configuration, or a specified configuration, to be the candidate configuration. Also, loads the last imported device state files.

Syntax

```
load
   {
   config |
     {
     key <value> |
     from <filename> |
     last-saved |
     partial |
        {
        from <filename> |
        from-xpath <value> |
        mode {merge | replace} |
        to-xpath <value>
        }
     repo device <value> {file <value> | version <value>} |
     version <value>
     }
   device-state
   }
```

Options

> config — Loads specified configuration
   + key — Key used for encryption
   > from — File name (select from the file names provided, or enter a new name)
   > last-saved — Loads the last saved configuration
   > partial — Loads partial configuration
      * from — File name (select from the file names provided, or enter a new name)
      * from-xpath — XML Path (XPath) of the source node
      * mode — Mode in which to load (merge or replace)
      * to-xpath — XML Path (XPath) of the destination's parent
   > repo — Loads device config from backup repository
      * device — Device name
      > file — Filename
      > version — Version
   > version — Selects from the provided versions
> device-state — Loads from imported device state files to GlobalProtect Portals.

Sample Output

The following command assigns **output.xml** to be the candidate configuration.

```
[edit]
    username@hostname# load config from output.xml

command succeeded

[edit]
    username@hostname#
```

The following command adds the “top-apps” report found in the x.xml configuration to the specified candidate configuration.

```
[edit]
    username@hostname# load config partial from x.xml from-xpath shared/
    reports/entry[@name='top-apps'] mode merge to-xpath/config/devices/
    entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/reports

command succeeded

[edit]
    username@hostname#
```

Required Privilege Level

superuser, deviceadmin

move

Relocates a node in the hierarchy along with its children to be at another location at the same hierarchy level.

Syntax

```
move <element1> {bottom | top | after <element2> | before <element2>}
```

Options

<element1> — Specifies the items to be moved. For available elements of the hierarchy, press <tab>.
<element2> — Indicates the element after or before which *element1* will be placed
after — Moves element to be after *element2*
before — Moves element to be before *element2*
bottom — Makes the element the last entry of the hierarchy level
top — Makes the element the first entry of the hierarchy level

Sample Output

The following command moves the policy **`policy1`** to the top level.

```
username@hostname# move policy rule1 top

[edit]
   username@hostname#
```

Required Privilege Level

superuser, deviceadmin

override

Overrides a node from the candidate configuration along with all its children. This is a device command that overrides a value pushed from a Panorama Template.

> ***Note:*** *No confirmation is requested when this command is entered.*

Syntax

```
override <node>
```

Options

<node> — Specifies the node to override. For available nodes of the hierarchy, press <tab>.

Sample Output

The following command overrides an configuration profile with a specified web clip from the candidate configuration.

```
username@hostname# override profiles android-configuration myconfig web-clip myclip
[edit]
  username@hostname#
```

Required Privilege Level

superuser, deviceadmin

quit

Exits from the current PAN-OS CLI level.

- From Operational mode — Exits the PAN-OS CLI.
- From Configuration mode, top hierarchy level — Exits Configuration mode, returning to Operational mode.
- From Configuration mode, lower hierarchy levels — Changes context to one level up in the hierarchy. Provides the same result as the **up** command.

Note: *The **exit** and **quit** commands are interchangeable.*

Syntax

```
quit
```

Options

None

Sample Output

The following command changes context from the network interface level to the network level.

```
[edit log-settings]
username@hostname# quit

[edit]
username@hostname#
```

The following command changes from Configuration mode to Operational mode.

```
[edit]
   username@hostname# quit
Exiting configuration mode

username@hostname>
```

Required Privilege Level

All

rename

Changes the name of a node in the hierarchy.

Syntax

```
rename <node1> to <node2>
```

Options

<node1> — Indicates the original node name. For available nodes of the hierarchy, press <tab>.
<node2> — Indicates the new node name

Sample Output

The following command changes the name of a policy from Policy1 to Policy2.

```
username@hostname# rename policy Policy1 to Policy2
```

Required Privilege Level

superuser, deviceadmin

run

Executes an Operational mode command while in Configuration mode.

For information about the syntax and options for each Operational mode command, refer to its command page in Chapter 4, “Operational Mode Commands”.

Syntax

```
run
   {
   check |
   debug |
   delete |
   grep |
   less |
   ls |
   netstat |
   ping |
   request |
   scp |
   set |
   show |
   ssh |
   tail |
   test |
   traceroute |
   }
```

Sample Output

The following command executes a **ping** command to the IP address **`1.1.1.2`** from Configuration mode.

```
username@hostname# run ping host 1.1.1.2
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
...
username@hostname#
```

Required Privilege Level

superuser, deviceadmin

save

Saves a snapshot of the firewall configuration or the device state files from a GlobalProtect Portal.

> ***Note:*** *This command saves the configuration on the firewall, but does not make the configuration active. Use the* **commit** *command to make the current candidate configuration active.*

Syntax

```
save
   {
   config to <filename> |
   device-state
   }
```

Options

> config — Saves the current configuration
   + to — File name (select from the file names provided, or enter a new name)
> device-state — Saves all files needed to restore a GlobalProtect Portal. This command is used to save the configuration and dynamic information from a firewall that is configured as a GlobalProtect Portal with the large scale VPN feature enabled. The file can then be imported to restore the Portal in the event of a failure. The export contains a list of all satellite devices managed by the Portal, the running configuration at the time of the export, and all certificate information (Root CA, Server, and Satellite certificates).

Sample Output

The following command saves a copy of the configuration to the file **`savefile`**.

```
[edit]
username@hostname# save config to savefile
Config saved to savefile

[edit]
   username@hostname#
```

Required Privilege Level

superuser, deviceadmin

set deviceconfig setting

Specifies general device settings on the device.

Syntax

```
set deviceconfig setting
      }
      custom-logo {
            login-screen {
              name <value>;
              content <value>;
            }
            main-ui {
              name <value>;
              content <value>;
            }
            pdf-report-header {
              name <value>;
              content <value>;
            }
            pdf-report-footer {
              name <value>;
              content <value>;
            }
      {
      jumbo-frame {
            mtu 512-9216;
          }
      management {
         auto-acquire-commit-lock {yes | no} |
         enable-certificate-expiration-check {yes | no} |
         hostname-type-in-syslog <value> |
         idle-timeout <value> |
         max-audit-versions <value> |
         max-rows-in-csv-export <value> |
         max-rows-in-pdf-report <value> |
         admin-lockout {failed-attempts <value> | lockout time <value>} |
         common-criteria-alarm-generation
         (
            enable-alarm-generation {yes | no} |
            enable-audible-alarms {yes | no} |
            enable-cli-alarm-notification {yes | no} |
            enable-web-alarm-notification {yes | no} |
            encrypt-decrypt-fail-count <value> |
            log-databases-alarm-threshold
            {
               config <value> |
               hipmatch <value> |
               mdm <value> |
               system <value> |
            }
```

```
                    rule-group-limits
                    {
                        count <value> |
                        time-interval <value> |
                        tags <value> |
                    }
                    security-policy-limit
                    {
                        count <value> |
                        time-interval <value> |
                    }
                disk-quota
                {
                    alarm <float>;
                    config <float>;
                    hipmatch <float>;
                    mdm <float>;
                    system <float>;
                }
            util {
                    assert-crash-once yes|no;
                 }

            {
```

Options

> setting
  > custom-logo
    > login-access — Import custom logo for login screen (from content or file)
      + content — Upload custom login screen page (base64 encoded)
      + name — File name alphanumeric string [0-9a-zA-Z./_-]
    > main-ui — Import custom logo for main user interface (from content or file)
      + content — Upload custom main user interface page (base64 encoded)
      + name — File name alphanumeric string [0-9a-zA-Z./_-]
    > pdf-report-footer — Import custom logo for PDF report footers (from content or file)
      + content — Upload custom PDF report footer page (base64 encoded)
      + name — File name alphanumeric string [0-9a-zA-Z./_-]
    > pdf-report-header — Import custom logo for PDF report headers (from content or file)
      + content — Upload custom lPDF report header page (base64 encoded)
      + name — File name alphanumeric string [0-9a-zA-Z./_-]
  > jumbo-frame
    + mtu — device MTU excluding Ethernet header (512-9216)
  > management
    + auto-acquire-commit-lock — Automatically add a commit lock when modifying configuration
    + enable-certificate-expiration-check — Check for expired certificates and stop using them
    + hostname-type-in-syslog — Choose type to send in hostname field in syslog header (FSDN, hostname, ipv4-address, or ipv6-address)
    + idle-timeout — Default administrative session idle timeout in minutes (1-1440; 0 = never)
    + max-audit-versions — Maximum number of audited versions of config to preserve (1-1048576)
    + max-rows-in-csv-export — Maximum number of rows in exported csv files (1-1048576)
    + max-rows-in-pdf-report — Maximum number of rows in user activity report (1-1048576)
    > admin-lockout — Administrative login lockout settings
      + failed-attempts — Number of failed login attempts to trigger lock-out (0-10)

```
            + lockout-time — Number of minutes to lock-out (0-60)
        > common-criteria-alarm-generation
            + enable-alarm-generation — Enable Common Criteria (CC) alarms generation
            + enable-audible-alarms — Enable audio sound for alarms
            + enable-cli-alarm-notification — Enable alarms notification on admin console
            + enable-web-alarm-notification — Enable alarms notification on Web
            + encrypt-decrypt-fail-count — Encryption/Decryption failure counts limit (1-4294967295)
            > log-databases-alarm-threshold — Log databases % full threshold value for alarms generation
                + config — configuration logs database % full threshold value for alarm  generation (1-100)
                + hipmatch — hipmatch logs database % full threshold value for alarm  generation (1-100)
                + mdm — Mobile Security Manager logs database % full threshold value for alarm  generation
                     (1-100)
                + system — system logs database % full threshold value for alarm  generation (1-100)
            > rule-group-limits — Security rule group violation notification threshold (count 1-4294967295;
                time-interval 30-86400). Security rule group limits are the number of times, and time in which,
                the rule groups that are tagged with "tags" are matched.
                + tags — Tags for rule group member value or list of values
            > security-policy-limits — Security rule violation notification threshold (count 1-4294967295; time-
                interval 30-86400). Security policy limits affect each individual rule in the security policy.  If any
                rule hits the specified count within the time-interval, an alarm is generated.
        > disk-quota — Quotas for logs, packet captures etc. (percentages between 0 and 90.0)
            + alarm — Alarm logs quota percentage
            + config — Configuration logs quota percentage
            + hipmatch — HIP match quota percentage
            + mdm — Mobile Security Manager logs quota percentage
            + system — System logs quota percentage
    > util
        + assert-crash-once — Enables/disables assert crash only once
```

Sample Output

The following command locks an administrative user out for **15** minutes after **5** failed login attempts.

```
username@hostname# set deviceconfig setting management admin-lockout 5
    lockout-time 15
```

Required Privilege Level

superuser, deviceadmin

set deviceconfig system

Specifies system-related settings on the firewall.

Syntax

```
set deviceconfig system
   {
   authentication profile <value>;
   certificate-profile <value>;
   default-gateway <ip/netmask>;
   domain <value>;
   domain-lookup-url <value>;
   hostname <value>;
   ip-address <ip/netmask>;
   ip-address-lookup-url <value>;
   ipv6-address <ip/netmask>;
   ipv6-default-gateway <ip/netmask>;
   locale <value>;
   login-banner <value>;
   mtu <value>;
   netmask <value>;
   ntp-server-1 <value>;
   ntp-server-2 <value>;
   secure-proxy-password <value>;
   secure-proxy-port <value>;
   secure-proxy-server <value>;
   secure-proxy-user <value>;
   speed-duplex auto-negotiate|10Mbps-half-duplex|10Mbps-fullduplex|100Mbps-
     half-duplex|100Mbps-full-duplex|1Gbps-full-duplex; link-state up|down;
         service {
           disable-http yes|no;
           disable-https yes|no;
           disable-telnet yes|no;
           disable-ssh yes|no;
           disable-icmp yes|no;
           disable-snmp yes|no;
           disable-mobile-device-checkin yes|no;
           disable-globalprotect-gateway yes|no;
         }
         permitted-ip {
           <address>;
         }
       }
       speed-duplex auto-negotiate|10Mbps-half-duplex|10Mbps-full-
     duplex|100Mbps-half-duplex|100Mbps-full-duplex|1Gbps-half-
     duplex|1Gbps-full-duplex;
   syslog-certificate <value>;
   timezone <value>;
   update-server <value>;
   web-server-certificate <value>;
   dns-setting {
           servers {
             primary <ip/netmask>;
             secondary <ip/netmask>;
           }
       }
   geo-location {
         latitude <value>;
         longitude <value>;
       }
   hsm-settings {
         provider {
             safenet-luna-sa {
               hsm-server {
                 <name> {
                   server-address <ip/netmask>;
                 }
               }
               ha {
                 auto-recovery-retry 0-500;
                 ha-group-name <value>;
               }
             }
             OR...
             thales-nshield-connect {
               hsm-server {
                 <name> {
                   server-address <ip/netmask>;
                 }
               }
               rfs-address <ip/netmask>;
             }
             OR...
             none;
         }
       }
   log-export-schedule {
         <name> {
           description <value>;
           enable yes|no;
           log-type device-state|hipmatch|mdm-log;
           start-time <value>;
           protocol {
             ftp {
               hostname <value>;
               port 1-65535;
               path <value>;
               username <value>;
               password <value>;
               passive-mode yes|no;
             }
             OR...
             scp {
               hostname <value>;
               port 1-65535;
               path <value>;
               username <value>;
               password <value>;
             }
           }
         }
   log-link {
         <name> {
           url <value>;
         }
       }
   ethernet1 {
      default-gateway <ip>;
      ip-address <ip>;
      link-state up|down;
      mtu <value>;
      netmask <ip>;
      speed-duplex auto-negotiate|10Mbps-half-duplex|10Mbps-
         fullduplex|100Mbps-half-duplex|100Mbps-full-duplex|1Gbps-full-
         duplex; link-state up|down;
      permitted-ip <ip/netmask>;
      service {
         disable-globalprotect-gateway yes|no;
         disable-http yes|no;
         disable-https yes|no;
         disable-mobile-device-checkin yes|no;
         disable-ssh yes|no;
         disable-icmp yes|no;
         disable-snmp yes|no;
         disable-telnet yes|no;
      }
   permitted-ip {
         <address>;
       }
   route {
         service {
           <name> {
             source {
               interface <value>;
               address <value>;
             }
           }
         }
         destination {
           <address> {
             source-address <value>;
           }
         }
       }
   service {
      disable-globalprotect-gateway yes|no;
      disable-http yes|no;
      disable-https yes|no;
      disable-mobile-device-checkin yes|no;
```

```
  disable-ssh yes|no;
  disable-icmp yes|no;
  disable-snmp yes|no;
  disable-telnet yes|no;
}
snmp-setting {
      snmp-system {
        location <value>;
        contact <value>;
        send-event-specific-traps yes|no;
      }
      access-setting {
        version {
          v2c {
            snmp-community-string <value>;
          }
          OR...
          v3 {
            views {
              <name> {
                view {
                  <name> {
                    oid <value>;
                    option include|exclude;
                    mask <value>;
                  }
                }
              }
            }
            users {
              <name> {
                view <value>;
                authpwd <value>;
                privpwd <value>;
              }
            }
          }
        }
      }
    }

}
update-schedule {
      statistics-service {
        device {
          software-crash-info yes|no;
        }
      }
      app-profile {
        recurring {
            daily {
              at <value>;
              action download-only|download-and-install;
            }
            OR...
            weekly {
              day-of-week
  sunday|monday|tuesday|wednesday|thursday|friday|saturday;
              at <value>;
              action download-only|download-and-install;
            }
          threshold 1-120;
        }
      }
      global-protect-datafile {
        recurring {
            hourly {
              at 0-59;
              action download-and-install;
            }
            OR...
            daily {
              at <value>;
              action download-and-install;
            }
            OR...
            weekly {
              day-of-week
  sunday|monday|tuesday|wednesday|thursday|friday|saturday;
              at <value>;
              action download-and-install;
            }
        }
      }
    }
  }
}
```

Options

> system

- + authentication-profile — Authentication profile to use for non-local administrators (RADIUS method is supported)
- + certificate-profile — Profile for verifying client certificates
- + default-gateway — Default gateway IP address
- + domain — Domain value
- + domain-lookup-url — Domain lookup URL
- + hostname — Hostname value
- + ip-address — IP address for the management interface
- + ip-address-lookup-url — IP address lookup URL
- + ipv6-address — IPv6/netmask for the management interface
- + ipv6-default-gateway — IPv6 for the default gateway
- + locale — System default locale (US, Japan, CN, or TW)
- + login-banner — Login banner text
- + mtu — Maximum Transmission Unit (MTU) for the management interface
- + netmask — IP address or IPv6 for the management interface network mask
- + ntp-server-1 — First Network Time Protocol (NTP) server IP address
- + ntp-server-2 — Second Network Time Protocol server IP address

```
+ secure-proxy-password — Secure Proxy password to use
+ secure-proxy-port — Port for secure proxy server (1-65535)
+ secure-proxy-server — Secure Proxy server to use
+ secure-proxy-user — Secure Proxy user name to use
+ speed-duplex — Speed and duplex for the management interface (100Mbps-full-duplex, 100Mbps-half-duplex, 10Mbps-full-duplex, 10Mbps-half-duplex, 1Gbps-full-duplex, 1Gbps-half-duplex, or auto-negotiate)
+ timezone — Time zone name (press <tab> for a list of time zones)
+ update-server — Palo Alto Networks update server
+ syslog-certificate — Client certificate for syslog
+ web-server-certificate — Certificate for secure web GUI
> dns-setting
   > servers — Primary and secondary DNS servers
      + primary — Primary DNS server IP address
      + secondary — Secondary DNS server IP address
> geo-location — Device geographic location
   + latitude — Latitude coordinate
   + longitude — Longitude coordinate
> hsm-setting — Specify HSM provider
   > provider
      > safenet-luna-sa — Safenet Luna SA
         + client-address — HSM client IP address
         > ha — ha
            + auto-recovery-retry   The number of times HSM HA function will attempt to automatically recover a member that has failed to synchronize or has dropped from the HA group. Setting to a value of zero switches the feature off.
            + ha-group-name         HA group name
         > hsm-server — hsm-server (server name)
      > thales-nshield-connect — Thales NShield
         + rfs-address — IP address of remote file system server (server IP address)
         > hsm-server — hsm-server (value)
            + server-address — HSM server IP address
      none — No HSM
> log-export-schedule — Schedule for exporting logs
   + description — description text
   + enable — Enable no or yes
   + log-type — Type of log
   + start-time — Time to start the scheduled export hh:mm (e.g. 03:30)
   > protocol — Protocol to use for export
      > ftp — Use FTP protocol for export
         + hostname — FTP hostname
         + passive-mode — Enable FTP Passive Mode
         + password — FTP password
         + path — FTP server path
         + port — FTP port (1-65535)
         + username — FTP username
      > scp — Use SCP protocol for export
         + hostname — SCP hostname
         + password — SCP password
         + path — SCP server path
         + port — SCP port (1-65535)
         + username — SCP username
> log-link — Link to external log (option to provide URL format of link)
> ethernet1
```

```
    + default-gateway — Default gateway
    + ip-address — IP address for VM download interface
    + link-state — Link state up or down
    + mtu — Maximum Transmission Unit for the management interface
    + netmask — IP netmask for VM download  interface
    + speed-duplex — Speed and duplex for Mobile Security Manager interface
    > permitted-ip — permitted-ip (ip/netmask)
    > service — service
        + disable-globalprotect-gateway — Disable the GlobalProtect gateway (no or yes)
        + disable-http — disable-http
        + disable-https — disable-https
        + disable-icmp — disable-icmp
        + disable-mobile-device-checkin — Disable mobile device check-in (no or yes)
        + disable-snmp — disable-snmp
        + disable-ssh — disable-ssh
        + disable-telnet — disable-telnet

> permitted-ip — Permitted IP address (x.x.x.x/y) or IPv6/netmask
> route
    > destination — Destination IP address or FQDN
        + source-address — Source IP address to use to reach destination
    > service — Service name (CRL servers, DNS server(s), SMTP gateway(s), NetFlow server(s), NTP
        server(s), Palo Alto update server, Panorama server, Proxy server, RADIUS server, SNMP server(s),
        Syslog server(s), user ID agent(s), URL update server)
        + source-address — Source IP address to use to reach destination
> service
    + disable-globalprotect-gateway — Disable the gateway (no or yes)
    + disable-http — Disable HTTP (no or yes)
    + disable-http-ocsp — Disable Online Certificate Status Protocol (OCSP) over HTTP (no or yes)
    + disable-https — Disable HTTPS (no or yes)
    + disable-icmp — Disable ICMP (no or yes)
    + disable-mobile-device-checkin — Disable mobile device check-in (no or yes)
    + disable-snmp — Disable SNMP (no or yes)
    + disable-ssh — Disable SSH (no or yes)
    + disable-telnet — Disable Telnet (no or yes)
    + disable-userid-service — Disable user ID service (no or yes)
> snmp-setting
    > access-setting — Access setting version
        version v2c
            + snmp-community-string — SNMP community string value
        version v3
            > users — User name
                + authpwd — Authentication Protocol Password
                + privpwd — Privacy Protocol Password
                + view — SNMP View Name
            > views — View name
                view — Oid subtree name
    > snmp-system
        + contact — Email contact information
        + location — System location
        + send-event-specific-traps — Whether to use event-specific trap definitions
> update-schedule — Schedule for downloading/installing updates
    > app-profile — Application profile database
        > recurring
            + threshold — Ignore if release date is new (1-120 hours)
            > daily — Schedule update everyday
            + action — Action (download and install or download and do not install)
            + at — Time specification hh:mm (e.g. 20:10)
            > weekly — Schedule update once a week
            + action — Action (download and install or download and do not install)
            + at — Time specification hh:mm (e.g. 20:10)
            + day-of-week — Day of the week (Friday, Monday, Saturday, Sunday, Thursday, Tuesday,
                Wednesday)
    > global-protect-datafile — GlobalProtect data file update
        > daily — Schedule update everyday
            + action — Action (download and install)
            + at — Time specification hh:mm (e.g. 20:10)
        > hourly — Schedule update every hour
            + action — Action (download and install)
            + at — Minutes past the hour
        > weekly — Schedule update once a week
            + action — Action (download and install)
            + at — Time specification hh:mm (e.g. 20:10)
            + day-of-week — Day of the week (Friday, Monday, Saturday, Sunday, Thursday, Tuesday,
                Wednesday)
    > statistics-service — Participates in anonymous statistics upload service
        > application-and-threat-reports — Uploads application and/or threat report statistics
            + application-usage — Application usage statistics (no or yes)
            + attackers — Threats by destination ports (no or yes)
            + attacking-countries — Threats by attacking countries (no or yes)
        > device — Uploads device statistics
            + software-crash-info — Back traces of crashes (no or yes)
        > unknown-application-reports — Uploads unknown application reports statistics
            + unknown-applications-by-destination-addresses — Unknown applications by destination IP
                addresses (no or yes)
            + unknown-applications-by-destination-ports — Unknown applications by destination ports (no
                or yes)
        > url-reports — Uploads URL reports statistics
            + dataplane-cache-url — Upload dataplane cache URLs (no or yes)
            + malware-categories-by-url — Upload malware categories by URLs (no or yes)
            + unknown-categories-by-url — Upload unknown categories by URLs (no or yes)
```

Required Privilege Level

superuser, deviceadmin

set directory-integration

Configures directory integration.

