Check Point
SOFTWARE TECHNOLOGIES LTD.

25 November 2019

SMB R80.20 1500 APPLIANCE CLI GUIDE

R80.20

Technical Reference Guide

[Classification: Protected]

Check Point
SOFTWARE TECHNOLOGIES LTD
INFINITY

Check Point Copyright Notice

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point R80.20

For more about this release, see the R80.20 home page.

Latest Version of this Document

Open the latest version of this document in a Web browser.

Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments.

Revision History

Date	Description
25 November 2019	Formatting update
26 September 2019	First release of this document

Table of Contents

Introduction

This guide contains all relevant CLI commands for the Small and Medium Business (SMB) 1500 appliance models:

- 1550
- 1590

Using Command Line Reference

You can make changes to your appliance with the WebUI or Command Line Interface (CLI). When using CLI note these aspects:

- The CLI default shell (clish) covers all the operations that are supported from the WebUI. It also supports auto-completion capabilities, similar to Gaia. For advanced operations that require direct access to the file system (such as redirecting debug output to a file), log in to Expert mode.
- SSH to the appliance is supported and is enabled through the WebUI.
- You can enable login directly to expert mode. To do this:
  - Login to Expert mode using the "Expert" password.
  - Run the command `bashUser on`
  - You will now always login directly to expert mode (this mode is not deleted during reboot)
  - To turn this mode off, run the command `bashUser off`
- SCP to the appliance is supported but you need to enable direct login to Expert mode. Note that SFTP that is commonly used by winSCP is not supported. For more information, see sk52763.

CLISH Auto-completion

All CLISH commands support auto-completion. Standard Check Point and native Linux commands can be used from the CLISH shell but do not support auto-completion. These are examples of the different commands:

- CLISH - `fetch`, `set`, `show`
- Standard Check Point - `cphaprob, ..., fw, vpn`
- Native Linux - `ping, tcpdump, traceroute`

CLI Syntax

The CLI commands are formatted according to these syntax rules.

Notation	Description
Text without brackets	Items you must type as shown
<Text inside angle brackets>	Placeholder for which you must supply a value
[Text inside square brackets]	Optional items
Vertical pipe (|)	Separator for mutually exclusive items; choose one
{Text inside curly brackets}	Set of required items; choose one
Ellipsis (?)	Multiple values or parameters can be entered

Running Gaia Clish Commands from Expert Mode

You can run Gaia Clish commands from Expert mode.

Syntax

```
clish [ -A -i { -c Cmd | -f File -v} -h -C ]
```

Parameters

Parameter	Description
`-c Cmd`	Single command to execute
`-f File`	File to load commands from
`-v`	Verbose
`-i`	Ignore cmd failure in batch mode and continue
`-A`	Run as admin
`-C`	List available commands
`-h`	Help (this message)

Note - If the default shell, in which you logged in, was Gaia Clish, and then you logged in to the Expert mode from it, you cannot run the `clish` command from the Expert mode (running `clish` -> `expert` -> `clish` commands does not work, but running `expert`-> `clish` commands works).

Supported Linux Commands

These standard Linux commands are also supported by the Check Point Small and Medium Business Appliance CLI.

- `arp`
- `netstat`
- `nslookup`
- `ping`
- `resize`
- `sleep`
- `tcpdump`
- `top`
- `traceroute`
- `uptime`

access-rule type outgoing

Relevant commands for outgoing access rule

add access-rule type outgoing

Description

Adds a new firewall access rule to the outgoing (clear) traffic Rule Base.

Syntax

```
add access-rule type outgoing [ action <action> ] [ log <log> ] [
source <source> ] [ source-negate <source-negate>] [ destination
<destination> ] [ destination-negate <destination-negate> ] [ service
<service> ] [ service-negate <service-negate> ] [ disabled <disabled> ]
[ comment  <comment> ] [ hours-range-enabled { true hours-range-from
<hours-range-from> hours-range-to <hours-range-to> | false } ] [ {
position <position>| position-above <position-above> | position-below
<position-below> } ] [ name <name> ] [ { [ application-name
<application-name> ] | [ application-id <application-id> ] } ] [
application-negate <application-negate> ] [ limit-application-download
{ true limit <limit> | false } ] [ limit-application-upload { true
limit <limit> | false } ]
```

Parameters

Parameter	Description
action	The action taken when there is a match on the rule Options: block, accept, ask, inform, block-inform
application-id	Applications or web sites that are accepted or blocked
application-name	Applications or web sites that are accepted or blocked
application-negate	If true, the rule accepts or blocks all applications but the selected application Type: Boolean (true/false)
comment	Description of the rule Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
destination	Network object that is the target of the connection
destination-negate	If true, the destination is all traffic except what is defined in the destination field Type: Boolean (true/false)
disabled	Indicates if the rule is disabled Type: Boolean (true/false)

Parameter	Description
hours-range-enabled	If true, time is configured Type: Boolean (true/false)
hours-range-from	Time in the format HH:MM Type: A time format hh:mm
hours-range-to	Time in the format HH:MM Type: A time format hh:mm
limit	Applications traffic upload limit (in kbps) Type: A number with no fractional part (integer)
limit-application-download	If true, download is limited Type: Boolean (true/false)
limit-application-upload	If true, upload is limited Type: Boolean (true/false)
log	Defines which logging method to use: None - do not log, Log - Create log, Alert - log with alert, Account - account rule Options: none, log, alert, account
name	name Type: A string of alphanumeric characters without space between them
position	The order of the rule in comparison to other manual rules Type: Decimal number
position-above	The order of the rule in comparison to other manual rules Type: Decimal number
position-below	The order of the rule in comparison to other manual rules Type: Decimal number
service	The network service object that the rule should match to
service-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)
source	Network object or user group that initiates the connection
source-negate	If true, the source is all traffic except what is defined in the source field Type: Boolean (true/false)

Example

```
add access-rule type outgoing action block log none source TEXT source-
negate true destination TEXT destination-negate true service TEXT
service-negate true disabled true comment "This is a comment." hours-
range-enabled true hours-range-from 23:20 hours-range-to 23:20 position
2 name word application-name hasOne application-negate true limit-
application-download true limit 200 limit-application-upload true limit
5
```

delete access-rule type outgoing

Description

Deletes an existing firewall access rule to the outgoing (clear) traffic Rule Base by rule position or rule name.

Syntax

```
delete access-rule type outgoing position <position>
delete access-rule type outgoing name <name>
```

Parameters

Parameter	Description
position	The order of the rule in comparison to other manual rules Type: Decimal number
name	name Type: A string of alphanumeric characters without space between them

Example

```
delete access-rule type outgoing position 2
```

```
delete access-rule type outgoing name word
```

set access-rule type outgoing

Description

Configures an existing firewall access rule to the outgoing (clear) traffic Rule Base by position or name.

Syntax