Syntax

```
set directory-integration <name>
{

   disabled yes|no;
   group-filter <value>;
   server-profile <value>;];
   update-interval 60-86400;
   use-modify-timestamp yes|no;
   user-filter <value>;
   container-object [ <container-object1> <container-object2>... ];
   email [ <email1> <email2>... ];
   group-include-list [ <group-include-list1> <group-include-list2>...
   group-member [ <group-member1> <group-member2>... ];
   group-name [ <group-name1> <group-name2>... ];
   group-object [ <group-object1> <group-object2>... ];
   last-modify-attr [ <last-modify-attr1> <last-modify-attr2>... ];
   user-name [ <user-name1> <user-name2>... ];
   user-object [ <user-object1> <user-object2>... ];
}
```

Options

<name> — Specifies the display name for the system
+ disabled — disabled (yes or no)
+ group-filter — ldap search filter for group
+ server-profile — LDAP server object
+ update-interval — Interval (seconds) for updating group membership, default is 3600 seconds
+ use-modify-timestamp — use-modify-timestamp
+ user-filter — ldap search filter for user
> container-object — container object class (start list of values)
> email — email object class (start list of values)
> group-include-list — include list (start list of values)
> group-member — group member attribute (start list of values)
> group-name — group name attribute (start list of values)
> group-object — group object class (start list of values)
> last-modify-attr — last modify timestamp attribute (start list of values)
> user-name — user name attribute (start list of values)
> user-object — user object class (start list of values)

Required Privilege Level

superuser, deviceadmin

set global-protect-mdm

Configures GlobalProtect Mobile Security Manager on the device. Mobile Security Manager provides security for client systems, such as laptops, that are used in the field by allowing easy and secure login from anywhere in the world.

Syntax

```
set global-protect-mdm
    {
    authentication-message <value>;
    authentication-profile <value>;
    check-in-interval 30-1440;
    check-in-port 443|7443|8443;
    consent-text <value>;
    enrollment-port 443|7443|8443;
    host <value>;
    organization-identifier <value>;
    organization-name <value>;
    save-password yes|no;
    server-certificate <value>;
    server-certificate-ca <value>;
    apns {
            certificate <value>;
          }
    device-identity-certificate {
      ca <value>;
      days-till-expiry 60-3650;
      renew-identity-certificate-display-msg <value>;
      require-reenroll yes|no;
      scep {
         certificate-profile <value>;
         scep <value>;
      }
    gateway {
      certificate-profile <value>;
      server-certificate <value>;
    }
    gcm {
      api-key <value>;
      sender-id <value>;
      }
    hip-collection {
      exclude-gps-location yes|no;
      exclude-tags [list tags to exclude]
      exclude-not-managed-apps yes|no
          }
    hip-notification {
            <name> {
              match-message {
                include-app-list yes|no;
                message <value>;
              }
              not-match-message {
                message <value>;
              }
            }
          }
    volume-purchase-program
      apple-auth-token <token>
      invite-at-enrollment yes|no
    }
```

Options

> global-protect-mdm — GlobalProtect Mobile Security Manager configuration
    + authentication-message — Authentication profile used for this Mobile Security Manager
    + authentication-profile — Authentication profile used for this Mobile Security Manager
    + check-in-interval — Device check-in interval (minutes)
    + check-in port — Device check-in port
    + consent-text — Mobile Security Manager installation Consent Text
    + enrollment-port — Device Enrollment Port
    + host — Mobile Security Manager Host Name
    + organization-identifier — Organization identifier
    + organization-name — Organization name
    + save-password — Whether save user's password into database
    + server-certificate — SSL server certificate name
    + server-certificate-ca — SSL server certificate's CA file name
    > apns — Configure APNS Parameters
        + certificate (specify name)
    > device-identity-certificate — Device identity certificate
        + ca — CA for Client certificate
        + days-till-expiry — Number of days till expiry for device identity certificate
        + renew-identity-certificate-display-msg — Message to be displayed in the push notification on the mobile device to renew enrollment
        + require-reenroll — Requiring Re-enroll will force all device users to unenroll and enroll their devices again with the Mobile Security Manager upon expiration of certificate issued during initial enrollment
        > scep — SCEP Configuration for IOS devices enrollment
            + certificate-profile — Profile for authenticating client certificates
            + scep — SCEP
    > gateway — Configure Gateway connections Parameters
        + certificate-profile — Profile for authenticating client certificates
        + server-certificate — Server Certificate for Connections from Gateways
    > gcm — Configure GCM Parameters
        + api-key — GCM API Key
        + sender-id — GCM Sender ID
    > hip-collection — Host information profile collection instructions
        + exclude-gps-location — Exclude GPS Location
    > hip-notification — host PC health evaluate (specify value)

Required Privilege Level

superuser, deviceadmin

set icon

Configures an icon for mobile devices.

Syntax

```
set icon <name>
    {
    description <value> |
    image <name> |
    }
```

Options

<name> — Name to identify the icon
+ description — Icon description
+ image — Icon image

Required Privilege Level

superuser, deviceadmin

set managed-application

Configures an icon for mobile devices.

Syntax

```
set managed-application <name>
    {
    package-name <value.
    category <app category>
    developer <name>
    platform
      pad yes no
      phone yes no
    price <value>
    source
         app-store track-id <application ID>
         google-play
         enterprise
            os ios/android
            display-name <name>
            description <description>
            version <value>
            icon <file>
            screen-shot-1 <image>
            screen-shot-2 <image>
    }
```

Options

<name> — Name to identify the icon
+ description — Icon description
+ image — Icon image

Required Privilege Level

superuser, deviceadmin

set managed-application-group

Configures an icon for mobile devices.

Syntax

```
set managed-application-group <name>
   application [list applications or application group names]

   up to 2000 applications or application groups can be added to a group
     (???)
   }
```

Options

<name> — Name to identify the icon
+ description — Icon description
+ image — Icon image

Required Privilege Level

superuser, deviceadmin

set mgt-config

Configures management accounts on the firewall.

Syntax

```
set mgt-config
   {
   devices <serial_number> |
     {
     disable-config-backup {no | yes} |
     hostname <value> |
     ip <value>
     }
   password-complexity |
     {
     block-repeated-characters <value> |
     block-username-inclusion {no | yes} |
     enabled {no | yes} |
     minimum-length <value> |
     minimum-lowercase-letters <value> |
     minimum-numeric-letters <value> |
     minimum-special-characters <value> |
     minimum-uppercase-letters <value> |
     new-password-differs-by-characters <value> |
     password-change-on-first-login {no | yes} |
     password-change-period-block <value> |
     password-history-count <value> |
     password-change
        {
        expiration-period <value> |
        expiration-warning-period <value> |
        post-expiration-admin-login-count <value> |
        post-expiration-grace-period <value>
        }
     }
   password-profile <name> |
     {
     password-change
        {
        expiration-period <value> |
        expiration-warning-period <value> |
        post-expiration-admin-login-count <value> |
        post-expiration-grace-period <value>
        }
     }
   test test-config <name>
   users <name>
     {
     authentication-profile <profile_name> |
     client-certificate-only {no | yes} |
     password-profile <value> |
        public-key <value> |
        permissions role-based |
           {
           deviceadmin <name> |
           devicereader <name> |
           custom |
              {
              profile <name> |
              }
           superreader yes |
           superuser yes |
           }
        phash <value> |
        preferences |
           {
           disable-dns {no | yes} |
           saved-device-query {
              device <name> query <value>
              }
           saved-log-query
              {
              alarm <name> query <query_value> |
              config <name> query <query_value> |
              data <name> query <query_value> |
              hipmatch <name> query <query_value> |
              mdm <name> query <query_value> |
              system <name> query <query_value> |
              }
           }
        password
     }
```

Options

> devices — (Panorama only) Device serial number
>
> + disable-config-backup — Enable config back up for this device
> + hostname — Device ost name
> + ip — Device IP address

> password-complexity — Password complexity settings
>
> + block-repeated-characters — Block repeated characters count (0-15)
> + block-username-inclusion — Block inclusion of username and it's reverse
> + enabled — Enable minimal password complexity enforcement
> + minimum-length — Minimum password length (0-15)
> + minimum-lowercase-letters — Minimum lowercase letters in the password (0-15)
> + minimum-numeric-letters — Minimum numeric characters in the password (0-15)
> + minimum-special-characters — Minimum special characters (non-alphanumeric) in the password (0-15)
> + minimum-uppercase-letters — Minimum uppercase letters in the password (0-15)
> + new-password-differs-by-characters — New Password must differ by the count chars (0-15)
> + password-change-on-first-login — Password must change on first time login
> + password-change-period-block — Password change block period, in days (0-365)
> + password-history-count — Save password history for password changes, in days (0-150)
>
> > password-change — Password change settings
> >
> > + expiration-period — Password expiry, in days (0-365)
> > + expiration-warning-period — Password expiry warning period, in days (0-30)

```
        + post-expiration-admin-login-count — Password post-expiry admin login count (0-3)
        + post-expiration-grace-period — Password post-expiry grace period (0-30)
> password-profile — Password profile name
    > password-change — Password change settings
        + expiration-period — Password expiry, in days (0-365)
        + expiration-warning-period — Password expiry warning period, in days (0-30)
        + post-expiration-admin-login-count — Password post-expiry admin login count (0-3)
        + post-expiration-grace-period — Password post-expiry grace period (0-30)
> test — Test the configuration
    + testconfig — Specify configuration name
> users — Select from the list of defined users or enter a new name
    + authentication-profile — Authentication profile or sequence name
    + client-certificate-only — Is client certificate authentication enough? (no or yes)
    + password-profile — Password profile name
    + public-key — Public key for SSH authentication
    > permissions — Role-based permissions
        + deviceadmin — Device name(s) (localhost.localdomain) or list of values enclosed in [ ]
        + devicereader — Device name(s) (localhost.localdomain) or list of values enclosed in [ ]
        > custom — Custom role-based permissions
            + profile — Select from the list of defined profiles or enter a new name
            + vsys — Virtual system name or list of values enclosed in [ ] (available only when virtual systems
                are enabled)
        > superreader — Assign superreader role to specified user
        > superuser — Assign superuser role to specified user
        > vsysadmin — Virtual system administrator (available only when virtual systems are enabled)
            + vsys — virtual system name(s) (localhost.localdomain) or list of values enclosed in [ ]
        > vsysreader — Virtual system reader (available only when virtual systems are enabled)
            + vsys — virtual system name(s) (localhost.localdomain) or list of values enclosed in [ ]
    > phash — phash value
    > preferences — Preferences for specified user
        + disable-dns — Disable Domain Name System (DNS)
        > saved-device-query— Specify device and query names
        > saved-log-query — Query a saved log
            > alarm — Alarm log name and query value
            > config — Configuration log name and query value
            > data — Data log name and query value
            > hipmatch — HIP match log name and query value
            > mdm — Mobile Security Manager log name and query value
            > system — System log name and query value
    password — Option to provide a password
```

Required Privilege Level

superuser, deviceadmin

set policy

Specifies settings for mobile device policies.

Syntax

```
set policy
   {
   <name> {
     disabled yes|no;
     android-profiles [ <android-profiles1> <android-profiles2>... ];
     hip-profiles [ <hip-profiles1> <hip-profiles2>... ];
     ios-profiles [ <ios-profiles1> <ios-profiles2>... ];
     users [ <users1> <users2>... ];
   }
   }
```

Options

<name> — Profile group to configure
+ disabled — Disable the rule
> android-profiles — Android profiles (name)
> hip-profiles — HIP profiles (name)
> ios-profiles — IOS profiles (name)
> users — Specify user

Required Privilege Level

superuser, deviceadmin

set profiles

Specifies settings for security profiles that can be applied to security policies for mobile devices.

Syntax

```
set profiles
{
android-configuration <name>
    {
    application <name or app group name>
      remove-when-unenroll yes/no
      install-option optional/required
    description <value>;
    identifier <value>;
    name <value>;
    passcode {
      auto-lock 1-60;
      max-failed-attempts 4-10;
      min-passcode-len 1-16;
      passcode-history 1-50;
      passcode-type {
         password |
            min-complex-len 1-4;
         pin
         }
    restrictions {
          allow-camera yes|no;
          require-encrypted-storage yes|no;
        }
    web-clip {
          <name> {
            label <value>;
            url <value>;
            icon <value>;
                   }
    vpn <name> {
      connection-name <name>;
      server <server address>;
      account {
         fixed <username>
            }
      proxy-setup {
         manual {
            port 1-65535;
            address <value>
      type {
         globalprotect {
            user-authentication {
                password {
                   fixed <value>;
                credential {
                   type {
```

```
                   certificate <value>;
         allow-portal-profile yes|no;
         connect-method {
            on-demand;
            user-logon
                   }
wifi <name> {
   auto-join yes|no;
   hidden yes|no;
   service-id <value>;
   proxy-setup {
           manual {
             port 1-65535;
             address <value>;}
         }
   security-type {
      any {password <value>;
           wep {
             password <value>;
           }
      any-enterprise {
         accepted-eap {
            eap-pwd | peap | tls | ttls {inner-identity
               NONE|GTC|PAP|MSCHAP|MSCHAPv2;}
         }
         password {
            fixed <value> |
            set-on-device |
            use-saved;
         }
         trusted-certificates [ <trusted-certificates1> <trusted-
            certificates2>... ];
         username {
            fixed <value> |
            set-on-device |
            use-saved;
             }
      none |
      wep password <value> |
      wep-enterprise {
         accepted-eap {
            eap-pwd | peap | tls | ttls {inner-identity
               NONE|GTC|PAP|MSCHAP|MSCHAPv2;}
         }
         password {
            fixed <value> |
            set-on-device |
            use-saved;
         }
         trusted-certificates [ <trusted-certificates1> <trusted-
            certificates2>... ];
         username {
            fixed <value> |
            set-on-device |
                use-saved;
                }
         wpa password <value> |
         wpa-enterprise {
            accepted-eap {
                eap-pwd | peap | tls | ttls {inner-identity
                   NONE|GTC|PAP|MSCHAP|MSCHAPv2;}
            }
            password {
                fixed <value> |
                set-on-device |
                use-saved;
            }
            trusted-certificates [ <trusted-certificates1> <trusted-
                certificates2>... ];
            username {
                fixed <value> |
                set-on-device |
                use-saved;
                }
    }
hip-objects <name> {
    description <value>;
    applications {
      criteria {
         has-malware <yes | no>
         {
            excludes <value>
                {
                package <value>;
                hash <value>;
                }
            }
         includes {
                {
                package <value>;
                hash <value>
                }
         has-unmanaged-app <yes | no>
                }
    host-info {
      criteria {
      }
         app-version {
                contains <value> |
                is <value> |
                is-not <value>
            }
         device-name {
                contains <value> |
                is <value> |
                is-not <value>
            }
         imei {
                contains <value> |
                is <value> |
                is-not <value>
            }
         model {
                contains <value> |
                is <value> |
                is-not <value>
            }
         os {
              is ios|android |
              is-not ios|android
            }
         os-version {
                greater-equal <value> |
                greater-than <value> |
                is <value> |
                is-not <value> |
                less-equal <value> |
                less-than <value>
         phone-number {
                contains <value> |
                is <value> |
                is-not <value>
            }
         serial-number {
                contains <value> |
                is <value> |
                is-not <value>
            }
         tag {
                contains <value> |
                is <value> |
                is-not <value>
            }
          }
        }
    settings {
      criteria {
         disk-encrypted <no | yes> |
         jailbroken <no | yes> |
         passcode-set <no | yes>
          }
    }
hip-profiles <name>
    {
    description <value>;
    match <value>;
    }
ios-configuration <name>
    {
    application <app name or group name>
         remove-when-unenroll <no | yes>
         collect-feedback <no | yes>
         prevent-backup <no | yes>
         app-configuration <name>
            name <configuration parameter name>
               value <configuration parameter value>
```

```
     app-vpn <vpn config name>
     install-option
        optional;
        required;
        app-lock
            disable-touch <no | yes>
            disable-volume button <no | yes>
            disable-sleep-wake <no | yes>
            enable-voice-over <no | yes>
            enable-insert-colors <no | yes>
            enable-speak-selection <no | yes>
            disable-device-rotation <no | yes>
            disable-ringer-switch <no | yes>
            disable-auto-lock <no | yes>
            enable-zoom <no | yes>
            enable-assistive-touch <no | yes>
            enable-mono-audio <no | yes>
application-data
  block-data-from-managed-apps-to-unmanaged-apps <no | yes>
  block-data-from-unmanaged-apps-to-managed-apps <no | yes>
description <value>;
identifier <value>;
name <value>;
activesync {
      <name> {
     account-name <value>;
     allow-move yes|no;
     domain <value>;
     enable-address-syncing yes|no;
     past-days-to-sync 0|1|3|7|14|31;
     server <value>;
     use-only-in-mail yes|no;
     use-ssl yes|no;
     email-address {
          fixed <value> |
          use-saved-username <value> |
          from-directory-server
                 }
     enable-smime yes|no;
               }
     identity-certificate {
          certificate <value> |
          scep <value>;
                 }
     password {
          fixed <value> |
          set-on-device |
          use-saved;
        }
     username {
          fixed <value> |
          use-saved
        }
apn {
        access-point-name <value>;
        proxy-server <value>;
        proxy-port 1-65535;
        password {
            fixed <value> |
            set-on-device |
            use-saved;
        }
        username {
            fixed <value> |
            set-on-device |
            use-saved
        }
auto-remove-profile {
  duration-until-removal 1-65535;
  never |
  removal-date <value> |
  }
certificates <name> {
        password <value>;
      }
email <name> {
     account-description <value>;
     allow-move yes|no;
     enable-address-syncing yes|no;
     use-only-in-mail yes|no;
     account-type {
          pop |
          imap {
            path-prefix <value>;
          }
     email-address {
          fixed <value> |
          use-saved-username <value> |
          from-directory-server;
        }
     enable-smime yes|no;
     incoming {
        authentication-type
            EmailAuthNone|EmailAuthPassword|EmailAuthCRAMMD5|EmailAuthNTL
            M|EmailAuthHTTPMD5;
        port <value>
        password {
            fixed <value> |
            set-on-device |
            use-saved
        }
        server <value>;
        username {
            fixed <value> |
            use-saved
          }
        use-ssl yes|no;
     }
     outgoing {
        authentication-type
```

```
            EmailAuthNone|EmailAuthPassword|EmailAuthCRAMMD5|EmailAuthNTL
            M|EmailAuthHTTPMD5;
        port <value>
        password {
            fixed <value> |
            set-on-device |
            use-saved
        }
        server <value>;
        username {
            fixed <value> |
            use-saved
          }
        use-ssl yes|no;
     }
     user-display-name {
          fixed <value> |
          use-saved
        }
}
ldap {
  <name> {
  account-description <value>;
  account-host <value>;
  use-ssl yes|no;
  password {
          fixed <value> |
          set-on-device |
          use-saved
        }
  search-settings <name> {
    base <value>;
    scope
          {LDAPSearchSettingScopeSubtree|LDAPSearchSettingScopeBase|LDAPS
          earchSettingScopeOneLevel;
          }
  }
  username {
          fixed <value> |
          set-on-device |
          use-saved;
        }
     }
passcode {
  allow-simple-value yes|no;
  auto-lock none|1|2|3|4|5|10|15;
  grace-period none|0|1|5|15|60|240;
  max-failed-attempts 4-10;
  max-passcode-age 1-730;
  min-complex-len 1-4;
  min-passcode-len 1-16;
  passcode-history 1-50;
  require-alphanumeric-value yes|no;
}
```

```
restrictions {
  accept-cookies 0|1|2;
  allow-installing-apps yes|no;
  allow-camera yes|no;
  allow-facetime yes|no;
  allow-screen-capture yes|no;
  allow-auto-sync-when-roaming yes|no;
  allow-siri yes|no;
  allow-siri-while-locked yes|no;
  allow-voice-dialing yes|no;
  allow-in-app-purchase yes|no;
  allow-multiplayer-gaming yes|no;
  allow-adding-game-center-friends yes|no;
  allow-youtube yes|no;
  allow-itunes yes|no;
  allow-safari yes|no;
  allow-safari-autofill yes|no;
  allow-icloud-backup yes|no;
  allow-icloud-doc-sync yes|no;
  allow-photo-stream yes|no;
  allow-diagnostics-submission yes|no;
  allow-untrusted-TLS-certificate yes|no;
  allow-explicit-content yes|no;
  allow-app-removal yes|no;
  allow-bookstore yes|no;
  allow-bookstore-erotica yes|no;
  allow-chat yes|no;
  allow-game-center yes|no;
  allow-passbook-while-locked yes|no;
  allow-shared-stream yes|no;
  allow-configuration-profile-installation yes|no;
  block-pop-ups yes|no;
  enable-safari-javascript yes|no;
  enable-siri-profanity-filter yes|no;
  force-encrypted-backup yes|no;
  force-itunes-password yes|no;
}
security {
      always |
      never |
      with-authorization {
        authorization-password <value>;
      }
        }
vpn <name> {
  app-level-vpn
     enabled yes;
     per-app-on-demand yes;
     safari domains <domain name>;
  connection-name <value>;
  device-level-vpn
     enabled yes/no
  server <value>;
  account {
          fixed <value> |
          set-on-device |
          use-saved;
        }
  proxy-setup
  {
     automatic url <value> |
     manual
     {
        address <value>;
        port <value>;
        password <value>;
        username <value>
     }
  }
  type {
     anyconnect {
            group <value>;
            user-authentication {
              password {
                fixed <value> |
                set-on-device |
                use-saved
                       }
     aruba user-authentication {
        credential {
                type {
                  scep <value> |
                  certificate <value>
                }
                vpn-on-demand {
                  domains {
                    <name> {
                      domain <value>;
                      action always|never|ondemand;
                    }
                  }
        password {
                fixed <value> |
                set-on-device |
                use-saved;
              }
     }
     custom {
            identifier <value>;
            data {
              <name> {
                value <value>;
              }
            }
            user-authentication {
              password {
                fixed <value> |
                set-on-device |
                use-saved
              }
              credential {
```

```
           type {
             scep <value> |
             certificate <value>
                    }
f5-ssl {
   credential {
           type {
             scep <value> |
             certificate <value>
           }
           vpn-on-demand {
             domains {
               <name> {
                 domain <value>;
                 action always|never|ondemand;
               }
             }
   password {
           fixed <value> |
           set-on-device |
           use-saved;
         }
}
globalprotect {
   allow-portal-profile yes|no;
   connect-method
       on-demand;
       user-logon
   user-authentication {
       credential {
           type {
             scep <value> |
             certificate <value>
           }
           vpn-on-demand {
             disconnect-on-idle 2
             domains {
               <name> {
                 domain <value>;
                 action always|never|ondemand;
               }
             }
       password {
           fixed <value> |
           set-on-device |
           use-saved;
         }

       vpn-on-demand {
           domains {
             <name> {
               domain <value>;
               action always|never|ondemand;
             }
}
l2tp {
   send-all yes|no;
   shared-secret <value>;
   authenticate-type {
         password |
         rsa-securid;
       }
}
ipsec machine-authentication {
   shared-secret {
           group-name <value>;
           use-hybrid-auth yes|no;
           prompt-for-password yes|no;
           shared-secret <value>;
         }
   credential {
      include-user-pin yes|no;
      type {
             scep <value> |
             certificate <value>;
           }
      vpn-on-demand {
             domains {
               <name> {
                 domain <value>;
                 action always|never|ondemand;
                               }
juniper-ssl {
       realm <value>;
       role <value>;
       user-authentication {
         password {
           fixed <value> |
           set-on-device |
           use-saved;
         }
         credential {
           type {
             scep <value> |
             certificate <value>;
           }
           vpn-on-demand {
             domains {
               <name> {
                 domain <value>;
                 action always|never|ondemand;
               }
             }
           }
         }
pptp {
       authenticate-type {
         password |
         rsa-securid;
       }
       encryption-level none|automatic|maximum;
       send-all yes|no;
     }
sonicwall {
        domain <value>;
        user-authentication {
            password {
                fixed <value> |
                set-on-device |
                use-saved;
              }
            credential {
                type {
                  scep <value> |
                  certificate <value>;
                }
                vpn-on-demand {
                  domains {
                    <name> {
                      domain <value>;
                      action always|never|ondemand;
                    }
                  }
                }
web-clip <name> {
     full-screen yes|no;
     icon <value>;
     label <value>;
     removable yes|no;
     precomposed yes|no;
     url <value>;
     }
}
wifi <name> {
  auto-join yes|no;
  hidden yes|no;
  service-id <value>;
  proxy-setup {
     automatic {
            url <value>;
          }
     manual {
        address <value>;
        password {
              fixed <value>;
              OR...
              set-on-device;
              OR...
              use-saved;
            }
        port 1-65535;
        username {
              fixed <value>;
              OR...
              set-on-device;
              OR...
              use-saved;
            }
        }
  security-type {
```

```
any {password <value>;
     wep {
       password <value>;
     }
any-enterprise {
   accepted-eap {
       eap-pwd | peap | tls | ttls {inner-identity
          NONE|GTC|PAP|MSCHAP|MSCHAPv2;}
   }
   password {
       fixed <value> |
       set-on-device |
       use-saved;
   }
   trusted-certificates [ <trusted-certificates1> <trusted-
       certificates2>... ];
   username {
       fixed <value> |
       set-on-device |
       use-saved;
       }
none |
wep password <value> |
wep-enterprise {
   accepted-eap {
       eap-pwd | peap | tls | ttls {inner-identity
          NONE|GTC|PAP|MSCHAP|MSCHAPv2;}
   }
   password {
       fixed <value> |
       set-on-device |
       use-saved;
   }
   trusted-certificates [ <trusted-certificates1> <trusted-
       certificates2>... ];
   username {
       fixed <value> |
       set-on-device |
       use-saved;
       }
wpa password <value> |
wep-enterprise {
   accepted-eap {
       eap-pwd | peap | tls | ttls {inner-identity
          NONE|GTC|PAP|MSCHAP|MSCHAPv2;}
   }
   password {
       fixed <value> |
       set-on-device |
       use-saved;
   }
   trusted-certificates [ <trusted-certificates1> <trusted-
       certificates2>... ];
   username {
```

```
                fixed <value> |
                set-on-device |
                use-saved;
                }
    }
ios-provisioning {
      <name> {
      app-identifier <value>;
      creation-date <value>;
      expiration-date <value>;
      profile <value>;
      profile-identifier <value>;
      }
scep {
    fingerprint <value>;
    keysize 1024|2048;
    name <value>;
    nt-principal-name <value>;
    retries 0-10;
    retry-delay 0-36000;
    scep-url <value>;
    subject <value>;
    subject-alternative-name-type
      None|rfc822Name|dNSName|uniformResourceIdentifier;
    subject-alternative-name <value>;
    use-as-digital-signature yes|no;
    use-for-key-encipherment yes|no;
    scep-challenge {
      none |
      fixed <value> |
      dynamic {
         otp-server-path <value>;
         password <value>;
         username <value>;
      }
      use-ssl {
              yes {
                scep-ca-cert <value>;
                scep-client-cert <value>;
              } |
              no;
            }
      }
```

Options

> android-configuration — Android Configuration Profiles (specify name)

+ description — Brief explanation of the contents or purpose of the profile

+ identifier — Unique identifier for the profile

+ name — Display name of the profile (shown on the device)

> passcode — Passcode configuration

+ auto-lock — Device automatically locks when time period elapses

+ max-failed-attempts   Number of passcode entry attempts allowed before all data on device will be erased

+ min-passcode-len — Smallest number of passcode characters allowed

```
    + passcode-history — Number of unique passcodes before reuse
    > passcode-type — passcode-type
        > password   Require passcodes to contain at least one letter
            + min-complex-len   Smallest number of non-alphanumeric characters allowed
        pin — Permit the use of only numbers
> restrictions   Restrictions configuration
    + allow-camera — Allow use of camera
    + require-encrypted-storage   Require encryption of stored data
> web-clip       Web Clip (name)
    + icon     The icon to use for the Web Clip
    + label    The name to display for the Web Clip
    + url      The URL to be displayed when opening the Web Clip
> wifi          wifi configuration (name)
    + auto-join      Automatically join the network
    + hidden         Enable if network is not open or is not broadcasting
    + service-id     identification of wireless network to connect to
    > proxy-setup     Configures Proxies to be used with this network
        > automatic   Automatically get proxy configuration
            + url      URL used to retrieve proxy settings
        > manual      Manually configure proxy
            + address    IP or fully qualified address
    > security-type   Wireless network authentication and encryption
        > any              Any (Personal)
            + password   password for the wireless network
        > any-enterprise   Any Enterprise
            > accepted-eap           authentication protocols supported on target network
                > ttls      ttls
                    + inner-identity   authentication protocol
                eap-pwd   EAP-PWD
                 peap      PEAP
                 tls       TLS
            > password — Password for the provided username
            > trusted-certificates   Certificates trusted/expected for authentication (specify value)
            > username — Username for connection to wireless network
        > none — No security protocol used (specify password)
        > wep              wep (specify password)
        > wep-enterprise   wep-enterprise
            > accepted-eap           authentication protocols supported on target network
                > ttls      ttls
                    + inner-identity   authentication protocol
                eap-pwd   EAP-PWD
                 peap      PEAP
                 tls       TLS
            > password — Password for the provided username
            > trusted-certificates   Certificates trusted/expected for authentication (specify value)
            > username — Username for connection to wireless network
        > wpa              WPA/WPA2 protocol (specify password)
        > wpa-enterprise   WPA/WPA2 Enterprise
            > accepted-eap           authentication protocols supported on target network
                > ttls — TTLS
                    + inner-identity   authentication protocol
                eap-pwd — EAP-PWD
                 pea — PEAP
                 tls — TLS
                > password — Password for the provided username
                > trusted-certificates   Certificates trusted/expected for authentication (specify value)
                > username — Username for connection to wireless network
> hip-objects           hip-objects
    + description    description
    > applications   applications
        > criteria — Specify matching criteria
            > has-malware   If device has malware applications (yes or no)
            > includes      includes (value)
                + hash      application hash
                + package   application package name
    > host-info      host-info
        > criteria — Specify matching criteria
            > app-version     app-version
                > contains — Contains (specify value)
                > is — Matches (specify value)
                > is-not — Does not match (specify value)
            > device-name     device-name
                > contains — Contains (specify value)
                > is — Matches (specify value)
                > is-not — Does not match (specify value)
            > imei            imei
                > contains — Contains (specify value)
                > is — Matches (specify value)
                > is-not — Does not match (specify value)
            > model           model
                > contains — Contains (specify value)
                > is — Matches (specify value)
                > is-not — Does not match (specify value)
            > os              os
                > contains — Contains (specify value)
                > is — Matches (specify value)
                > is-not — Does not match (specify value)
            > os-version      os version
                > contains — Contains (specify value)
                > is — Matches (specify value)
                > is-not — Does not match (specify value)
            > phone-number    phone-number
                > contains — Contains (specify value)
                > is — Matches (specify value)
                > is-not — Does not match (specify value)
            > serial-number   serial-number
                > contains — Contains (specify value)
                > is — Matches (specify value)
                > is-not — Does not match (specify value)
            > tag             tag
                > contains — Contains (specify value)
                > is — Matches (specify value)
                > is-not — Does not match (specify value)
    > settings       settings
        > criteria — Specify matching criteria
            + disk-encrypted   If device's disk is encrypted (yes or no)
            + jailbroken       If device is by rooted/jailbroken (yes or no)
            + passcode-set     If device's passcode is present (yes or no)
```

```
> hip-profiles          hip profiles
      + description   description
      + match         match
> ios-configuration     iOS Configuration Profiles (specify value)
      + description          Brief explanation of the contents or purpose of the profile
      + identifier           Unique identifier for the profile
      + name                 Display name of the profile (shown on the device)
      > activesync           Exchange ActiveSync
           + account-name            Name for the Exchange ActiveSync account
           + allow-move              Allow user to move messages from the account
           + domain                  Domain for the account.
           + enable-address-syncing   Allow Recent Address syncing
           + past-days-to-sync       The number of past days of mail to synchronize
           + server                  Microsoft Exchange Server
           + use-only-in-mail        Send outgoing mail from this account only from Mail app
           + use-ssl                 Send all communication through secure socket layer
           > email-address           The address of the account
           > enable-smime            Support S/MIME for this account
           > identity-certificate    The protocol for accessing email account
           > password                The password for the account
           > username                User for the account. Domain and User must be blank for device to prompt for user
      > apn                 APN configuration
           + access-point-name   The name of the carrier (GPRS) access point
           + proxy-port          Port number for the proxy server
           + proxy-server        Hostname or IP address for the proxy server
           > password            The password to connect to the access point
           > username            The username to connect to the access point
      > auto-remove-profile   Settings for automatic profile removal
           > duration-until-removal   Duration until removal
           > removal-date             Removal date in format YYYY-MM-DD
             never                    never
      > certificates        Credentials configuration
      > email               Email configuration
           + account-description      The display name of the account(e.g. Company Mail Account)
           + allow-move               Allow user to move messages from this account
           + enable-address-syncing   Allow Recent Address syncing
           + use-only-in-mail         Send outgoing mail from this account only from Mail app
           > account-type             The protocol for accessing email account
           > email-address            The address of the account
           > enable-smime             Support S/MIME for this account
           > incoming                 Incoming Mail
           > outgoing                 Outgoing Mail
           > user-display-name        The display name of the user
      > ldap                LDAP Configuration
           + account-description   The display name of the account
           + account-host          The LDAP hostname or IP address
           + use-ssl               Enable Secure Socket Layer for this connection
           > password              The password for this LDAP account.
           > search-settings       Search settings for this LDAP server
           > username              The username for this LDAP account.
      > passcode            Passcode configuration
           + allow-simple-value        Permit the use of repeating, ascending, and descending character sequences
           + auto-lock                 Device automatically locks when time period elapses
           + grace-period              Amount of time the device can be locked without prompting for passcode on
```

```
          unlock
      + max-failed-attempts        Number of passcode entry attempts allowed before all data on device will be
          erased
      + max-passcode-age           Days after which passcode must be changed
      + min-complex-len            Smallest number of non-alphanumeric characters allowed
      + min-passcode-len           Smallest number of passcode characters allowed
      + passcode-history           Number of unique passcodes before reuse
      + require-alphanumeric-value   Require passcodes to contain at least one letter
  > restrictions         Enable use of device features
      + accept-cookies                          Accept cookies
      + allow-adding-game-center-friends          Allow adding Game Center friends
      + allow-app-removal                         Allow removing apps (Supervised Only)
      + allow-auto-sync-when-roaming              Allow automatic sync while roaming
      + allow-bookstore                           Allow Bookstore (Supervised Only)
      + allow-bookstore-erotica                   Allow Erotica (Supervised Only)
      + allow-camera                              Allow use of camera
      + allow-chat                                Allow iMessage (Supervised Only)
      + allow-configuration-profile-installation   Allow Configuration Profile Installation (Supervised Only)
      + allow-diagnostics-submission              Allow diagnostic data to be sent to Apple
      + allow-explicit-content                    Allow explicit music, podcasts and iTunes U
      + allow-facetime                            Allow FaceTime
      + allow-game-center                         Allow use of  Game Center (Supervised Only)
      + allow-icloud-backup                       Allow iCloud backup
      + allow-icloud-doc-sync                     Allow iCloud document sync
      + allow-in-app-purchase                     Allow In-App Purchase
      + allow-installing-apps                     Allow installing apps
      + allow-itunes                              Allow use of iTunes Store
      + allow-multiplayer-gaming                  Allow multiplayer gaming
      + allow-passbook-while-locked               Allow Passbook notifications while locked
      + allow-photo-stream                        Allow Photo Stream (disabling can cause data loss)
      + allow-safari                              Allow use of Safari
      --more--
      + allow-safari-autofill                     Enable autofill
      + allow-screen-capture                      Allow screen capture
      + allow-shared-stream                       Allow Shared Photo Streams
      + allow-siri                                Allow Siri
      + allow-siri-while-locked                   Allow Siri while device locked
      + allow-untrusted-TLS-certificate           Allow user to accept untrusted TLS certificates
      + allow-voice-dialing                       Allow voice dialing
      + allow-youtube                             Allow use of YouTube
      + block-pop-ups                             Block pop-ups
      + enable-safari-javascript                  Enable JavaScript
      + enable-siri-profanity-filter              Enable Siri Profanity Filter (Supervised Only)
      + force-encrypted-backup                    Force encrypted backups
      + force-itunes-password                     Require iTunes Store password for all purchases
      + force-safari-fraud-warning                Force fraud warning
  > security             Controls when the profile can be removed
      > with-authorization   with-authorization
        always               always
        never                never
  > vpn                  VPN
      + connection-name   Display name of the connection (displayed on the device)
      + server            Hostname or IP address for server
      > account           User account for authenticating the connection
```

```
        > proxy-setup    Configures Proxies to be used with VPN connection
        > type           The type of connection enabled by this policy
    > web-clip           Web Clip
        + full-screen   Displays the web clip as a full screen application
        + icon          The icon to use for the Web Clip
        + label         The name to display for the Web Clip
        + precomposed   The icon will be displayed with no added visual effects
        + removable     Enable removal of the Web Clip
        + url           The URL to be displayed when opening the Web Clip
    > wifi               wifi configuration
        + auto-join      Automatically join the network
        + hidden         Enable if network is not open or is not broadcasting
        + service-id     identification of wireless network to connect to
        > proxy-setup    Configures Proxies to be used with this network
        > security-type  Wireless network authentication and encryption
> ios-provisioning       iOS Provisioning Profiles (specify value)
    + app-identifier     app-identifier
    + creation-date      creation-date
    + expiration-date    expiration-date
    + profile            profile
    + profile-identifier  profile-identifier
> scep — scep (specify value)
    + fingerprint                  Hex String to use as a fingerprint
    + keysize                      Key size in bits
    + name                         Name of the SCEP server
    + nt-principal-name            An NT principal name for use in the certificate request
    + retries                      Number of times to retry after a PENDING response
    + retry-delay                  Number of seconds to wait before each retry
    + scep-url                     The base URL for the SCEP server
    + subject                      Representation of a X.500 name
    + subject-alternative-name      The value of a subject alternative name
    + subject-alternative-name-type  The type of a subject alternative name
    + use-as-digital-signature      Use as digital signature
    + use-for-key-encipherment      Use for key encipherment
    > scep-challenge               Challenge for SCEP server configuration on mobile clients
```

Required Privilege Level

superuser, deviceadmin

set setting

Configures limits on device resources.

Syntax

```
set setting resource max-devices <value>
```

Options

> resource   Limits on resources used by this vsys
   + max-devices — Maximum number of devices allowed

Required Privilege Level

superuser, deviceadmin

set shared admin-role

Specifies the access and responsibilities that are assigned to administrative users.

Syntax

```
set shared admin-role <name>
   {
   description <value> |
   role
     {
     device
        {
        cli {deviceadmin | devicereader | superreader | superuser} |
        webui
           {
           commit {disable | enable | read-only} |
           dashboard {disable | enable | read-only} |
           devices {disable | enable | read-only} |
           device-actions <value> {disable | enable | read-only} |
           monitor
              {
              view-custom-reports {disable | enable | read-only} |
              custom-reports
              {
                 hipmatch {disable | enable | read-only} |
                 hostinfo {disable | enable | read-only} |
              }
              logs
                 {
                 configuration {disable | enable | read-only} |
                 hipmatch {disable | enable | read-only} |
                 mdm {disable | enable | read-only} |
                 system {disable | enable | read-only} |
              pdf-reports {
                 email-scheduler {disable | enable | read-only} |
                 manage-pdf-summary {disable | enable | read-only} |
                 pdf-summary-reports {disable | enable | read-only} |
                 report-groups {disable | enable | read-only} |
                 }
           policies {
              policy-rulebase {disable | enable | read-only} |
              configurations {
                 android {disable | enable | read-only} |
                 ios {disable | enable | read-only} |
                 provisioning-profiles {disable | enable | read-only} |
                 scep {disable | enable | read-only} |
                 web-clip-icons {disable | enable | read-only} |
              }
           privacy {disable | enable} |
              show-full-ip-address {disable | enable} |
              show-user-names-in-logs-and-reports {disable | enable} |
           }
           setup {
              admin-roles {disable | enable | read-only} |
              administrators {disable | enable | read-only} |
              authentication-profile {disable | enable | read-only} |
              authentication-sequence {disable | enable | read-only} |
              config-audit {disable | enable | read-only} |
              dynamic-updates {disable | enable | read-only} |
              licenses {disable | enable | read-only} |
              master-key {disable | enable | read-only} |
              network {disable | enable | read-only} |
              scheduled-log-export {disable | enable | read-only} |
              settings {disable | enable | read-only} |
              software {disable | enable | read-only} |
              support {disable | enable | read-only} |
              tags {disable | enable | read-only} |
              virtual-systems {disable | enable | read-only} |
              certificate-management {
                 certificate-profile {disable | enable | read-only} |
                 certificates {disable | enable | read-only} |
              }
              log-settings {
                 config {disable | enable | read-only} |
                 hipmatch {disable | enable | read-only} |
                 manage-log {disable | enable | read-only} |
                 mdm {disable | enable | read-only} |
                 system {disable | enable | read-only} |
                 }
              server-profile
                 email {disable | enable | read-only} |
                 kerberos {disable | enable | read-only} |
                 ldap {disable | enable | read-only} |
                 radius {disable | enable | read-only} |
                 snmp-trap {disable | enable | read-only} |
                 syslog {disable | enable | read-only} |
                 }
              user-database {
              directory-integration {disable | enable | read-only} |
              user-groups {disable | enable | read-only} |
              users {disable | enable | read-only} |
              }
           }
        xmlapi
           {
           commit {disable | enable} |
           config {disable | enable} |
           export {disable | enable} |
           import {disable | enable} |
           log {disable | enable} |
           op {disable | enable} |
           report {disable | enable} |
           }
        }
```

Options

```
<name> — Shared administrative role name
+ description — Description text
> role — Sets access and responsibilities for the role
    > device — Device settings
        + cli — Command Line Interface access
            - deviceadmin — Device Administrator
            - devicereader — Device Reader
            - superreader — Super Reader
            - superuser — Super User
        > webui — Sets enable, disable, or read-only access to the web user interface
            + commit — Commit
            + dashboard — Dashboard
            + devices — Devices (enable/disable)
            > device-actions — Device settings
                + check-in
                + delete— Admin roles
                + import — Administrators
                + locate — Authentication profile
                + lock — Authentication sequence
                + message — Block pages
                + push-policy — Configuration audit
                + show-pending — Dynamic updates
                + tag — GlobalProtect Client
                + unenroll— High Availability
                + unlock — Licenses
                + view-imported— Disable, enable, or read-only device master key
                + wipe— Password profiles
            > monitor — Monitor settings
                + view-custom-reports — View custom reports (enable/disable)
                > custom-reports — Custom report settings
                    + hipmatch — hipmatch report
                    + hostinfo — host info report
                > logs — Logs settings
                    + configuration — Configuration logs
                    + hipmatch — HIPmatch logs
                    + mdm — Mobile Security Manager logs
                    + system — System logs
                > pdf-reports — PDF reports
                    + email-scheduler — Email scheduler
                    + manage-pdf-summary — manage PDF summary
                    + pdf-summary-reports — PDF summary reports
                    + report-groups — Report groups
            > policies — Policy settings
                + policy-rulebase — Application override rulebase
                > configurations— Policy configurations
                    +  android— Enabled/disable/read-only
                    + ios— Enabled/disable/read-only
                    + provisioning-profiles— Enabled/disable/read-only
                    + scep — Enabled/disable/read-only
                    + web-clip-icons — Enabled/disable/read-only
                > hip
                    + data-collection — Enabled/disable/read-only
                    + hip-notifications — Enabled/disable/read-only
                    + hip-objects — Enabled/disable/read-only
                    + hip-profiles — Enabled/disable/read-only
            > privacy — Privacy settings
                + show-full-ip-addresses — Show full IP addresses
                + show-user-names-in-logs-and-reports — Show user names in logs and reports
            > setup — Other setup settings (enable/disable/read-only)
                + admin-roles
                + administrator
                + authentication-profile
                + authentication-sequence
                + config-audit
                + dynamic-updates
                + licenses
                + master-key
                + network
                + scheduled-log-export
                + settings
                + software
                + support
                + tags
                + virtual-systems
                > certificate-management
                    + certificate-profile
                    + certificates
                > log-settings
                    + config
                    + hipmatch
                    + manage-log
                    + mdm
                    + system
                > server-profile
                    + email
                    + kerberos
                    + ldap
                    + radius
                    + snmp-trap
                    + syslog
                > user-database
                    + directory-integration
                    + user-groups
                    + users
        > xmlapi — Sets enable or disable access to the XML API user interface
            + commit — Commit
            + config — Configuration
            + export — Export
            + import — Import
            + log — Log
            + op — Operation
            + report — Report
            + user-id — User ID
```

Required Privilege Level

superuser, deviceadmin

set shared authentication-profile

Specifies local database, RADIUS, or LDAP settings for assignment to administrator accounts, SSL VPN access, and captive portal. When an administrator attempts to log in to the firewall directly or through an SSL VPN or captive portal, the firewall checks the authentication profile that is assigned to the account and authenticates the user based on the authentication settings.

Syntax

```
set shared authentication-profile <group_name> |
   {
   allow-list {all | <value>} |
   lockout |
     {
     failed-attempts <value> |
     lockout-time <minutes>
     }
   method
     {
     kerberos {server-profile <object_name>} |
     ldap |
        {
        login-attribute <value> |
        passwd-exp-days <value> |
        server-profile <name>
        }
     radius {server-profile <object_name>}
     local-database |
     none
     }
   }
```

Options

<group_name> — Specify group to share the profile
+ allow-list — List of allowed users and groups enclosed in [ ]; option to specify all
> lockout — Network user login lockout settings
    + failed-attempts — Number of failed login attempts to trigger lock-out
    + lockout-time — Number of minutes to lock-out
> method — method
    > kerberos — Kerberos authentication
        + server-profile — Kerberos server profile object
    > ldap — Lightweight Directory Access Protocol (LDAP) authentication
        + login-attribute — Login attribute in LDAP server to authenticate against; default = uid
        + passwd-exp-days — Days until the password expires
        + server-profile — LDAP server profile object
    > radius — Remote Authentication Dial In User Service (RADIUS) authentication
        + server-profile — RADIUS server profile object
    - local-database — Local database authentication
    - none — No authentication

Required Privilege Level

superuser, deviceadmin

set shared authentication-sequence

Specifies a set of authentication profiles that are applied in order when a user attempts to log in to the firewall. Useful in environments where user accounts (including guest and other accounts) reside in multiple directories. The firewall tries each profile in sequence until the user is identified. Access to the firewall is denied only if authentication fails for any of the profiles in the authentication sequence.

For information on configuring authentication profiles using the CLI, refer to “set shared authentication-profile” on page 650.

Syntax

```
set shared authentication-sequence <name>
   {
   authentication-profiles <value> |
   lockout
     {
     failed-attempts <value> |
     lockout-time <value>
     }
   }
```

Options

<name> — Authentication sequence name
+ authentication-profiles — Authentication profiles to apply in the sequence (name or list of names enclosed in [ ])
> lockout — Network user login lockout settings
    + failed-attempts— Number of failed login attempts to trigger lock-out (0-10)
    + lockout-time— Number of minutes to lock-out (0-60)

Required Privilege Level

superuser, deviceadmin

set shared certificate

Specifies settings for security certificates.

Syntax

```
set shared certificate <name> |
   {
   common-name <value> |
   expiry-epoch <value> |
   issuer <value> |
   issuer-hash <value> |
   not-valid-after <value> |
   not-valid-before <value> |
   revoke-date-epoch <value> |
   status {revoked | valid} |
   subject <value> |
   subject-hash <value> |
   csr <value> |
   private-key <value> |
   public-key <value>
   }
```

Options

<name> — Shared certificate name
+ common-name — Common name value
+ expiry-epoch — Expiry epoch value
+ issuer — Issuer value
+ issuer-hash — Issuer-hash value
+ not-valid-after — Not-valid-after value
+ not-valid-before — Not-valid-before value
+ revoke-date-epoch — Revoke date epoch value
+ status — Status (revoked or valid)
+ subject — Subject value
+ subject-hash — Subject-hash value
> csr — Certificate Signing Request (CSR) value
> private-key — Private key value
> public-key — Public key value

Required Privilege Level

superuser, deviceadmin

set shared certificate-profile

Specifies settings for client security certificates. You can create client certificate profiles and then attach a profile to an administrator login on the Setup page or to a Secure Socket Layer (SSL) virtual private network (VPN) login for authentication purposes.

Syntax

```
set shared certificate-profile <name> |
   {
   cert-status-timeout <value> |
   crl-receive-timeout <value> |
   domain <name> |
   ocsp-receive-timeout <value> |
   use-crl {no | yes} |
   use-ocsp {no | yes} |
   CA <name> |
     {
     default-ocsp-url <value> |
     ocsp-verify-ca <value>
     }
   username-field
     {
     subject common-name |
     subject-alt {email | principal-name}
     }
   }
```

Options

<name> — Profile name
+ cert-status-timeout — Set certificate status query timeout value in seconds (0-60)
+ crl-receive-timeout — Set CRL receive timeout value in seconds (0-60)
+ domain — Domain name (alphanumeric string [0-9a-zA-Z._-])
+ ocsp-receive-timeout — Set OCSP receive timeout value in seconds (0-60)
+ use-crl — Use Certificate Revocation List (CRL)
+ use-ocsp — Use Online Certificate Status Protocol (OCSP)
> CA — Certificate Authority (CA) name
    + default-ocsp-url — Default URL for OCSP verification
    + ocsp-verify-ca — CA file for OCSP response verify
> username-field — User name field population
    > subject — Get user name from subject
    > subject-alt — Get user name from subject alternative name (email or principal name)

Required Privilege Level

superuser, deviceadmin

set shared email-scheduler

Specifies shared settings for email delivery of PDF summary reports.

Syntax

```
set shared email-scheduler <name>
   {
   email-profile <value> |
   recipient-emails <value> |
   report-group <value> |
   recurring
     {
     weekly {friday | monday | saturday | sunday | thursday | tuesday |
        wednesday} |
     daily |
     disabled
     }
   }
```

Options

<name> — Specifies the name for the email scheduler
+ email-profile — Email profile value
+ recipient-emails — Recipient emails value
+ report-group — Report group value
> recurring — Recurring frequency
   > weekly — Once a week; specify the day
   - daily — Every day
   - disabled — No scheduling

Required Privilege Level

superuser, deviceadmin

set shared icon

Configures a shared icon for mobile devices.

Syntax

```
set icon <name>
   {
   description <value> |
   image <name> |
   }
```

Options

<name> — Name to identify the icon
+ description — Icon description
+ image — Icon image

Required Privilege Level

superuser, deviceadmin

set shared local-user-database

Configures a local database on the firewall to store authentication information for administrator access, captive portal, and Secure Socket Layer (SSL) virtual private network (VPN) remote users.

Syntax

```
set shared local-user-database
   {
   user <name> |
     {
     disabled {no | yes} |
     phash <value> |
     password
     }
   user-group <name> {user <value>}
   }
```

Options

> user — User name
    + disabled — Disabled (no or yes)
    + phash — phash value
    password—Prompts to set password
> user-group — User group name
    > user — User name or list of names enclosed in [ ]

Required Privilege Level

superuser, deviceadmin

set shared log-settings

Configures log settings on the firewall.

Syntax

```
set shared log-settings
   {
   config |
     {
     any
        {
        send-email using-email-setting <value> |
        send-snmptrap using-snmptrap-setting <value> |
        send-syslog using-syslog-setting <value>
        }
     }
   email <name> |
     {
     format |
        {
        config <value> |
        hip-match <value> |
        system <value> |
        escaping {escape-character <value> | escaped-characters <value>}
        }
     server <name>
        {
        and-also-to <value> |
        display-name <name> |
        from <value> |
        gateway <value> |
        to <value>
        }
     }
   hipmatch |
     {
     any
        {
        send-email using-email-setting <value> |
        send-snmptrap using-snmptrap-setting <value> |
        send-syslog using-syslog-setting <value>
        }
   mdm |
     {
     critical | high | informational | low | medium
        {
        send-email using-email-setting <value> |
        send-syslog using-syslog-setting <value>
        }

     }}
   snmptrap <name> |
     {
     version
        {
        v2c server <name> |
           {
           community <value> |
           manager <value> |
           }
        v3 server <name>
           {
           authpwd <value> |
           engineid <value> |
           manager <value> |
           privpwd <value> |
           user <value>
           }
        }
     }
   syslog <name>
     {
     format |
        {
        config <value> |
        hip-match <value> |
        system <value> |
        escaping {escape-character <value> | escaped-characters <value>}
        }
     server <name>
        {
        facility {LOG_LOCAL0 | LOG_LOCAL1 | LOG_LOCAL2 | LOG_LOCAL3 |
           LOG_LOCAL4 | LOG_LOCAL5 | LOG_LOCAL6 | LOG_LOCAL7 | LOG_USER} |
        format {BSD | IETF}
        port <value> |
        server <value> |
        transport {SSL | TCP | UDP}
        }
     }
   system {critical | high | informational | low | medium}
     {
     send-email using-email-setting <value> |
     send-snmptrap using-snmptrap-setting <value> |
     send-syslog using-syslog-setting <value>
     }
   }
```

Options

> config — Configuration log settings (any)
> > send-email — Send email using email setting value
> > send-snmptrap — Send SNMP trap using SNMP trap setting value
> > send-syslog — Send syslog using syslog setting value
> email — Email log settings name
> > format — Custom formats for forwarded logs

```
            + config — Config value
            + hip-match — HIP match value
            + system — System value
            > escaping — Escaping values
                + escape-character — Escape character
                + escaped-characters — List of characters to be escaped
        > server — Server address
            + and-also-to — Email address (e.g. admin@mycompany.com)
            + display-name — Display name of server
            + from — Email address (e.g. admin@mycompany.com)
            + gateway — IP address or FQDN of SMTP gateway to use
            + to — Email address (e.g. admin@mycompany.com)
    > hipmatch — HIP match log settings
        > any — Specify values
            > send-email — Send email using email setting value
            > send-snmptrap — Send SNMP trap using SNMP trap setting value
            > send-syslog — Send syslog using syslog setting value
    > mdm — Mobile Security Manager log settings (critical, high, informational, low, medium)
        > send-email — Add using-email-setting with value
        > send-syslog — Include using syslog-setting with value
    > snmptrap — SNMP trap log settings
        > version v2c server — Server address
            + community — Community value
            + manager — IP address or FQDN of SNMP manager to use
        > version v3 server — Server address
            + authpwd — Authentication Protocol Password
            + engineid — A hex number in ASCII string
            + manager — IP address or FQDN of SNMP manager to use
            + privpwd — Privacy Protocol Password
            + user — User value
    > syslog — syslog settings
        > format — Custom formats for forwarded logs (escaping)
            + config — Config value
            + hip-match — HIP match value
            + system — System value
            > escaping — Escaping values
                + escape-character — Escape character
                + escaped-characters — List of characters to be escaped
        > server — Server address
            + facility — Facility (LOG_LOCAL0, LOG_LOCAL1, LOG_LOCAL2, LOG_LOCAL3,
                LOG_LOCAL4, LOG_LOCAL5, LOG_LOCAL6, LOG_LOCAL7, LOG_USER)
            + format — BSD or IETF
            + port — Port (1-65535)
            + server — IP address or FQDN of SYSLOG server to use
            + transport — Transport protocol (SSL, TCP, or UDP)
    > system — System log settings (critical, high, informational, low, or medium)
        > send-email — Send email using email setting value
        > send-snmptrap — Send SNMP trap using SNMP trap setting value
        > send-syslog — Send syslog using syslog setting value
```

Required Privilege Level

superuser, deviceadmin

set shared pdf-summary-report

Specifies shared format settings for PDF summary reports.

Syntax

```
set shared pdf-summary-report <name>
   {
   custom-widget <name> |
     {
     chart-type {bar | line | pie | table} |
     column <value> |
     row <value>
     }
   footer {note <value>} |
   header {caption <value>}|
   predefined-widget <name> |
     {
     chart-type {bar | line | pie | table} |
     column <value> |
     row <value>
     }
   }
```

Options

<name> — PDF report to configure
> custom-widget — Report widget layout information
   + chart-type — Chart type (bar, line, pie, or table)
   + column — Column number (1-3)
   + row — Row number (1-6)
> footer — Footer information for PDF summary layout
   + note — Static string to be printed as a note
> header — Header information for PDF summary layout
   + caption — Caption for the layout
> predefined-widget — Predefined report widget layout information
   + chart-type — Chart type (bar, line, pie, or table)
   + column — Column number (1-3)
   + row — Row number (1-6)

Required Privilege Level

superuser, deviceadmin

set shared report-group

Specifies settings for report groups. Report groups allow you to create sets of reports that the system can compile and send as a single aggregate PDF report with an optional title page and all the constituent reports included.

Syntax

```
set shared report-group <name> |
   {
   title-page {no | yes} |
   custom-widget <value> |
     {
     custom-report <value> |
     log-view <value> |
     pdf-summary-report <value>
     predefined-report <value>
     }
   variable <name> {value <value>}
   }
```

Options

<name> — Report group to configure
+ title-page — Include title page
> custom-widget — Custom-widget value
   > custom-report — Custom report value
   > log-view — Log view value
   > pdf-summary-report — PDF summary report value
   > predefined-report — Predefined report value
> variable — Variable name; option to include a value

Required Privilege Level

superuser, deviceadmin

set shared reports

Specifies shared settings for generating reports.

Syntax

```
set shared reports <name>
   {
   caption <value> |
   disabled {no | yes} |
   end-time <value> |
   frequency daily |
   period {last-12-hrs | last-15-minutes | last-24-hrs | last-30-days | last-
     60-seconds | last-7-calendar-days | last-7-days | last-calendar-day |
     last-calendar-month | last-calendar-week | last-hour} |
   query <value> |
   start-time <value> |
   topm <value> |
   topn <value> |
   type
     {
     hipmatch |
        {
        group-by {day-of-receive_time | hour-of-receive_time | machinename |
           matchname | matchtype | quarter-hour-of-receive_time | src |
           srcuser | vsys} |
        last-match-by time_generated |
        aggregate-by {day-of-receive_time | hour-of-receive_time |
           machinename | matchname | matchtype | quarter-hour-of-
           receive_time | src | srcuser | vsys | <value>} |
        labels <value> |
        values {repeatcnt | <value>}
        }
     hostinfo |
        {
        sortby {encryption-not-set | enrollment-time | has-malware | last-
           checkin-time | last-unenroll-time | mac-address | managed | model
           | os | os-version | passcode-not-set | rooted-or-jailbroken |
           udid | user} |
        aggregate-by {day-of-receive_time | hour-of-receive_time |
           machinename | matchname | matchtype | quarter-hour-of-
           receive_time | src | srcuser | vsys | <value>} |
        labels <value> |
        }
```

Options

<name> — Report to configure
+ caption — Caption value
+ disabled — Disabled (no or yes)

```
+ end-time — End time (e.g. 2008/12/31 11:59:59)
+ frequency — Configure the report to automatically run daily.
+ period — Time period to include in report (last 12 hrs, last 15 minutes, last 24 hrs, last 30 days, last 60 seconds,
     last 7 calendar days, last 7 days, last calendar day, last calendar month, last calendar week, or last hour)
+ query — Query value
+ start-time — Start time (e.g. 2008/01/01 09:00:00)
+ topm — TopM value (1-50)
+ topn — TopN value (1-500)
> type — Report type
     > hipmatch — HIP match report
          + group-by — Select from the list provided
          + last-match-by — Last match by time generated
          > aggregate-by — Select from the list provided or specify a list of values enclosed in [ ]
          > labels — Label value or list of values enclosed in [ ]
          > values — Values (repeat count, or list of values enclosed in [ ])
     > hostinfo — Host information report
          + sortby — sortby (specify item)
          > aggregate-by — aggregate-by (specify item)
          > labels — labels (specify item)
```

Required Privilege Level

superuser, deviceadmin

set shared server-profile

Specifies settings for Kerberos, Lightweight Directory Access Protocol (LDAP), NetFlow, and RADIUS servers.

Syntax

```
set shared server-profile
   {
   kerberos <name> |
     {
     admin-use-only {no | yes} |
     domain <name> |
     realm <name> |
     server <name> {host <value> | port <value>}
     }
   ldap <name> |
     {
     admin-use-only {no | yes} |
     base <value> |
     bind-dn <value> |
     bind-password <value> |
     bind-timelimit <value> |
     disabled {no | yes} |
     domain <name> |
     ldap-type {active-directory | e-directory | none | sun} |
     retry-interval <value> |
     ssl {no | yes} |
     timelimit <value> |
     server <name> {address <value> | port <value>}
     }
   netflow <name> |
     {
     active-timeout {value} |
     export-enterprise-fields {no | yes} |
     server <name> {host {<ip/netmask> | <value>} | port <value>} |
     template-refresh-rate {minutes <value> | packets <value>}
     }
   radius <name>
     {
     admin-use-only {no | yes} |
     checkgroup {no | yes} |
     domain <name> |
     retries <value> |
     timeout <value> |
     server <name> {ip-address <ip_address> | port <value> | secret <value>}
     }
   }
```

Options

> kerberos — Kerberos profile name

```
  + admin-use-only — Can only be used for administrative purposes
  + domain — Domain name to be used for authentication
  + realm — Realm name to be used for authentication
  > server — Server name
    + host — Hostname running Kerberos Domain Controller
    + port — Kerberos Domain Controller (0-65535)
> ldap — LDAP profile name
  + admin-use-only — Can only be used for administrative purposes
  + base — Default base distinguished name (DN) to use for searches
  + bind-dn — Bind distinguished name
  + bind-password — Bind password
  + bind-timelimit — Number of seconds to use for connecting to servers (1-30)
  + disabled — Disabled (no or yes)
  + domain — Domain name to be used for authentication
  + ldap-type — LDAP type (Active Directory, E Directory, SUN, or other)
  + retry-interval — Interval (seconds) for retrying connecting to ldap search (1-3600, default = 60 seconds)
  + ssl — SSL (no or yes)
  + timelimit — number of seconds to wait for performing searches (1-30)
  > server — Server specification
    + address — LDAP server IP address (x.x.x.x or IPv6) or host name
    + port — Port (0-65535)
> netflow — NetFlow profile name
  + active-timeout — Number of minutes for the profile to remain active (1-60)
  + export-enterprise-fields — Include PAN-OS-specific field types in the NetFlow record
  > server — Server name
    + host — NetFlow server IP address and network mask (x.x.x.x/y) or host name
    + port — Port (0-65535)
  > template-refresh-rate — Refresh the NetFlow template ID after the specified number of minutes or packets
    + minutes — Number of minutes before refreshing the NetFlow template ID (1-3600)
    + packets — Number of packets before refreshing the NetFlow template ID (1-600)
> radius — RADIUS profile name
  + admin-use-only — Can only be used for administrative purposes
  + checkgroup — Retrieve user group from RADIUS
  + domain — Domain name to be used for authentication
  + retries — Number of attempts before giving up authentication (1-5)
  + timeout — Number of seconds to wait when performing authentication (1-30)
  > server — Server name
    + ip-address — RADIUS server IP address (x.x.x.x or IPv6)
    + port — RADIUS server port (0-65535)
    + secret — Shared secret for RADIUS communication
```

Required Privilege Level

superuser, deviceadmin

set shared tags

Configures shared tags.

Syntax

```
set shared tags <name> comment
```

Options

<name> — Specifies tag to configure
    + comment — Specify optional text comment

Required Privilege Level

superuser, deviceadmin

show

Displays information about the current candidate configuration.

Syntax

```
show <context>
```

Options

<context> — Specifies a path through the hierarchy. For available contexts in the hierarchy, press <tab>.

Sample Output

The following command shows the full candidate hierarchy.

```
username@hostname# show
```

The following commands can be used to display the hierarchy segment for *network interface*.

- Specify context on the command line:

  ```
  show setting
  ```

- Use the **edit** command to move to the level of the hierarchy, and then use the **show** command without specifying context:

  ```
  edit setting
  [edit network interface] show
  ```

Required Privilege Level

superuser, deviceadmin

top

Changes context to the top hierarchy level.

Syntax

```
top
```

Options

None

Sample Output

The following command changes context from the network level of the hierarchy to the top level.

```
[edit network]
username@hostname# top

[edit]
    username@hostname#
```

Required Privilege Level

All

up

Changes context to the next higher hierarchy level.

Syntax

```
up
```

Options

None

Sample Output

The following command changes context from the *setting* level of the hierarchy to the network level.

```
[edit setting]
   username@hostname# up

[edit network]
   username@hostname#
```

Required Privilege Level

All

GP-100 GlobalProtect Mobile Security Manager Operation Mode Commands

The Operational Mode commands for the GP-100 GlobalProtect Mobile Security Manager appliance are described in the following sections. For Configuration Mode commands, see “Configuration Mode Commands” on page 587.

- “show counter” on page 744
- “show host-info” on page 746
- “show interface” on page 747
- “show log” on page 750
- “show malware” on page 753
- “show management-clients” on page 754
- “show mobile-device” on page 755
- “show operational-mode” on page 756
- “show query” on page 757
- “show report” on page 758
- “show system” on page 759
- “show user” on page 761
- “ssh” on page 763
- “tail” on page 764
- “test” on page 766
- “traceroute” on page 767

clear

Resets information, counters, sessions, or statistics.

Syntax

```
clear
   {
   job <id> |
   log {alarm | config | hipmatch | mdm | system} |
   query {all-by-session | id <value> |
   report {all-by-session | id <value> |
```

Options

> job— Clears the download job with the specified ID
> log — Clears the specified log (alarm, config, hipmatch, mdm, or system)
> query — Clears counters
   > all-by-session — Clears all query jobs for this session
   > id — Clears the query job with the specified ID
> report — Clears report jobs
   > all-by-session — Clears all report jobs for this session
   > id — Clears the report job with the specified ID

Sample Output

The following command clears the job with ID 223.

```
username@hostname> clear job id 233
Session 2245 cleared
username@hostname>
```

Required Privilege Level

superuser, deviceadmin

configure

Enters Configuration mode.

Syntax

```
configure
```

Options

None

Sample Output

To enter Configuration mode from Operational mode, enter the following command.

```
username@hostname> configure
Entering configuration mode

[edit]
    username@hostname#
```

Required Privilege Level

superuser, deviceadmin

debug authd

Defines settings for authd service debug logging.

Syntax

```
debug authd {off | on | show}
```

Options

> off — Turns off debug logging
> on — Turns on authd service debug logging
> show — Displays current debug logging setting

Sample Output

The following command turns the authd debugging option on.

```
admin@PA-HDF> debug authd on
admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug cli

Defines settings and display information for debugging the CLI connection.

Syntax

```
debug cli
   {
   detail |
   off |
   on |
   show
   }
```

Options

> detail — Shows details information about the CLI connection
> off — Turns the debugging option off
> on — Turns the debugging option on
> show — Shows whether this command is on or off

Sample Output

The following command shows details of the CLI connection.

```
admin@PA-HDF> debug cli detail
Environment variables :
(USER . admin)
(LOGNAME . admin)
(HOME . /home/admin)
(PATH . /usr/local/bin:/bin:/usr/bin)
(MAIL . /var/mail/admin)
(SHELL . /bin/bash)
(SSH_CLIENT . 10.31.1.104 1109 22)
(SSH_CONNECTION . 10.31.1.104 1109 10.1.7.2 22)
(SSH_TTY . /dev/pts/0)
(TERM . vt100)
(LINES . 24)
(COLUMNS . 80)
(PAN_BASE_DIR . /opt/pancfg/mgmt)

PAN_BUILD_TYPE : DEVELOPMENT

Total Heap : 7.00 M
Used       : 5.51 M
Nursery    : 0.12 M
admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug cryptod

Sets the debug options for the cryptod daemon.

Syntax

```
debug cryptod
    {
    global {off | on | show}
    show counters
    }
```

Options

> global — Controls debug levels
    > show — Shows whether this command is on or off
    > off — Turns the debugging option off
    > on — Turns the debugging option on
> show — Shows Cryptod debug counters

Sample Output

The following command displays the current cryptod debugging setting.

```
admin@PA-HDF> debug cryptod global show

sw.cryptod.runtime.debug.level: debug


admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug management-server

Configures settings for debugging the management server.

Syntax

```
debug management-server

   clear |
   client {disable <value> | enable <value>} |
   config version <value> |
   conn |
   db-intervals db {dailythsum | dailytrsum | hourlythsum | hourlytrsum |
      thsum | trsum | weeklythsum | weeklytrsum} |
      {
      end-time <value> |
      period {last-12-hours | last-24-hrs | last-30-days | last-7-calendar-
         days | last-7-days | last-calendar-day | last-calendar-month | last-
         calendar-week | last-hour} |
      start-time <value>
      }
   db-rollup {off | on} |
   log-collector-agent-status |
   log-forwarding-status |
   memory {info | trim} |
   off |
   on {debug | dump | error | info | warn} |
   rolledup-intervals db {dailythsum | dailytrsum | hourlythsum | hourlytrsum
      | thsum | trsum | weeklythsum | weeklytrsum} |
      {
      end-time <value> |
      period {last-12-hours | last-24-hrs | last-30-days | last-7-calendar-
         days | last-7-days | last-calendar-day | last-calendar-month | last-
         calendar-week | last-hour} |
      start-time <value>
      }
   set {all | <name> {all | basic | detail}
   show |
   template dump-config{
      xpath <value> |
      from {local | merged | template}
      }
   unset {all | <name> {all | basic | detail}
   user info name <value>
```

Options

> clear — Clears all debug logs
> client — Enables or disables management server client processes (specify process type)
> conn — Prints management server connection entries
> db-intervals — Displays available summary intervals for a given period
   + end-time — End Time, e.g. 2008/12/31 11:59:59

```
     + period — Select from available time periods
     + start-time — Start Time, e.g. 2008/01/01 09:00:00
     * db — Database to display
> db-rollup — Enables or disables summary database roll up
> log-collector-agent-status — Shows the agent status
> log-forwarding-status — Shows the log forwarding status
> memory — Specifies memory debugging settings (info/trim)
> off — Turns off debug logging
> on — Turns on management server debug logging
     debug — Only output error, warning, info and debug logs
     dump — Output all logs
     error — Only output error logs
     info — Only output error, warning and info logs
     warn — Only output error and warning logs
> rolledup-intervals — Displays summary intervals rolled up optimally into summary-based partial reports
     + end-time — End Time, e.g. 2008/12/31 11:59:59
     + period — Select from available time periods
     + start-time — Start Time, e.g. 2008/01/01 09:00:00
     * db — Database to display
> set — Turns on management server component debug logging
     > all — Debug logging for all components
     > auth — Auth debug logging (all, basic, detail)
     > cfg — CFG debug logging (all, basic, detail)
     > comm — Comm debug logging (all, basic, detail)
     > commit — Commit debug logging (all, basic, detail)
     > commoncriteria — Common Criteria debug logging (all, basic, detail)
     > content — Content debug logging (all, basic, detail)
     > fqdn — FQDN debug logging (all, basic, detail)
     > log — Log debug logging (all, basic, detail)
     > logaction — Log action debug logging (all, basic, detail)
     > logforwarding — Log forwarding debug logging (all, basic, detail)
     > logquery — Log query debug logging (all, basic, detail)
     > proxy — Proxy debug logging (all, basic, detail)
     > report — Report debug logging (all, basic, detail)
     > schema — Schema debug logging (all, basic, detail)
     > server — Server debug logging (all, basic, detail)
     > settings — Settings debug logging (all, basic, detail)
> show — Displays current debug logging setting
> template — Helpers for debugging templates
     + xpath — XPath of part to be dumped
     * from — Dump from specified config tree
          - local — Dumps non-template part of local config
          - merged — Dumps the merged config
          - template — Dumps template part of the local config
> unset — Turns off management server component debug logging
     > all — Debug logging for all components
     > auth — Auth debug logging (all, basic, detail)
     > cfg — CFG debug logging (all, basic, detail)
     > comm — Comm debug logging (all, basic, detail)
     > commit — Commit debug logging (all, basic, detail)
     > commoncriteria — Common Criteria debug logging (all, basic, detail)
     > content — Content debug logging (all, basic, detail)
     > fqdn — FQDN debug logging (all, basic, detail)
     > log — Log debug logging (all, basic, detail)
     > logaction — Log action debug logging (all, basic, detail)
```

> logforwarding — Log forwarding debug logging (all, basic, detail)
> logquery — Log query debug logging (all, basic, detail)
> proxy — Proxy debug logging (all, basic, detail)
> report — Report debug logging (all, basic, detail)
> schema — Schema debug logging (all, basic, detail)
> server — Server debug logging (all, basic, detail)
> settings — Settings debug logging (all, basic, detail)
> user info name— Shows user name information for specified user

Sample Output

The following example turns management server debugging on.

```
admin@PA-HDF> debug management-server on
(null)
admin@PA-HDF>
```

The following example enables the management server network processor agent.

```
admin@PA-HDF> debug management-server client enable npagent

admin@PA-HDF>
```

The following example displays all of the available hourly summary intervals for the trsum database.

```
username@hostname> debug management-server db-intervals period last-calendar-
   day db hourlytrsum

hourlytrsum periods from 2011/06/15 00:00:00 to 2011/06/15 23:59:59

    hourlytrsum 2011/06/15 00:00:00 to 2011/06/15 11:59:59
    hourlytrsum 2011/06/15 13:00:00 to 2011/06/15 23:59:59
```

The following example displays the breakdown of the trsum report into summary-based partial reports.

```
username@hostname> debug management-server rolledup-intervals period last-7-
   days db trsum

Rolled up periods from 2011/02/17 14:03:38 to 2011/02/24 14:03:37

          trsum 2011/02/17 14:03:38 to 2011/02/19 23:59:59
     dailytrsum 2011/02/20 00:00:00 to 2011/02/23 23:59:59
    hourlytrsum 2011/02/24 00:00:00 to 2011/02/24 13:59:59
```

Required Privilege Level

superuser, vsysadmin

debug master-service

Configures settings for debugging the master service.

Syntax

```
debug master-service
    {
    internal-dump |
    off |
    on {debug | dump | error | info | warn} |
    show
    }
```

Options

> internal-dump — Dumps internal state of service to its log
> off — Turns off debug logging
> on — Turns on masterd service debug logging
    debug — Only output error, warning, info and debug logs
    dump — Output all logs
    error — Only output error logs
    info — Only output error, warning and info logs
    warn — Only output error and warning logs
> show — Displays current debug logging setting

Sample Output

The following command dumps the internal state of the master server to the log.

```
admin@PA-HDF> debug master-service internal-dump

admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug mdmd

Configures settings for debugging Mobile Security Manager devices.

Syntax

```
debug mdmd
    {
    clear
      {domain-map |
      group {all | <value>} |
      log |
      pending-actions filter <value>
      } |
    db {count <value> | find <value>} |
    encrypt-configure-profile {no | yes} |
    get |
    ignore-client-cert {no | yes}|
    off |
    on <level> |
    refresh directory-integration {all | <value> |
    reset {cloud-connection | directory-integration | gateway-connection |
      stats} |
    set
      agent {all | basic | detail} |
      all |
      base {all | config | id} |
      comm {all | basic | detail} |
      db {all | basic | detail} |
      hip {all | basic | detail} |
      ldap {all | basic | detail} |
      mdm {all | apns | app | basic | cloud | detail | device | gsm,user |
         warn} |
      misc {all | misc}
      }
    show {cloud-stats | gateway-connection | log-stats | memory | setting |
      stats | thread-state} |
    unset |
    use-cloud-notifications |
    }
```

Sample Output

The following command configures debugging settings to ignore verification of the client certificate.

```
admin@PA-HDF> debug mdmd ignore-client-cert yes
admin@PA-HDF>
```

Options

- > clear — Clear data
  - > domain-map — Clear the domain map
  - > group — Clear group data (specify value or all)
  - > log — Clear debug logs
  - > pending-actions — Clear pending actions for devices (can specify device filter)
- > db — Run command vs database
  - > count — Count HIP database (specify number)
  - > find — Find in HIP database (specify value to match)
- > encrypt-configure-profile — Specify whether to encrypt iOS configuration profile (yes or no)
- > get — Display current debug logging setting
- > ignore-client-cert — Specify whether to ignore the verification of client cert
- > off — Turn off debug logging
- > on — Turn on debug logging (specify level: debug, dump, error, info, or warn)
- > refresh — Refresh data
  - > directory-integration (specify all of value)
- > reset — Reset data
  - > cloud-connection — Reset cloud connection
  - > directory-integration — Reset group mapping data (specify all or value)
  - > gateway-connection — Reset gateway connection
  - > stats — Reset mdm statistics
- > set — Turn on component debug logging
  - > agent (specify all, basic, or detail)
  - > all
  - > base (specify all, config, or id)
  - > comm (specify all, basic, or detail)
  - > db (specify all, basic, or detail)
  - > hip (specify all, basic, or detail)
  - > ldap (specify all, basic, or detail)
  - > mdm (specify all, apns, app, basic, cloud, detail, device, gsm,user, or warn)
  - > misc (specify all or misc)
- > show — Show debug data
  - > cloud-stats — Show cloud connection statistics
  - > gateway-connection — Show GlobalProtect Gateway Connections (specify detail or summary)
  - > log-stats — Show log statistics
  - > memory — Show memory usage (specify detail or summary)
  - > setting — Show debug setting
  - > stats — Show mdm process statistics (can specify all)
  - > thread-state — Show daemon threads
- > unset — Turn off component debug logging
- > use-cloud-notifications — Specify whether to use or turn off cloud notifications for testing purposes

Required Privilege Level

superuser, vsysadmin

debug software

Configures software processes debugging features.

Syntax

```
debug software
   {
   core { management-server | mdmd | web-server} |
   fd-limit {limit <value> | service <value>} |
   no-fd-limit service <value> |
   no-virt-limit service <value> |t
   restart {appdb | hipdb | management-server | mdmd | web-server} |
   trace {management-server | mdmd | web-server} |
   virt-limit {limit <value> | service <value>}
   }
```

Options

> core — Debugs process core
   > management-server — Management server process
   > mdmd — Mobile Security Manager process
   > web-server — Web server process
> fd-limit — Sets open fd limit (0-4294967295) and service value
> no-fd-limit — Disables open fd limit service
> no-virt-limit — Disables maximum virtual memory limit service
> restart — Restarts processes
   > appdb — App database process
   > hipdb— HIP database process
   > management-server — Management server process
   > mdmd — Mobile Security Manager process
   > web-server — Web server process
> trace — Gets process backtraces
   > management-server — Management server process
   > mdmd— Mobile Security Manager process
   > web-server — Web server process
> virt-limit — Sets maximum virtual memory limit (0-4294967295) and service value

Sample Output

The following command restarts the web server.

```
admin@PA-HDF> debug software restart web-server

admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug swm

Configures settings for debugging the Palo Alto Networks software manager.

Syntax

```
debug swm
   {
   history |
   info {image <image_name>} |
   install {image <image_name> | patch <value>} |
   list |
   load {image <image_name>} |
   log |
   rebuild-content-db |
   refresh content |
   revert |
   status |
   unlock
   }
```

Options

> history — Shows history of software install operations
> info — Displays info on current or specified image
> install — Installs specified image and optional patch
> list — Lists software versions available for install
> load—Loads specified image
> log — Shows log of PAN Software Manager
> rebuild-content-db—Rebuilds content database
> refresh — Reverts back to last successfully installed content
> revert — Reverts back to last successfully installed software
> status — Shows status of PAN Software Manager
> unlock — Unlocks PAN Software Manager

Sample Output

The following command shows the list of available software versions.

```
admin@PA-HDF> debug swm list

3.1.0-c4.dev
3.1.0-c1.dev_base
3.0.0-c207
3.0.0-c206
admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug system

Defines settings for system debugging actions.

Syntax

```
debug system
   {
   check-fragment |
   disk-smart-info disk-1 |
   disk-sync |
   maintenance-mode |
   route-table {ethernet1 | management}
   }
```

Options

> check-fragment — Checks disk fragmentation
> disk-smart-info — Get disk drive SMART information
> disk-sync — Flushes all writes out to disk
> maintenance-mode — Reboots the system to maintenance mode
> route-table—Show ip route table (specify ethernet1 or management}

Sample Output

The following command reboots the system to maintenance mode.

```
admin@PA-HDF> debug system maintenance-mode
admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug tac-login

Configures settings for debugging the Palo Alto Networks Technical Assistance Center (TAC) connection.

Syntax

```
debug tac-login {challenge | permanently-disable | response}
```

Options

> challenge — Gets challenge value for TAC login
> permanently-disable — Permanently turns off TAC login debugging
> response — Runs verification of challenge response for TAC login

Sample Output

The following command runs the verification of the response value for TAC debugging.

```
admin@PA-HDF> debug tac-login response
Defaulting to root passwd login in debug mode
Password:

admin@PA-HDF>
```

Required Privilege Level

superuser, vsysadmin

debug user

Configures settings for debugging user accounts.

Syntax

```
debug user
{
   clear {domain-map | group {all | <value>} | log} |
   dump {domain-map | id {all | id <value> | name <value>} | state} |
   refresh group-mapping {all | id <value> |
   refresh group-mapping {all | id <value>
}
```

Options

> clear — Clear data.
>> domain-map — Clear domain map
>> group — Clear group data (all or value)
>> log — Clear debug logs

> dump — Dump debug data
>> domain-map — Dump domain map
>> id — Dump id data
>>> all — Display all name and id
>>> id
>>> name
>>> state

> refresh — Refresh data (group-mapping all or value)
> reset — Reset data (group-mapping all or value)

Sample Output

The following command clears all user group information for debugging.

```
username@hostname> debug user clear group all


username@hostname>
```

Required Privilege Level

superuser, vsysadmin

delete

Removes specified types of files from disk or restore the default comfort pages that are presented when files or URLs are blocked.

Syntax

```
delete
   {
   admin-sessions |
   config |
      saved <file_name>
   config-audit-history |
   content |
      {
      cache |
         {
         curr-content type {aho-regex | all | decoder | dfa | sml | tdb}
            version <value> |
         old-content
         }
      update <file_name>
      }
   core {management-plane file <file_name>} |
   license key <value> |
   logo |
   pcap directory <directory_name> |
   radius-user {admin-name <name>} |
   report |
      {
      custom scope <name> report-name <name> file-name <name> |
      predefined scope <name> report-name <name> file-name <name> |
      summary scope <name> report-name <name> file-name <name>
      }
   software {image <file_name> | version <value>} |
   ssh-authentication-public-key |
   sslmgr-store |
      {
      certificate-info {portal} |
         {
         db-serialno <value> |
         name <value> |
         serialno <value>
         }
      satellite-info {portal} |
         {
         name <value> |
         serialno <value> |
         state {assigned | unassigned}
         }
      satellite-info-revoke-certificate portal <value> {serialno <value>}
      }
   user-file ssh-known-hosts |
        }
```

Options

> admin-sessions — Removes all active administrative sessions
> config — Removes configuration files on disk
    > repo — Config repository
        * device — Device name
        > file — Named snapshot
        > running-config — Versioned running configuration
    > saved — Filename
> config-audit-history — Removes the configuration audit history
> content — Removes content images or cache on disk
    > cache — Removes cache files based
        > curr-content — Removes cache files based on Engine version and type
            * type — Type of content to be deleted
                aho-regex — Aho-regex cache
                all — All caches
                decoder — Decoder cache
                dfa — DFA cache
                sml — SML cache
                tdb — TDB cache
            * version — Content version to delete
        > old-content — Remove ALL old content
    > update — Filename to remove
> core — Removes core management or data plane cores on disk
> license — Removes a license key file
> logo — Removes a custom logo file
> pcap — Removes packet capture files
> radius-user— Removes a RADIUS user’s local account
> report — Removes specified reports (custom, predefined, or summary)
> software — Removes a software image
> ssh-authentication-public-key — Deletes SSH authentication public key
> sslmgr-store — Deletes the specified SSL manager dynamic configuration
> user-group-cache — Deletes user group cache files in disk

Sample Output

The following command deletes the saved configuration file named *running-config.xml.bak*.

```
username@hostname> delete config saved running-config.xml.bak
username@hostname>
```

Required Privilege Level

superuser, deviceadmin

exit

Exits the PAN-OS CLI.

> ***Note:*** *The* ***exit*** *command is the same as the* ***quit*** *command.*

Syntax

```
exit
```

Options

None

Required Privilege Level

All

find

Lists CLI commands containing the specified keyword.

Syntax

```
find command keyword <value>
```

Options

<value> — Specifies a keyword.

Sample Output

The following command lists all CLI commands containing the keyword mdm.

```
username@hostname# find command keyword mdm
debug mdmd on <error|warn|info|debug|dump>
debug mdmd encrypt-configure-profile <yes|no>
debug mdmd ignore-client-cert <yes|no>
debug mdmd use-cloud-notifications <yes|no>
debug mdmd set agent <basic|detail|all>
debug mdmd set base <config|id|all>
...
username@hostname#
```

Required Privilege Level

All

grep

Finds and lists lines from log files that match a specified pattern.

Syntax

```
grep pattern <value>
   {
   after-context <number> |
   before-context <number> |
   context <number> |
   count |
   ignore-case {no | yes} |
   invert-match {no | yes} |
   line-number {no | yes} |
   max-count <number> |
   no-filename {no | yes} |
   dp-log <file_name> |
   mp-log <file_name>
   }
```

Options

+ after-context — Prints the matching lines plus the specified number of lines that follow the matching lines
+ before-context — Prints the matching lines plus the specified number of lines that precede the matching lines
+ context — Prints the specified number of lines in the file for output context
+ count — Specifies whether a count is included in the results
+ ignore-case — Ignores case distinctions
+ invert-match — Selects non-matching lines instead of matching lines
+ line-number — Adds the line number at the beginning of each line of output
+ max-count — Stops reading a file after the specified number of matching lines
+ no-filename — Does not add the filename prefix for output
* pattern — Indicates the string to be matched
> dp-log — Indicates the data plane log file to search for the pattern (press <tab> for a list of file names)
> mp-log — Indicates the management plane log file to search for the pattern (press <tab> for a list of file names)

Sample Output

The following command searches the *brdagent.log* file for occurrences of the string “HEARTBEAT.”

```
username@hostname> grep dp-log sysdagent.log pattern HEARTBEAT
*
Jan 20 14:35:48 HEARTBEAT: Heartbeat failure on core 4
Jan 20 14:35:53 HEARTBEAT: Heartbeat failure on core 1
Jan 20 14:35:54 HEARTBEAT: Heartbeat failure on core 8
Jan 20 14:35:55 HEARTBEAT: Heartbeat failure on core 2
username@hostname>
```

Required Privilege Level

All

less

Lists the contents of the specified log file.

Note: The `dp-log` option will not be available on devices that do not have a dataplane, such as the PA-200.

Syntax

```
less
    {
    dp-log <filename> |
    mp-backtrace <filename> |
    mp-log <filename> |
    webserver-log <filename>
    }
```

Options

> dp-log — Lists contents of the specified data plane log file (press <tab> for a list of log files)
> mp-backtrace — Lists contents of the specified management plane backtrace file (press <tab> for a list of log files)
> mp-log — Lists contents of the specified management plane log file (press <tab> for a list of log files)
> webserver-log — Lists contents of the specified webserver log file (press <tab> for a list of log files)

Sample Output

The following command lists the contents of the web server error log.

```
username@hostname> less webserver-log error.log
   default:2 main  Configuration for Mbedthis Appweb
   default:2 main  -------------------------------------------
   default:2 main  Host:               pan-mgmt2
   default:2 main  CPU:                i686
   default:2 main  OS:                 LINUX
   default:2 main  Distribution:       unknown Unknown
   default:2 main  OS:                 LINUX
   default:2 main  Version:            2.4.0.0
   default:2 main  BuildType:          RELEASE
   default:2 main  Started at:         Mon Mar  2 12
   ...
```

Required Privilege Level

All

ls

Displays debug file listings.

Syntax

```
ls
   {
   long-format {no | yes} |
   reverse-order {no | yes} |
   sort-by-time {no | yes} |
   content {apps | cache | decoders | global | pan_appversion | scripts |
     threats} |
   database <value> |
   global <filename> |
   mp-backtrace <filename> |
   mp-global <filename> |
   mp-log <filename> |
   webserver-log <filename>
   }
```

Options

+ long-format — File listing format (use long format)
+ reverse-order — File listing order (list in reverse order)
+ sort-by-time — Sort file listing by time
> content — Specify content to display
> database — Database listing
> global — Global files (select file from the list provided; press <tab> for list)
> mp-backtrace — MP backtrace file (select file from the list provided; press <tab> for list)
> mp-global — MP global files (select file from the list provided; press <tab> for list)
> mp-log — MP logs (select file from the list provided; press <tab> for list)
> webserver-log — Web server logs (select file from the list provided; press <tab> for list)

Required Privilege Level

All

netstat

Displays network connections and statistics.

Syntax

```
netstat
   {
   all {no | yes} |
   cache {no | yes} |
   continuous {no | yes} |
   extend {no | yes} |
   fib {no | yes} |
   groups {no | yes} |
   interfaces {no | yes} |
   listening {no | yes} |
   numeric {no | yes} |
   numeric-hosts {no | yes} |
   numeric-ports
   numeric-users {no | yes} |
   programs {no | yes} |
   route {no | yes} |
   statistics {no | yes} |
   symbolic {no | yes} |
   timers {no | yes} |
   verbose {no | yes}
   }
```

Options

+ all — Display all sockets (default = connected)
+ cache — Display routing cache instead of Forwarding Information Base (FIB)
+ continuous — Continuous listing
+ extend — Display other/more information
+ fib — Display FIB (default)
+ groups — Display multicast group memberships
+ interfaces — Display interface table
+ listening — Display listening server sockets
+ numeric — Do not resolve names
+ numeric-hosts — Do not resolve host names
+ numeric-ports — Do not resolve port names
+ numeric-users — Do not resolve user names
+ programs — Display PID/Program name for sockets
+ route — Display routing table
+ statistics — Display networking statistics (like SNMP)
+ symbolic — Resolve hardware names
+ timers — Display timers
+ verbose — Display full details

Sample Output

The following command shows an excerpt from the output of the **netstat** command.

```
username@hostname> netstat all yes
...
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     5366   /tmp/ssh-lClRtS1936/
    agent.1936
unix  2     [ ]         DGRAM                  959    @/org/kernel/udev/udevd
unix  18     [ ]         DGRAM                    4465   /dev/log
...
```

Required Privilege Level

All

ping

Checks network connectivity to a host.

Syntax

```
ping host <value>
   {
   bypass-routing {no | yes} |
   count <value> |
   do-not-fragment {no | yes} |
   inet6 {no | yes} |
   interval <value> |
   no-resolve {no | yes} |
   pattern <value> |
   size <value> |
   source <value> |
   tos <value> |
   ttl <value> |
   verbose {no | yes}
   }
```

Options

> bypass-routing — Sends the ping request directly to the host on a direct attached network, bypassing usual routing table
> count — Specifies the number of ping requests to be sent (1-2,000,000,000)
> do-not-fragment — Prevents packet fragmentation by use of the do-not-fragment bit in the packet’s IP header
> inet6 — Specifies that the ping packets will use IP version 6
> interval — Specifies how often the ping packets are sent (0 to 2000000000 seconds)
> no-resolve — Provides IP address only without resolving to hostnames
> pattern — Specifies a custom string to include in the ping request (you can specify up to 12 padding bytes to fill out the packet that is sent as an aid in diagnosing data-dependent problems)
> size — Specifies the size of the ping packets (0-65468 bytes)
> source — Specifies the source IP address for the ping command
> tos — Specifies the type of service (TOS) treatment for the packets by way of the TOS bit for the IP header in the ping packet (1-255)
> ttl — Specifies the time-to-live (TTL) value for the ping packet (IPv6 hop-limit value) (0-255 hops)
> verbose — Requests complete details of the ping request.
* host — Specifies the host name or IP address of the remote host

Sample Output

The following command checks network connectivity to the host 66.102.7.104, specifying 4 ping packets and complete details of the transmission.

```
username@hostname> ping count 4 verbose yes host 66.102.7.104
PING 66.102.7.104 (66.102.7.104) 56(84) bytes of data.
64 bytes from 66.102.7.104: icmp_seq=0 ttl=243 time=316 ms
64 bytes from 66.102.7.104: icmp_seq=1 ttl=243 time=476 ms
64 bytes from 66.102.7.104: icmp_seq=2 ttl=243 time=376 ms
64 bytes from 66.102.7.104: icmp_seq=3 ttl=243 time=201 ms

--- 66.102.7.104 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3023ms
rtt min/avg/max/mdev = 201.718/342.816/476.595/99.521 ms, pipe 2

username@hostname>
```

Required Privilege Level

superuser, deviceadmin

quit

Exits the current session for the firewall.

> ***Note:*** *The **quit** command is the same as the **exit** command.*

Syntax

```
quit
```

Options

None

Required Privilege Level

All

request certificate

Generate a self-signed security certificate.

Syntax

```
request certificate
   {
   generate certificate-name <value> name <value> |
     {
     ca {no | yes} |
     country-code <value> |
     days-till-expiry <value> |
     digest <value> |
     email <value> |
     filename <value> |
     locality <value> |
     nbits <value> |
     ocsp-responder-url <value> |
     organization <value> |
     signed-by <value> |
     state <value> |
     certificate-name <value> |
     name <ip> |
     alt-email <value> |
     hostname <value> |
     ip <ip/netmask> |
     organization-unit <value>
     }
   renew certificate-name <value> {days-till-expiry <value>} |
   }
```

Options

> generate — Generate certificate
+ ca — Make this a signing certificate
+ country-code — Two-character code for the country in which the certificate will be used
+ days-till-expiry — Number of days until expiry (1-7300)
+ digest — Digest Algorithm (md5, sh1, sha256, sha384, sha512)
+ email — Email address of the contact person
+ filename — File name for the certificate
+ locality — Locality (city, campus, or other local area)
+ nbits — Length of the key (number of bits in the certificate 1024, 15360, 2048, 3072, 512)
+ organization — Organization using the certificate
+ signed-by — CA for the signing certificate
+ state — Two-character code for the state or province in which the certificate will be used
* certificate-name — Name of the certificate object
* name — IP address or fully qualified domain name (FQDN) to appear on the certificate
> alt-email — Subject alternate email type (value or list of values enclosed in [ ])
> hostname — Subject alternate name DNS type (value or list of values enclosed in [ ])
> ip — Subject alternate name IP type (IP address and network mask; value or list of values enclosed in [ ])
> organization-unit — Department using the certificate (value or list of values enclosed in [ ])

> renew — Renew certificate
    + days-till-expiry   Number of days till expiry (1-7300)
    * certificate-name   Name of the certificate object

Sample Output

The following command renews the certificate mycert.

```
username@hostname> request certificate renew certificate-name mycert
username@hostname>
```

Required Privilege Level

superuser, deviceadmin

request commit-lock

Sets options for locking commits.

Syntax

```
request commit-lock
    {
    add {comment <value>} |
    remove {admin <value>}
    }
```

Options

> add — Prevents other users from committing
    + comment — Comment value
> remove — Releases commit lock previously held
    + admin — Administrator holding the lock

Required Privilege Level

superuser, deviceadmin

request config-lock

Sets options for locking configurations.

Syntax

```
request config-lock {add {comment <value>} | remove}
```

Options

> add — Prevents other users from changing the configuration
> remove — Releases a previously held configuration lock

Required Privilege Level

superuser, deviceadmin

request content

Perform application level upgrade operations.

Syntax

```
request content
   {
   downgrade install {<value> |
   upgrade
     {
     check |
     download latest {sync-to-peer {no | yes}} |
     info |
     install
        {
        commit {no | yes} |
        sync-to-peer {no | yes} |
        file <filename> |
        version latest
        }
     }
   }
```

Options

> downgrade — Installs a previous content version
> upgrade — Performs content upgrade functions
   > check — Obtains information on available packages from the Palo Alto Networks server
   > download — Downloads content packages
      + sync-to-peer — Sends a copy to HA peer
   > info — Shows information about available content packages
   > install — Installs content packages
      + commit — Indicates whether the installed package will be committed to the firewall
      + sync-to-peer — Indicates whether a copy of the package will be provided to another high-availability peer firewall
      > file — Specifies the name of the file containing the content package
      > version — Specifies the latest version of the content software package

Sample Output

The following command lists information about the firewall server software.

```
username@hostname> request content upgrade check

Version               Size         Released on Downloaded
-------------------------------------------------------------------------
13-25                 10MB 2007/04/19  15:25:02       yes

username@hostname>
```

Required Privilege Level

superuser, deviceadmin

request device-registration

Performs device registration.

Syntax

```
request device-registration password <pwd> username <user>
```

Options

* password — Specifies the support portal password for device access
* username — Specifies the support portal user name for device access

Sample Output

The following command registers the device with the specified user name and password.

```
username@hostname> request device-registration username admin password
    adminpwd

username@hostname>
```

Required Privilege Level

superuser, deviceadmin

request generate-report

Requests a report. Use the **show report** command to obtain reports that have been generated using this command.

Syntax

```
request generate-report type <type>
```

Options

all
compliance
least-installed-android-apps
least-installed-ios-apps
managed-devices
most-installed-android-apps
most-installed-ios-apps
os-count
top--android-models
top-hardware-models
top-ios-models
top-malware

Sample Output

The following command generates the OS count report.

```
username@hostname> request generate-report type os-count

Report was successfully generated

username@hostname>
```

Required Privilege Level

superuser, deviceadmin

request global-protect-gateway

Requests performance of GlobalProtect gateway functions.

Syntax

```
request global-protect-gateway
   {
   client-logout gateway <value> reason force-logout user <value> |
     {
     computer <value> |
     domain <value>
     }
   satellite-logout gateway <value> reason force-logout serialno <value> |
   unlock auth-profile <value> user <value> vsys <value> {is-seq {no | yes}}
   }
```

Options

> client-logout — GlobalProtect gateway user logout
   + computer — User's computer name
   + domain — User's domain name
   * gateway — Name of the GlobalProtect gateway remote user tunnel name
   * reason — Reason for logout (force)
   * user — User name
> satellite-logout — GlobalProtect gateway satellite logout
   * gateway — Name of the GlobalProtect gateway site-to-site tunnel name
   * reason — Reason for logout (force)
   * serialno — Device serial number
> unlock — Unlock locked users
   + is-seq — Is this authentication sequence?
   * auth-profile — Auth Profile
   * user — User name
   * vsys — Virtual System

Required Privilege Level

superuser, deviceadmin

request global-protect-mdm

request global-protect-mdm

refresh application all/application-package-name

request device action

selective-wipe filter <device-filter>

request license

Performs license-related operations.

Syntax

```
request license {fetch <auth-code> | info | install}
```

Options

> fetch — Gets a new license key using an authentication code
    + auth-code — Specifies the authentication code to use in fetching the license
> info — Displays information about currently owned licenses
> install — Installs a license key

Sample Output

The following command requests a new license key with the authentication code **123456**.

```
username@hostname> request license fetch auth-code 123456

username@hostname>
```

Required Privilege Level

superuser, deviceadmin

request master-key

Changes the master key.

Syntax

```
request master-key lifetime <value> new-master-key <value>
   {
   current-master-key <value> |
   reminder <value> |
   }
```

Options

+ current-master-key — Specifies the current master key (64-bit encoded public key)
+ reminder — When to send expiry reminder, in hours (1-8760)
* lifetime — Lifetime of the new key, in hours (1-17520)
* new-master-key — Specifies a new master key (64-bit encoded public key)

Required Privilege Level

superuser, deviceadmin

request password-change-history

Displays the history of the user password and re-encrypts it.

Syntax

```
request password-change-history
   {
   dump-history {master-key <value>} |
   re-encrypt old-master-key <value> {master-key <value>}
   }
```

Options

> dump-history — Dumps contents of password history
```
   + master-key — Master key used to encrypt passwords
```
> re-encrypt — Re-encrypts password
```
   + master-key — Masterkey to encrypt historical passwords
   * old-master-key — Old masterkey used to encrypt historical passwords
```

Required Privilege Level

superuser, deviceadmin

request password-hash

Generates a hashed string for the user password.

Syntax

```
request password-hash password <pwd>
```

Options

* username—Specifies the plain text user name for the password that requires the hash string
* password — Specifies the plain text password that requires the hash string

Sample Output

The following command generates a hash of the specified password.

```
username@hostname> request password-hash password mypassword

$1$flhvdype$qupuRAx4SWWuZcjhxn0ED.
```

Required Privilege Level

superuser, deviceadmin

request quota-enforcement

Enforces disk quotas for logs and packet captures.

Syntax

```
request quota-enforcement
```

Options

None

Sample Output

The following command enforces the disk quotas.

```
username@hostname> request quota-enforcement
```

Required Privilege Level

superuser, deviceadmin

request restart

Restarts the system or software modules.

> ***CAUTION:*** *Using this command causes the firewall to reboot, resulting in the temporary disruption of network traffic. Unsaved or uncommitted changes will be lost.*

Syntax

```
request restart {system}
```

Options

> system — Reboots the system

Sample Output

The following command restarts all the firewall software.

```
username@hostname> request restart system
```

Required Privilege Level

superuser, deviceadmin

request shutdown

Performs a clean shutdown of the system.

> ***CAUTION:*** *Using this command causes the firewall to shut down, and network traffic will be disrupted. In addition, unsaved or uncommitted changes will be lost.*

Syntax

```
request shutdown system
```

Options

None

Sample Output

The following command shuts down the firewall.

```
username@hostname> request shutdown system
```

Required Privilege Level

superuser, deviceadmin

request stats

Generates a dump of the statistics.

Syntax

```
request stats dump
```

Options

None

Sample Output

The following command orders a statistics dump.

```
username@hostname> request stats dump

Exec job enqueued with jobid 56
56

username@hostname>
```

Required Privilege Level

superuser, deviceadmin

request support

Obtains technical support information.

Syntax

```
request support {check | info}
```

Options

> check — Gets support information from the Palo Alto Networks update server
> info — Shows downloaded support information

Sample Output

The following command shows downloaded support information.

```
username@hostname> request support info
0
Support Home
https://support.paloaltonetworks.com
Manage Cases
https://support.paloaltonetworks.com/pa-portal/
    index.php?option=com_pan&task=vie
wcases&Itemid=100
Download User Identification Agent
https://support.paloaltonetworks.com/pa-portal/
    index.php?option=com_pan&task=sw_
updates&Itemid=135
866-898-9087
support@paloaltonetworks.com
November 07, 2009
Standard
10 x 5 phone support; repair and replace hardware service

username@hostname>
```

Required Privilege Level

superuser, deviceadmin

request system

Performs system functions, including self testing, downloading system software, and requesting information about the available software packages.

Syntax

```
request system
   {
   private-data-reset |
   raid
     {
     add <drive> {force {no-format}} |
     remove <drive> |
     }
   self-test |
     {
     crypto |
     force-crypto-failure {dp <value> | mp <value>} |
     software-integrity
     }
   self-test-job {crypto | software-integrity} |
   software
     {
     check |
     download {sync-to-peer {no | yes} | file <file> | version <version>} |
     info |
     install {load-config <value> | file <file> | version <version>}
     }
   }
```

Options

> private-data-reset — Removes all of the logs and resets the configuration but does not reset content and software versions
> raid — Perform RAID operations (add or remove a drive)
> self-test — This option is available in Common Criteria (CC) mode and Federal Information Processing Standard 140-2 (FIPS 140-2) mode (for more information, refer to Chapter 6, “Maintenance Mode”)
> crypto — Performs a self-test on all of the cryptographic algorithms the system has on it; if a failure occurs, the system will go into maintenance mode
> force-crypto-failure — Causes the system to reboot and fail the specified cryptographic self-test when it reboots; if a failure occurs, the system will go into maintenance mode
> dp — Fail test on data plane
> mp — Fail test on management plane
> software-integrity — Performs a software integrity test; if a failure occurs, the system will go into maintenance mode
> self-test-job — Runs FIPS/CC self-test jobs
> crypto — Runs crypto self-test job
> software-integrity — Runs software integrity self-test job
> software — Performs system software installation functions
> check — Gets information from Palo Alto Networks server
> download — Downloads software packages

+ sync-to-peer — Sends a copy to HA peer
> file — Downloads software packages by filename
> version — Downloads software packages by version
> info — Shows information about available software packages
> install — Installs a downloaded software package
+ load-config — Configuration to use for booting new software
> file — Upgrades to a software package by filename
> version — Upgrades to a software package by version

Sample Output

The following command requests information about the software packages that are available for download.

```
username@hostname> request system software info

Version      Filename                         Size   Released Downloaded
-------------------------------------------------------------------------
3.0.1       panos.4050-3.0.1.tar.gz        127MB 2010/02/07  00:00:00
   no
3.1.0       panos.4050-3.1.0.tar.gz        127MB 2009/02/07  00:00:00
   no

username@hostname>
```

Required Privilege Level

superuser, deviceadmin

request tech-support

Obtains information to assist technical support in troubleshooting.

Syntax

```
request technical support dump
```

Options

None

Sample Output

The following command creates a dump for technical support.

```
username@hostname> request tech-support dump

Exec job enqueued with jobid 1
1

username@hostname>
```

Required Privilege Level

superuser

scp export

Uses SCP (secure copy) to upload files from the device to another system. Use this command to copy files between the firewall and another host.

Syntax

```
scp export <option> to <target> {remote-port <port_number> | source-ip
   <ip_address>}
   {
   certificate {certificate-name <value> | format <value> | include-key
     <value> to <value>}|
   configuration from <file_name> |
   core-file {data-plane | management-plane} from <file_name> |
   device-state |
   log-file {data-plane | management-plane} |
   logdb |
   pdf-reports from <file_name> |
   tech-support |
   web-interface-certificate
   }
```

Options

+ remote-port — SSH port number on remote host (1-65535)
+ source-ip — Set source address to specified interface address (x.x.x.x or IPv6)
* to — Destination (username@host:path)
> certificate— Use scp to export a certificate
> configuration — Use scp to export a configuration file
    * from — File name
> core-file — Use scp to export a core file
    > data-plane — Use scp to export a data plane core file
        * from — File name
    > management-plane — Use scp to export a management plane core file
        * from — File name
> device-state — Use scp to export device state files from a GlobalProtect Portal
> log-file — Use scp to export log file
    > data-plane — Use scp to export data-plane core-file
    > management-plane — Use scp to export management-plane core-file
> logdb — Use scp to export a log database
> pdf-reports — Use scp to export PDF reports
    * from — File name
> web-interface-certificate — Use scp to export a web interface certificate

Required Privilege Level

superuser, deviceadmin

scp import

Uses SCP (secure copy) to download files to the device. Use this command to download a customizable HTML replacement message (comfort page) in place of a malware infected file.

Syntax

```
scp import <option> from <source> {remote-port <port_number> | source-ip
   <ip_address>}
   {
   certificate |
   configuration |
   content |
   device-state |
   keypair certificate-name <name> format {pem | pkcs12} passphrase <value> |
   license |
   logdb |
   mobile-device-tags |
   private-key certificate-name <name> format {pem | pkcs12} passphrase
     <value> |
   provisioning-profile |
   software |
   web-clip-icon {description}
   }
```

Options

+ remote-port — SSH port number on remote host (1-65535)
+ source-ip — Set source address to specified interface address (x.x.x.x or IPv6)
* from — Source (username@host:path)
> certificate — Use scp to import an X.509 certificate
> configuration — Use scp to import a configuration file
> content — Use scp to import database content
> device-state — Use scp to import device state files for a GlobalProtect Portal
> keypair — Use scp to import an X.509 key pair

    * certificate-name — Name of the certificate object
    * format — Format of the keypair (PEM or PKCS12)
    * passphrase — Passphrase value

> license — Use scp to import a license file
> logdb — Use scp to import a log database
> mobile-device-tags— Use scp to import mobile device tags
> private-key — Use scp to import an X.509 key

    * certificate-name — Name of the certificate object
    * format — Format of the keypair (PEM or PKCS12)
    * passphrase — Passphrase for private key

> provisioning-profile— Use scp to import a provisioning profile
> software — Use scp to import a software package
> web-clip-icon — Use scp to import web clip icons

Sample Output

The following command imports a license file from a file in user1’s account on the machine with IP address 10.0.3.4.

```
username@hostname> scp import certificate from user1@10.0.3.4:/tmp/
    certificatefile
```

Required Privilege Level

superuser, deviceadmin

set cli

Configures scripting and pager options for the PAN-OS CLI. Options are included to display configuration commands in default format, XML format, or as operational **set** commands.

Syntax

```
set cli
   {
   config-output-format {default | json | set | xml} |
   confirmation-prompt {off | on} |
   hide-ip |
   hide-user |
   op-command-xml-output {off | on} |
   pager {off | on} |
   scripting-mode {off | on} |
   terminal {height <value> | type <value> | width <value>} |
   timeout idle {never | value>}
   }
```

Options

> config-output-format — Sets the output format for the configuration file to the default, JSON, XML format, or **set** command format
> configuration-prompt — Enables or disables presentation of a confirmation prompt for some configuration commands
> hide-ip — Hides the last octet of the IP address in logs
> hide-user — Hides user names in logs
> op-command-xml-output—Display xml response in operational commands
> pager — Enables or disables pagers
> scripting-mode — Toggles scripting mode (scripting mode will modify the CLI output such that special characters used for formatting are suppressed)
> terminal — Sets terminal parameters for CLI access
   > height — Sets terminal height (1-500)
   > type — Sets terminal type (press <tab> for list)
   > width — Sets terminal width (1-500)
> timeout — Sets administrative session timeout values
   + idle — Idle timeout (never or 0-1440 minutes; default = 60 minutes)

Sample Output

The following command sequence sets the configuration mode to use **set** command format for output and then displays the output of the **show system log-export-schedule** command in Configuration mode.

```
username@hostname> set cli config-output-format set
username@hostname> configure
Entering configuration mode
[edit]
username@hostname# edit deviceconfig
[edit deviceconfig]
username@hostname# show system log-export-schedule
```

```
set deviceconfig system log-export-schedule 10.16.0.97 description 10.16.0.97
set deviceconfig system log-export-schedule 10.16.0.97 enable yes
set deviceconfig system log-export-schedule 10.16.0.97 start-time 03:00
set deviceconfig system log-export-schedule 10.16.0.97 protocol ftp hostname
    10.16.0.97
set deviceconfig system log-export-schedule 10.16.0.97 protocol ftp port 21
set deviceconfig system log-export-schedule 10.16.0.97 protocol ftp passive-
    mode yes
set deviceconfig system log-export-schedule 10.16.0.97 protocol ftp username
    admin
set deviceconfig system log-export-schedule 10.16.0.97 protocol ftp password
    mZDB7rbW5y8=
username@hostname#
```

The following command sequence shows the same example after XML is specified as the command output format.

```
username@hostname> set cli config-output-format xml
username@hostname> configure
Entering configuration mode
[edit]
username@hostname# edit deviceconfig
[edit deviceconfig]
username@hostname# show system log-export-schedule

<log-export-schedule>
  <entry name="10.16.0.97">
    <description>10.16.0.97</description>
    <enable>yes</enable>
    <start-time>03:00</start-time>
    <protocol>
      <ftp>
        <hostname>10.16.0.97</hostname>
        <port>21</port>
        <passive-mode>yes</passive-mode>
        <username>admin</username>
        <password>mZDB7rbW5y8=</password>
      </ftp>
    </protocol>
  </entry>
</log-export-schedule>
[edit deviceconfig]
[edit deviceconfig]
username@hostname#
```

Required Privilege Level

superuser, deviceadmin

set clock

Configures the system date and time.

Syntax

```
set clock {date <value> | time <value>}
```

Options

+ date — Specify the date in *yyyy/mm/dd* format
+ time — Specify the time in *hh:mm:ss* format (*hh*: 0-23, *mm*: 0-59, *ss*: 0-59)

Sample Output

The following command sets the system date and time.

```
username@hostname> set clock date 2009/03/20 time 14:32:00
username@hostname>
```

Required Privilege Level

superuser, deviceadmin

set data-access-password

Configures the access password for the data filtering logs. The data filtering log records information on the security policies that help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall.

Syntax

```
set data-access-password <pwd>
```

Options

<pwd> — Specifies the password for accessing data filtering logs

Sample Output

The following command sets the password for data filtering logs.

```
username@hostname> set data-access password 12345678
username@hostname>
```

Required Privilege Level

superuser, deviceadmin

set management-server

Configures parameters for the management server, which manages configuration, reports, and authentication for the firewall.

Syntax

```
set management-server
   {
   logging {import-end | import-start | off | on} |
   unlock admin <user_name>
   }
```

Options

> logging — Sets the following logging options:
   import-end — Exit import mode
   import-start — Enter import mode
   off — Disable logging
   on — Allow logging
> unlock — Unlocks locked administrators (specify username of administrator to unlock)

Sample Output

The following command enables logging on the management server.

```
username@hostname> set management-server logging on
username@hostname>
```

Required Privilege Level

superuser, deviceadmin

set password

Configures the firewall password. When you issue this command, the system prompts you to enter the old and new password and to confirm the new password.

Syntax

```
set password
```

Options

None

Sample Output

The following example shows how to reset the firewall password.

```
username@hostname> set password
Enter old password : (enter the old password)
Enter new password : (enter the new password0
Confirm password   : (reenter the new password)

Password changed

username@hostname>
```

Required Privilege Level

superuser, deviceadmin

set ssh-authentication

Configures a public key for Secure Shell (SSH) authentication.

Syntax

```
set ssh-authentication {public-key <value>}
```

Options

+ public-key — Specifies the public key (RSA or DSA)

Sample Output

The following command configures the public key for SSH authentication.

```
username@hostname> set ssh-authentication public-key ssh-rsa AAAAB3N....
username@hostname>
```

Required Privilege Level

superuser, deviceadmin

set system

Configures system logging parameters.

Syntax

```
set system
   {

      logging |
         {
         default |
         default-policy-logging <value> |
         log-suppression {no | yes} |
         max-log-rate <value> |
         max-packet-rate <value>
         }
      }
```

Options

> logging — Sets logging parameters
  > default — Restores logging parameters to the default settings
  > default-policy-logging — Sets the default log policy
  > log-suppression — Enables or disables log suppression (1-300)
  > max-packet-rate value — Sets the maximum packet rate for logging (0-50000)
  > max-log-rate value — Sets the maximum logging rate (0-2560)

Sample Output

The following command enables logging suppression.

```
username@hostname> set system setting logging log-suppression yes
username@hostname>
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show admins

Displays information about the active firewall administrators.

Syntax

```
show admins {all}
```

Options

+ all — Lists the names of all administrators

Sample Output

The following command displays administrator information for the 10.0.0.132 firewall.

```
username@hostname> show admins | match 10.0.0

Admin                           From     Type Session-start      Idle-for
--------------------------------------------------------------------------
admin                     10.0.0.132      Web 02/19 09:33:07     00:00:12s

username@hostname>
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show arp

Displays current Address Resolution Protocol (ARP) entries.

Syntax

```
show arp <interface_name>
```

Options

<interface_name> — Specifies the interface for which the ARP table is displayed
all — Displays information for all ARP tables
ethernet1 — Displays information for the specified interface
management — Displays management ARP information

Sample Output

The following command displays ARP information for the ethernet1/1 interface.

```
username@hostname> show arp ethernet1

maximum of entries supported :      8192
default timeout:                    1800 seconds
total ARP entries in table :        0
total ARP entries shown :           0
status: s - static, c - complete, i - incomplete

username@hostname>
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show authentication

Displays authentication information.

Syntax

```
show authentication {allowlist | groupdb | groupnames}
```

Options

> allowlist — Displays the authentication allow list
> groupdb — Lists the group authentication databases
> groupnames — Lists the distinct group names

Sample Output

The following command shows the list of users that are allowed to access the firewall.

```
username@hostname> show authentication allowlist
vsysname                             profilename            username
              shared                    my-ldap-auth-profilerd-
    test\administrator
             shared                  my-ldap-auth-profile      administrator
             shared                   my-ldap-auth-profile               all
             shared                    my-rsa-auth-profile               all
             shared                       local-auth-users               all
             shared                          auth-kerberos               all
             shared                             radius-abi               all
             shared                                   test               all
             shared                                   testrd-test\cn=account
    operators,cn
=builtin,dc=rd-test,dc=eng,dc=paloaltonetworks,dc=local
...
username@hostname>
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show cli

Displays information about the current CLI session.

Syntax

```
show cli {idle-timeout | info | permissions}
```

Options

> idle-timeout — Displays timeout information for this administrative session
> info — Displays various CLI information
> permissions — Displays the information about the user role

Sample Output

The following command shows information about the current CLI session.

```
username@hostname> show cli info
User                     : admin
Process ID               : 19510
Pager                    : enabled
Config Display Format    : default
Vsys configuration mode  : enabled
Vsys                     : vsys1

username@hostname>
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show clock

Shows the current time on the firewall.

Syntax

```
show clock {more}
```

Options

+ more — Displays dataplane time

Sample Output

The following command shows the current time.

```
username@hostname> show clock

Mon Jun 20 21:03:54 PDT 2011

username@hostname>
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show commit-locks

Displays the list of administrators who hold commit locks.

Syntax

```
show commit-locks
```

Options

None

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show config

Displays the active configuration.

Syntax

```
show config
   {
   audit |
     {
     base-version <value> |
     base-version-no-deletes <value> |
     info |
     version <value>
     }
   candidate |
   diff |
   disk-space |
   logdb-quota |
   running {xpath <value>} |
   saved <value> |
   synced
   }
```

Options

> audit — Displays config audit information

   > base-version — Base version to show

   > base-version-no-deletes — Version with no deletes to show

   > info — Audit information to show

   > version — Audit version to show

> candidate— Displays the candidate configuration

> diff — Displays the differences between the running and candidate configurations

> disk-space — Displays filesystem disk space usage

> logdb-quota — Displays logdb quotas

> running — Displays running configuration

   + xpath — XPath of the node to retrieve

> saved — Displays saved configuration

> synced — Displays configuration last synchronized with HA peer

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show config-locks

Displays the list of administrators who hold configuration locks.

Syntax

```
show config-locks
```

Options

None

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show counter

Displays system counter information.

Syntax

```
show counter
   {
   interface {all | management | <value>} |
   management-server
   }
```

Options

> interface — Displays system counter information grouped by interface
   all — Show all interface counters
   management — Show management interface counter information
> management-server — Displays management server counter information

Sample Output

The following command displays all configuration counter information grouped according to interface.

```
username@hostname> show counter interface


hardware interface counters:
------------------------------------------------------------------------

interface: ethernet1/1
------------------------------------------------------------------------
bytes received                           0
bytes transmitted                        0
packets received                         0
packets transmitted                      0
receive errors                           0
packets dropped                          0
------------------------------------------------------------------------

...

username@hostname>
```

The following command displays all global counter information about the number of file forwards found.

```
username@hostname> show counter global name ctd_file_forward

Name:           ctd_file_forward
Value:          0
Severity:       Informational
Category:       ctd
```

```
Aspect:          pktproc
Description:      The number of file forward found

username@hostname>
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show host-info

Displays host information logs.

Syntax

```
show hostinfo
    {
    anchor <value>
    direction {ascending | descending}
    num-records <value>
    query <value>
    sortby <value>
}
```

Options

+ anchor— Specify value to start from
+ direction — Specify sort direction (ascending or descending)
+ num-records — Specify number of records to include
+ query — Specify string to match
+ sortby — Specify field to sort on

Sample Output

The following command shows one host info record.

```
username@hostname> show hostinfo 1

{ "@status":"success","@code":"19", "result" : { "@total-count" : "9", "@
count" : "1", "@prefilter-total-count" : "9", "entry" : [ {"os" : "androi
d", "os-version" : "4.2.1", "managed" : "no", "last-checkin-time" : "2013
/09/06 10:20:35", "enrollment-time" : "2013/09/06 09:20:33", "last-unenro
ll-time" : "2013/09/06 10:20:35", "udid" : "2085017e5fa50f28", "mac-addre
ss" : "60:a4:4c:94:02:0b", "@name" : "60:a4:4c:94:02:0b", "user" : "sound
", "encryption-not-set" : "no", "passcode-not-set" : "no", "device-name"
: "Nexus 7", "device-serial" : "015d4b33e834180d", "model" : "Asus Nexus
7", "phone-number" : "", "iccid" : "", "location" : "37.381890,-121.96779
0"}]}}


username@hostname>
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show interface

Displays information about system interfaces.

Syntax

```
show interface {<interface_name> | all}
```

Options

all — Displays information for all ARP tables
ethernet1 — Displays Mobile Security Manager interface information
management — Displays management interface information

Sample Output

The following command displays information about the Mobile Security Manager interface.

```
username@hostname> show interface ethernet1


---------------------------------------------------------------------------
Name: ethernet1 Interface
Link status:
  Runtime link speed/duplex/state: unknown/unknown/down
  Configured link speed/duplex/state: auto/auto/auto
MAC address:
  Port MAC addresss 00:21:cc:da:04:3f

Ip address: 192.168.1.5
Netmask: 255.255.255.0
Default gateway: 192.168.1.1
Ipv6 address: unknown
Ipv6 link local address: unknown
Ipv6 default gateway: unknown
---------------------------------------------------------------------------



---------------------------------------------------------------------------
Logical interface counters:
---------------------------------------------------------------------------
bytes received                    0
bytes transmitted                 0
packets received                  0
packets transmitted               0
receive errors                    0
transmit errors                   0
receive packets dropped           0
transmit packets dropped          0
multicast packets received        0
-----------------------------------------
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show jobs

Displays information about current system processes.

Syntax

```
show jobs {all | id <value> | pending | processed}
```

Options

> all — Displays information for all jobs
> id number — Identifies the process by number (1-4294967296)
> pending — Displays recent jobs that are waiting to be executed
> processed — Displays recent jobs that have been processed

Sample Output

The following command lists jobs that have been processed in the current session.

```
username@hostname> show jobs processed

Enqueued                   ID     Type Status Result Completed
--------------------------------------------------------------------------
2007/02/18 09:34:39         2  AutoCom    FIN     OK 2007/02/18 09:34:40
2007/02/18 09:33:00         1  AutoCom    FIN   FAIL 2007/02/18 09:33:54

username@hostname>
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show log

Displays system logs.

Syntax

```
show log
   {
   config |
     {
     client {equal | not-equal} {cli | web} |
     cmd {equal | not-equal} {add | clone | commit | create | delete | edit
        | get | load-from-disk | move | rename | save-to-diak | set}|
     csv-output equal {no | yes} |
     direction equal {backward | forward} |
     end-time equal <value> |
     query equal <value> |
     receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
        days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
        day | last-calendar-month | last-hour} |
     result {equal | not-equal} {failed | succeeded | unauthorized} |
     start-time equal <value>
     }
   hipmatch |
     {
     direction equal {backward | forward} |
     machinename {equal | not-equal} <name> |
     matchname {equal | not-equal} <name> |
     matchtype {equal | not-equal} {object | profile} |
     os {equal | not-equal} <name> |
     query equal <value> |
     receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
        days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
        day | last-calendar-month | last-hour} |
     src {in | not-in} <ip/netmask> |
     srcuser equal <user_name>
     }
   mdm |
     {
     csv-output equal {no | yes} |
     direction equal {backward | forward} |
     end-time equal <value> |
     query equal <value> |
     receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
        days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
        day | last-calendar-month | last-hour} |
     start-time equal <value>
     }
   system |
     {
     csv-output equal {no | yes} |
     direction equal {backward | forward} |
     end-time equal <value> |
     eventid {equal | not-equal} <value>
     id {equal | not-equal} <value>
     object {equal | not-equal} <value>
     opaque contains <value> |
     query equal <value> |
     receive_time in {last-12-hrs | last-15-minutes | last-24-hrs | last-30-
        days | last-6-hrs | last-60-seconds | last-7-days | last-calendar-
        day | last-calendar-month | last-hour} |
     severity {equal | greater-than-or equal | less-than-or-equal | not-
        equal} {critical | high | informational | low | medium} |
     start-time equal <value> |
     subtype {equal | not-equal} <value>
     }
  }
```

Options

> config — Displays config logs
    + client — Client equals or does not equal CLI or Web
    + cmd — Command equals or does not equal (press <tab> for list for commands)
    + csv-output — Equals CSV output (no or yes)
    + direction — Backward or forward direction
    + end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
    + query — Equal to query value
    + receive_time — Receive time in the last specified time period (press <tab> for list)
    + result — Result equals or does not equal failed, succeeded, or unauthorized
    + start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
> hipmatch — Displays host IP match logs
    + csv-output — Equals CSV output (no or yes)
    + machinename — Equals or does not equal machine name
    + matchname — Equals or does not equal match name
    + matchtype — Equals or does not equal object or profile
    + os — Equals or does not equal object
    + query — Equal to query value
    + receive_time — Receive time in the last specified time period (press <tab> for list)
    + src — Source IP address in or not in (x.x.x.x/y or IPv6/netmask)
    + srcuser — Equals source user name
> mdm — Displays Mobile Security Manager logs
    + csv-output — Equals CSV output (no or yes)
    + direction — Backward or forward direction
    + end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
    + query — Equal to query value
    + receive_time — Receive time in the last specified time period (press <tab> for list)
    + start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
> system — Displays system logs
    + csv-output — Equals CSV output (no or yes)
    + direction — Backward or forward direction
    + end-time — Ending date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
    + eventid — Equals or does not equal value
    + id — Equals or does not equal value
    + object — Equals or does not equal value
    + opaque — Opaque contains substring value
    + query — Equal to query value

+ receive_time — Receive time in the last specified time period (press <tab> for list)
+ severity — Equal to, greater than or equal to, less than or equal to, or not equal to critical, high, informational, low, or medium
+ start-time — Starting date and time YYYY/MM/DD@hh:mm:ss (e.g., 2011/08/01@10:00:00)
+ subtype — Equal to subtype value

Sample Output

The following command shows the Mobile Security Manager log.

```
username@hostname> show log mdm
Domain,Receive Time,Serial #,seqno,actionflags,Type/Content Type,C
onfig Version,Generate Time,User,mac,Virtual System,devname,os,desc,Repea
t Count,errcode,Severity,padding1
2013/05/06 03:15:00           2013/05/06 03:15:00
2013/05/06 03:15:00           2013/05/06 03:15:00
2013/05/06 03:15:00           2013/05/06 03:15:00
2013/05/06 03:15:00           2013/05/06 03:15:00

...

username@hostname>
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show malware

Displays the malware name based on the specified ID.

Syntax

```
show malware id <value>
```

Options

<value> — Specifies the malware ID

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show management-clients

Shows information about internal management server clients.

Syntax

```
show management-clients
```

Options

None

Sample Output

The following command shows information about the internal management server clients.

```
username@hostname> show management-clients

              Client PRI    State Progress
-------------------------------------------------------------------------
              routed 30    P2-ok      100
              device 20    P2-ok      100
              ikemgr 10    P2-ok      100
              keymgr 10     init        0    (op cmds only)
               dhcpd 10    P2-ok      100
            ha_agent 10    P2-ok      100
             npagent 10    P2-ok      100
            exampled 10     init        0    (op cmds only)

Overall status: P2-ok. Progress: 0
Warnings:
Errors:
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show mobile-device

Shows information about mobile devices.

Syntax

```
show mobile-device
```

Options

> hip — Show detailed HIP information
  > device-id — Specify device ID
  > device-mac — Specify device MAC address

```
> hip — Show detailed HIP information
    > device-id — Specify device ID
    > device-mac — Specify device MAC address
> imported-devices — Show imported devices and tags
> list          List mobile devices
    + limit — Specify limit value
    + offset — Specify offset value
> pending-actions    Show devices with pending actions
    + limit — Specify limit value
    + offset — Specify offset value
    + query — Specify device filter
```

Sample Output

The following command lists the known mobile devices.

```
username@hostname> show mobile-device list

Name      User   Model  Product Status  MAC        Device-ID
---------------------------------------------------------------------------
Dev iPad 2     sound    iPad 2   iPad2,2  unmanaged 04:54:53:31:e0:77
    c6e1a5f156fa79e786946ebed0509f29a5e1a1d0
Nexus 7        sound    Asus Nexus 7 nakasi   unmanaged 60:a4:4c:94:02:0b
    2085017e5fa50f28
iPod touch     sound    iPod touch 5 iPod5,1  unmanaged 02:00:00:00:00:00
    881a41cd3182311ad1fcaffbec16bcbf0d9c139a
               bhu                        unmanaged 10:BF:48:CD:4A:2D
    3e9ff108c86632fa
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show operational-mode

Displays the device operational mode (normal, fips, or cc).

Syntax

```
show operational-mode
```

Options

None

Sample Output

The following command shows the device operational mode.

```
username@hostname> show operational-mode

normal
username@hostname>
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show query

Displays information about query jobs.

Syntax

```
show query {id <value> | jobs}
```

Options

> id — Displays job information for the specified ID (1-4294967296)
> jobs — Displays all job information

Sample Output

The following command shows information about all current query jobs.

```
username@hostname> show query jobs
Enqueued          ID Last Upd
--------------------------------------------------------------------------
13:58:19          16 13:58:19

    Type         ID Dequeued?
-----------------------------------------------------
username@hostname>
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show report

Displays information about process jobs.

Syntax

```
show report
   {
   directory-listing |
   id <value> |
   jobs |
   }
```

Options

> directory-listing — Displays report of directory listings
> id — Displays reports by ID (1-4294967296)
> jobs — Reports all jobs

Sample Output

The following command shows the report of directory listings.

```
username@hostname> show report directory-listing

/opt/pancfg/mgmt/custom-reports:
total 44K
drwxr-xr-x 2 root root 4.0K Jan 12 02:02 test
drwxr-xr-x 2 root root  20K Jan 14 02:02 test-report
drwxr-xr-x 2 root root  20K Jan 14 02:02 test-hip-report

/opt/pancfg/mgmt/custom-reports/test:
total 184K
-rw-r--r-- 1 root root 1.6K May  7  2013 604800s-ending-20130506.xml
-rw-r--r-- 1 root root 1.9K May  8  2013 604800s-ending-20130507.xml
-rw-r--r-- 1 root root 2.5K May  9  2013 604800s-ending-20130508.xml

username@hostname>
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show system

Displays system-related information.

Syntax

```
show system
   {
   disk-space |
   environmentals {fans | power | thermal} |
   files |
   info |
   logdb-quota |
   masterkey-properties |
   raid {detail} |
   resources {follow} |
   services |
   setting mp-memory-monitor |
   software status |
   state {browser | filter | filter-pretty} |
   }
```

Options

> disk-space — Reports file system disk space usage
> environmentals — Displays system environment state
> files — Lists important files in the system
> info — Displays system information
> log-summary status — Reports time of last generated thsum and trsum logs
> logdb-quota — Reports log data base quotas
> masterkey-properties — Displays Master key expiry and reminders times
> raid — Displays status of RAID devices
> resources — Displays system resources
> services — Displays system services
> setting — Displays system settings for memory management
> software — Displays software information
> state — Displays system state
    > browser — Navigate in a text-mode browser
    > filter — Filter by subtree/wildcard
    > filter-pretty — Filter by subtree/wildcard with pretty printing
> statistics — Displays system statistics
    > application — Displays application statistics for the specified virtual system
    > session — Displays statistics for the session

Sample Output

The following command displays system information.

```
username@hostname> show system info

hostname: GP-100
ip-address: 10.5.36.5
netmask: 255.255.255.0
```

```
default-gateway: 10.5.36.1
mac-address: 00:21:cc:da:04:3e
ethernet1-ip-address: 192.168.1.5
ethernet1-netmask: 255.255.255.0
ethernet1-default-gateway: 192.168.1.1
time: Tue Jan 14 10:28:01 2014
uptime: 10 days, 18:49:26
family: m
model: GP-100
serial: 009801000004
sw-version: 6.0.0-b58
mdmbase-version: 233-507
mdmapp-version: 181-432
mdmapp-release-date: 2014/01/13  13:09:14
logdb-version: 6.0.6
platform-family: m


username@hostname>
```

The following command displays log database quotas and disk usage.

```
username@hostname> show system logdb-quota

Quotas:
              system: 10.00%, 5.044 GB
              config: 10.00%, 5.044 GB
            hipmatch: 30.00%, 15.133 GB
                 mdm: 20.00%, 10.088 GB

Disk usage:
system: Logs and Indexes: 16M
config: Logs and Indexes: 246M
alarm: Logs and Indexes: 28K
hipmatch: Logs and Indexes: 20M
mdm: Logs and Indexes: 25M
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

show user

Displays user identification information. You can show information for a specified IP address, user, or all.

Syntax

```
show user
   directory-integration |
     {
     naming-context |
        {is-active-directory {no | yes}|
        server-port <value> |
        use-ssl {no | yes}|
        server {<ip/netmask> | <hostname>} |
     state {all | <value>} |
     statistics
     }
   group |
     {
     list |
        + xmlapi
        | {except <value>| match <value>}
     name <value>}
     }

   group-selection server {<ip/netmask> | <host_name>} |
     {
     base <value> |
     bind-dn <value> |
     bind-password <value> |
     container-object <value> |
     filter <value> |
     force {no | yes} |
     group-object <value> |
     name-attribute <value> |
     search-scope {one | subtree} |
     server <value> |
     server-port <value> |
     use-ssl {no | yes}
     }
   local-user-db |
     {
     disabled {no |yes} |
     username <name> |
     vsys <name>
     }
   name <value>
   }
```

Options

> directory-integration — Displays user groups data
> > naming-context   Show naming context for directory server
> > > + is-active-directory — is-active-directory
> > > + server-port — ldap server listening port
> > > + use-ssl — use-ssl
> > > * server — ldap server ip or host name.
> > state — Show state of one or all group mapping data (specify all or value)
> > statistics — Show group mapping `statistics`

> group — Displays user groups data
> > list — Lists all groups
> > > `+xml_api— Lists groups from XML API`
> > name — Displays group's members

> group-selection — Show members under one container
> + base — Default base distinguished name (DN) to use for searches
> + bind-dn — Bind distinguished name
> + bind-password — Bind password
> + container-object — Container object class (comma-separated)
> + filter — Search filter
> + force — Whether to force
> + group-object — Group object class (comma-separated)
> + name-attribute — Name attribute
> + use-ssl — Whether to use SSL
> + search-scope — Search scope (one or subtree)
> > server-port — LDAP server listening port (1-65535)
> > server — LDAP server IP address/network mask or host name

> local-user-db — Displays the local user database
> + disabled — Filters by disabled/enabled
> + username — Specifies user name
> + vsys — Specifies virtual system name

> name — Displays statistics for the specified user

Sample Output

The following command indicates group membership for the user Amy.

```
username@hostname> show user name amy

User 'amy' is in 0 group

username@hostname>
```

Required Privilege Level

superuser, deviceadmin, superreader, vsysreader

ssh

Opens a secure shell (SSH) connection to another host.

Syntax

```
ssh host <value>
   {
   inet {no | yes} |
   port <port_number> |
   source <ip_address> |
   v1 {no | yes} |
   v2 {no | yes}
   }
```

Options

+ inet — Force to IPv4 destination
+ port — Port to connect to on the remote host (1-65535; default = 22))
+ source — Source address for SSH session
+ v1 — Force SSH to try protocol version 1 only (default = version 2)
+ v2 — Force SSH to try protocol version 2 only
* host — Host name or IP address of remote host

Sample Output

The following command opens an SSH connection to host 10.0.0.250 using SSH version 2.

```
username@hostname> ssh v2 user@10.0.0.250
user@10.0.0.250's password:

#
```

Required Privilege Level

superuser, deviceadmin

tail

Prints the last 10 lines of a debug file.

Note: The `dp-log` option will not be available on devices that do not have a dataplane, such as the PA-200.

Syntax

```
tail
   {
   follow {no | yes} |
   lines <value> |
   dp-log <file> |
   mp-log <file> |
   webserver-log <file>
   }
```

Options

+ follow — Outputs appended data as the file grows
+ lines — Outputs the last N lines, instead of the last 10 (1-65535)
> dp-log — Data plane log file to display (press <tab> for list of files)
> mp-log — Management plane log file to display (press <tab> for list of files)
> webserver-log — Web server log file to display (press <tab> for list of files)

Sample Output

The following command displays the last 10 lines of the *mappdb.log* file.

```
username@hostname> tail db-log mappdb.log
Tue Jan 14 10:31:33.439 [initandlisten] connection accepted from
   127.0.0.1:44878 #15523 (5 connections now open)
Tue Jan 14 10:31:33.442 [conn15523] end connection 127.0.0.1:44878 (4
   connections now open)
Tue Jan 14 10:32:33.495 [initandlisten] connection accepted from
   127.0.0.1:44888 #15524 (5 connections now open)
Tue Jan 14 10:32:33.498 [conn15524] end connection 127.0.0.1:44888 (4
   connections now open)
Tue Jan 14 10:33:33.550 [initandlisten] connection accepted from
   127.0.0.1:44897 #15525 (5 connections now open)
Tue Jan 14 10:33:33.553 [conn15525] end connection 127.0.0.1:44897 (4
   connections now open)
Tue Jan 14 10:34:33.606 [initandlisten] connection accepted from
   127.0.0.1:44912 #15526 (5 connections now open)
Tue Jan 14 10:34:33.609 [conn15526] end connection 127.0.0.1:44912 (4
   connections now open)
Tue Jan 14 10:35:33.662 [initandlisten] connection accepted from
   127.0.0.1:44937 #15527 (5 connections now open)
Tue Jan 14 10:35:33.664 [conn15527] end connection 127.0.0.1:44937 (4
   connections now open)
username@hostname>

username@hostname>
```

Required Privilege Level

superuser, deviceadmin

test

Runs tests based on installed security policies.

Syntax

```
test
   {
   mdm {
     hip-report distribute {device-id <value> type <value>}
     log {
        hip-match {device <value> | object <value> | os <value> | username
           <value>} |
        mdm {device-id <value> | os <value> | type <value> | username
           <value>} |
   }
   scp-server-connection |
     {
     confirm hostname <value> key <value> |
     initiate hostname <value> password <value> username <value> {path
        <value> | port <value>}
```

}Options

> mdm
   > hip-report distribute— Tests Mobile Security Manager
      * device-id — Device ID
      * type — Type
   > log — Test log operation
      * hip-match—Test hipmatch log (specify device name, object, os, or user name)
      * mdm — Test Mobile Security Manager log (specific device ID, os, type, or user name)
> scp-server-connection — Tests SCP server connection
   > confirm — Confirms SCP server connection
      * hostname — Specifies an SCP hostname
      * key — Specifies an RSA key
   > initiate — Initiates SCP server connection
      + path — Specifies an SCP path
      + port — Specifies an SCP port (1-65535)
      * hostname — Specifies an SCP hostname
      * password — Specifies an SCP password
      * username — Specifies an SCP username

Required Privilege Level

superuser, deviceadmin

traceroute

Displays information about the route packets take to another host.

Syntax

```
traceroute host <value>
   {
   bypass-routing {no | yes} |
   debug-socket {no | yes} |
   do-not-fragment {no | yes} |
   first-ttl <value> |
   gateway <value> |
   ipv4 {no | yes} |
   ipv6 {no | yes} |
   max-ttl <value> |
   no-resolve {no | yes} |
   pause <value> |
   port <value> |
   source <ip_address> |
   tos <value> {verbose} |
   wait <value>
   }
```

Options

+ bypass-routing — Sends the request directly to the host on a direct attached network, bypassing usual routing table
+ debug-socket — Enables socket-level debugging
+ do-not-fragment — Sets the do-not-fragment bit
+ first-ttl — Sets the time-to-live (in number of hops) in the first outgoing probe packet
+ gateway — Specifies a loose source router gateway (maximum = 8)
+ ipv4 — Specifies that IPv4 is used
+ ipv6 — Specifies that IPv6 is used
+ max-ttl — Sets the maximum time-to-live in number of hops
+ no-resolve — Does not attempt to print resolved domain names
+ pause — Sets the time to pause between probes (in milliseconds)
+ port — Sets the base port number used in probes (default for UDP = 33434; for TCP = 80; for ICMP = 1)
+ source — Specifies the source IP address in outgoing probe packets
+ tos — Specifies the type of service (TOS) treatment for the packets by way of the TOS bit for the IP header in the ping packet (0-255)
+ wait — Specifies a delay in transmission of the traceroute request (in seconds)
* host — Specifies the IP address or name of the remote host (required)

Sample Output

The following command displays information about the route from the firewall to www.google.com.

```
username@hostname> traceroute www.paloaltonetworks.com
traceroute to www.paloaltonetworks.com (72.32.199.53), 30 hops max, 38 byte
    packets
1  10.1.0.1 (10.1.0.1)  0.399 ms  1.288 ms  0.437 ms
2  64.0.27.225.ptr.us.xo.net (64.0.27.225)  1.910 ms dsl027-186-
    189.sfo1.dsl.speakeasy.net (216.27.186.189)  1.012 ms
    64.0.27.225.ptr.us.xo.net (64.0.27.225)  1.865 ms
3  dsl027-182-001.sfo1.dsl.speakeasy.net (216.27.182.1)  16.768 ms  581.420
    ms 64.3.142.37.ptr.us.xo.net (64.3.142.37)  219.190 ms
4  ge5-0-0.mar2.fremont-ca.us.xo.net (207.88.80.21)  228.551 ms 110.ge-0-0-
    0.cr1.sfo1.speakeasy.net (69.17.83.189)  12.352 ms ge5-0-0.mar2.fremont-
    ca.us.xo.net (207.88.80.21)  218.547 ms
5  ge-5-3-0.mpr3.pao1.us.above.net (209.249.11.177)  13.212 ms p4-0-
    0.rar2.sanjose-ca.us.xo.net (65.106.5.137)  273.935 ms  221.313 ms
6  p1-0.ir1.paloalto-ca.us.xo.net (65.106.5.178)  139.212 ms so-1-2-
    1.mpr1.sjc2.us.above.net (64.125.28.141)  13.348 ms p1-0.ir1.paloalto-
    ca.us.xo.net (65.106.5.178)  92.795 ms
7  so-0-0-0.mpr2.sjc2.us.above.net (64.125.27.246)  12.069 ms
    206.111.12.146.ptr.us.xo.net (206.111.12.146)  93.278 ms so-0-0-
    0.mpr2.sjc2.us.above.net (64.125.27.246)  556.033 ms
8  tbr1p013201.sffca.ip.att.net (12.123.13.66)  52.726 ms so-3-2-
    0.cr1.dfw2.us.above.net (64.125.29.54)  61.875 ms
    tbr1p013201.sffca.ip.att.net (12.123.13.66)  58.462 ms

     MPLS Label=32537 CoS=0 TTL=1 S=1

 9  64.124.12.6.available.above.net (64.124.12.6)  74.828 ms
    tbr1cl3.la2ca.ip.att.net (12.122.10.26)  62.533 ms
    64.124.12.6.available.above.net (64.124.12.6)  60.537 ms
10  tbr1cl20.dlstx.ip.att.net (12.122.10.49)  60.617 ms
    vlan901.core1.dfw1.rackspace.com (72.3.128.21)  59.881 ms  60.429 ms
11  gar1p360.dlrtx.ip.att.net (12.123.16.169)  108.713 ms
    aggr5a.dfw1.rackspace.net (72.3.129.19)  58.049 ms
    gar1p360.dlrtx.ip.att.net (12.123.16.169)  173.102 ms
12  72.32.199.53 (72.32.199.53)  342.977 ms  557.097 ms  60.899 ms

username@hostname>
```

Required Privilege Level

superuser, deviceadmin

Chapter 6

Maintenance Mode

Maintenance mode provides support for error recovery and diagnostics, and allows you to reset the firewall to factory defaults.

This chapter describes how to enter Maintenance mode:

- “Entering Maintenance Mode” in the next section
- “Using Maintenance Mode” on page 772

Entering Maintenance Mode

The system enters Maintenance mode automatically if a critical error is discovered, or you can enter Maintenance mode explicitly when booting the firewall. Critical failure can be due to service errors, bootloader corruption, or disk file system errors.

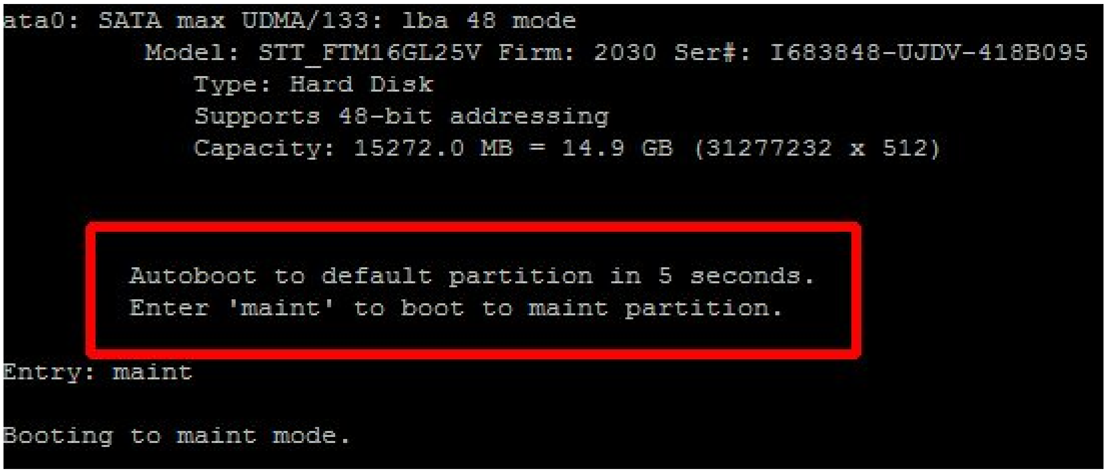
You can enter Maintenance mode in either of the following ways:

- Serial cable to the serial port on the firewall. For serial cable specifications, refer to the *Hardware Reference Guide* for your firewall model.
- Secure Socket Layer (SSL). SSL access is supported if the firewall has already entered Maintenance mode (either automatically or explicitly during bootup).

Entering Maintenance Mode Upon Bootup

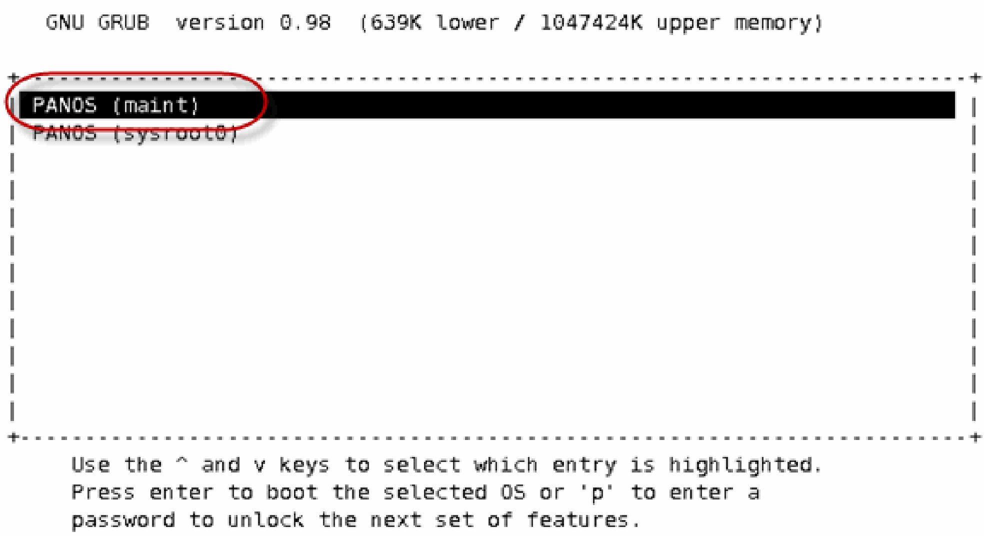
To enter Maintenance mode upon bootup:

1. Enter **maint** when prompted by the bootloader.



```
ata0: SATA max UDMA/133: lba 48 mode
         Model: STT_FTM16GL25V Firm: 2030 Ser#: I683848-UJDV-418B095
            Type: Hard Disk
            Supports 48-bit addressing
            Capacity: 15272.0 MB = 14.9 GB (31277232 x 512)


        Autoboot to default partition in 5 seconds.
        Enter 'maint' to boot to maint partition.

Entry: maint

Booting to maint mode.
```

2. Press any key on your keyboard when prompted to stop the automatic boot, and then select **maint** as the booting partition.

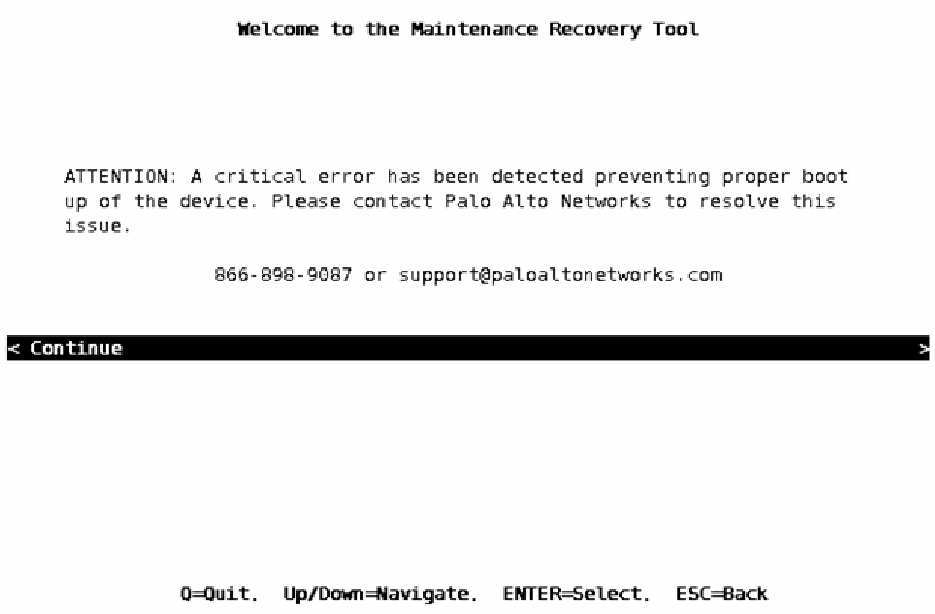


```
   GNU GRUB  version 0.98  (639K lower / 1047424K upper memory)

+-------------------------------------------------------------------------+
| PANOS (maint)                                                           |
| PANOS (sysroot0)                                                        |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
+-------------------------------------------------------------------------+
     Use the ^ and v keys to select which entry is highlighted.
     Press enter to boot the selected OS or 'p' to enter a
     password to unlock the next set of features.
```

Entering Maintenance Mode Automatically

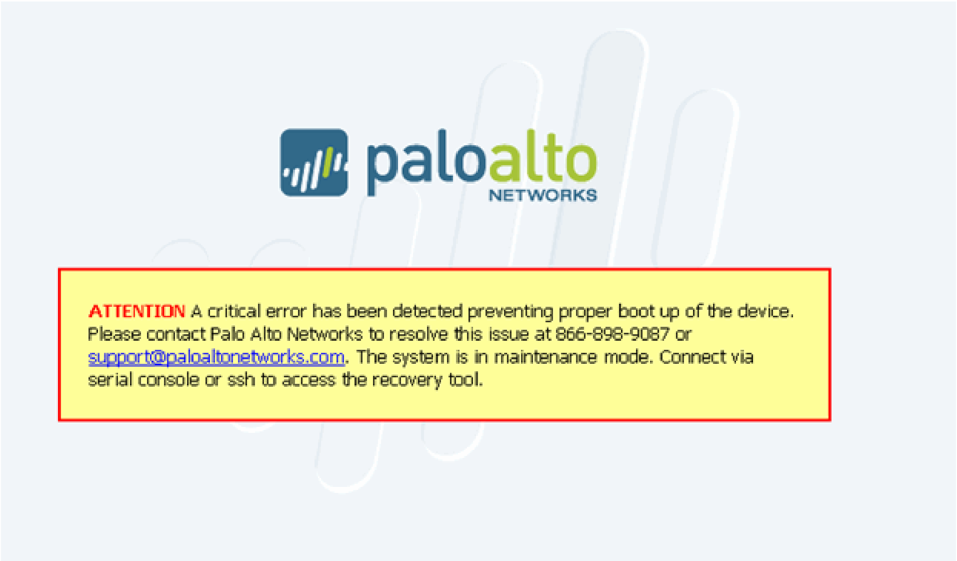
If the system detects a critical error it will automatically fail over to Maintenance mode. When the firewall enters Maintenance mode, messages are displayed on the serial console, web interface, and CLI interface.

The serial console displays the following message.



```
                  Welcome to the Maintenance Recovery Tool



     ATTENTION: A critical error has been detected preventing proper boot
     up of the device. Please contact Palo Alto Networks to resolve this
     issue.

                 866-898-9087 or support@paloaltonetworks.com

< Continue                                                                    >





              Q=Quit.  Up/Down=Navigate.  ENTER=Select.  ESC=Back
```

The web interface displays the following message.



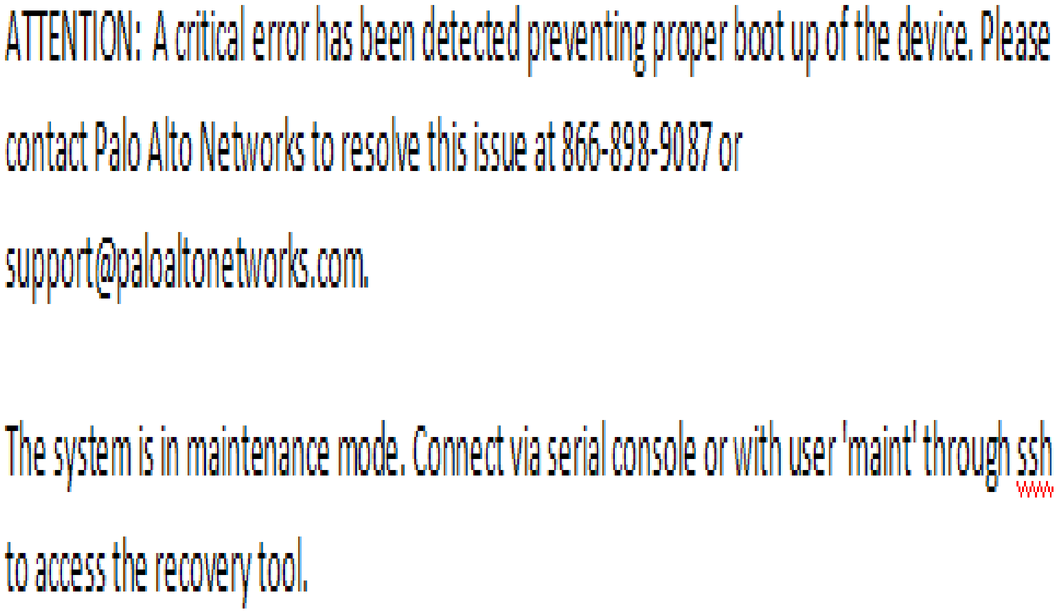
ATTENTION A critical error has been detected preventing proper boot up of the device. Please contact Palo Alto Networks to resolve this issue at 866-898-9087 or support@paloaltonetworks.com. The system is in maintenance mode. Connect via serial console or ssh to access the recovery tool.

The SSH interface displays the following message.

```
ATTENTION:  A critical error has been detected preventing proper boot up
of the device. Please contact Palo Alto Networks to resolve this issue at
866-898-9087 or support@paloaltonetworks.com.
The system is in maintenance mode. Connect via serial console or with user
'maint' through ssh to access the recovery tool.
```

Using Maintenance Mode

The Maintenance mode main menu displays the following options.



ATTENTION: A critical error has been detected preventing proper boot up of the device. Please
contact Palo Alto Networks to resolve this issue at 866-898-9087 or
support@paloaltonetworks.com.

The system is in maintenance mode. Connect via serial console or with user 'maint' through ssh
to access the recovery tool.

The following table describes the Maintenance mode selections that are accessible without entering a password.

Table 1. General Maintenance Mode Options

Option	Description
Maintenance Entry Reason	Indicates why the system entered Maintenance mode and includes possible recovery steps.
Get System Info	Displays basic information about the system. This information is useful when obtaining assistance from Customer Support.
FSCK (Disk Check)	Provides the ability to run a file system check (FSCK) on various partitions.
Log Files	Allows viewing and copying of log files from the system.
Disk Image	Allows the system to revert back to the previously installed software version.
Content Rollback	Allows a rollback to the previously installed content version.
Reboot	Reboots the firewall.

Some of the options are password protected to prevent accidental changes that could leave the system in an inoperative state. The password is intended as a safeguard and it not meant to be secret. The password is **MA1NT** (numeral 1).

Table 2. General Maintenance Mode Options

Option	Description
Factory Reset	Returns the firewall into the factory default state. The reset includes an option to scrub the Config and Log partitions using a National Nuclear Security Administration (NNSA) or Department of Defense (DOD) compliant scrubbing algorithm. The scrub operation can take up to six hours, depending on the platform and the size of the installed drive(s). ***Note:*** *After resetting to the factory default state, you must power cycle the device.*
Set FIPS Mode	Enables and disables FIPS mode. For more information about support for FIPS 140-2, refer to the “Federal Information Processing Standards Support” appendix in the *Palo Alto Networks Web Interface Reference Guide*.
Bootloader Recovery	Reprograms the main bootloader with the latest bootloader image on the system. Use this option if the failsafe bootloader is running and recovery of the main bootloader is required. (PA-2000 and PA-500 systems only)
Disk Image Advanced	These options provide greater granularity and control over installation, including status, history, bootstrapping, and other commands.
Diagnostics	Tests the data plane booting and data plane memory, and run disk performance with bonnie++.

Appendix A
PAN-OS CLI KEYBOARD SHORTCUTS

This appendix lists the supported keyboard shortcuts and control characters supported in the PAN-OS Command Line Interface.

Note: *Some shortcuts depend upon the SSH client that is used to access the PAN-OS CLI. For some clients, the* ***Meta*** *key is the* ***Control*** *key; for some it is the* ***Esc*** *key.*

Table 3 lists the keyboard shortcuts.

Table 3. Keyboard Shortcuts

Item	Description
Commands for Moving	
beginning-of-line (C-a)	Move to the start of the current line.
end-of-line (C-e)	Move to the end of the line.
forward-char (C-f)	Move forward a character.
backward-char (C-b)	Move back a character.
forward-word (M-f)	Move forward to the end of the next word. Words consist of alphanumeric characters (letters and digits).
backward-word (M-b)	Move back to the start of this, or the previous, word. Words consist of alphanumeric characters (letters and digits).
clear-screen (C-l)	Clear the screen and place the current line at the top of the screen. If an argument is included, refresh the current line without clearing the screen.
Commands for Manipulating Command History	
accept-line (Newline, Return)	Accept the line regardless of where the cursor is. If the line is non-empty, add it to the history list. If the line is a modified history line, then restore the history line to its original state.
previous-history (C-p)	Fetch the previous command from the history list, moving back in the list.
next-history (C-n)	Fetch the next command from the history list, moving forward in the list.
beginning-of-history (M-<)	Move to the first line in the history.
end-of-history (M->)	Move to the end of the input history (the line currently being entered).
reverse-search-history (C-r)	Search backward starting at the current line and moving up through the history as necessary. This is an incremental search.

Table 3. Keyboard Shortcuts (Continued)

Item	Description
forward-search-history (C-s)	Search forward starting at the current line and moving down through the history as necessary. This is an incremental search.
non-incremental-reverse-search-history (M-p)	Search backward through the history starting at the current line using a non-incremental search for a string supplied by the user.
non-incremental-forward-search-history (M-n)	Search forward through the history using a non-incremental search for a string supplied by the user.
Commands for Changing Text	
delete-char (C-d)	Delete the character under the cursor. If point is at the beginning of the line, there are no characters in the line, and the last character typed was not C-d, then return EOF.
backward-delete-char (backspace)	Delete the character behind the cursor.
transpose-chars (C-t)	Drag the character before point forward over the character at point. Point moves forward as well. If point is at the end of the line, then transpose the two characters before point.
transpose-words (M-t)	Drag the word behind the cursor past the word in front of the cursor moving the cursor over that word as well.
upcase-word (M-u)	Make the current (or following) word uppercase. With a negative argument, do the previous word, but do not move point.
downcase-word (M-l)	Make the current (or following) word lowercase. With a negative argument, change the previous word, but do not move point.
capitalize-word (M-c)	Capitalize the current (or following) word. With a negative argument, do the previous word, but do not move point.
Deleting and Yanking Text	
`kill-line (C-k)`	Delete the text from the current cursor position to the end of the line.
`backward-kill-line (C-x backspace)`	Delete backward to the beginning of the line.
`unix-line-discard (C-u)`	Delete backward from point to the beginning of the line
`kill-word (M-d)`	Delete from the cursor to the end of the current word, or if between words, to the end of the next word. Word boundaries are the same as those used by forward-word.
`backward-kill-word (M-backspace)`	Delete the word behind the cursor. Word boundaries are the same as those used by backward-word.
`unix-word-backspace (C-w)`	Delete the word behind the cursor, using white space as a word boundary. The word boundaries are different from backward-kill-word.
`yank (C-y)`	Place the top of the deleted section into the buffer at the cursor.
`yank-pop (M-y)`	Rotate the kill-ring, and yank the new top. Only works following yank or yank-pop.
Completing Commands	
complete (TAB)	Attempt to perform completion on the text before point.
`possible-completions (?)`	List the possible completions of the text before point.

Table 3. Keyboard Shortcuts (Continued)

Item	Description
Performing Miscellaneous Functions	
`undo (C-_, C-x C-u)`	Perform an incremental undo, separately remembered for each line.
`revert-line (M-r)`	Undo all changes made to this line. This is like typing the undo command enough times to return the line to its initial state.

Table 4 lists the CLI control characters. The control characters used in the CLI are similar to those used in the EMACS editor.

Table 4. CLI Control Characters

Command	Description
Standard bindings	
C-A	beginning-of-line
C-B	backward-char
C-D	delete-char
C-E	end-of-line
C-F	forward-char
C-G	abort
C-H	backward-delete-char
C-I	complete
C-J	accept-line
C-K	kill-line
C-L	clear-screen
C-M	accept-line
C-N	next-history
C-P	previous-history
C-R	reverse-search-history
C-S	forward-search-history
C-T	transpose-chars
C-U	unix-line-discard
C-W	unix-word-backspace
C-Y	yank
C-_	undo
Meta bindings	
M-C-H	backward-kill-word
M-C-R	revert-line
M-<	beginning-of-history

Table 4. CLI Control Characters (Continued)

Command	Description
M->	end-of-history
?	possible-completions
M-B	backward-word
M-C	capitalize-word
M-D	kill-word
M-F	forward-word
M-L	downcase-word
M-N	non-incremental-forward-search-history
M-P	non-incremental-reverse-search-history
M-R	revert-line
M-T	transpose-words
M-U	upcase-word
M-Y	yank-pop

Index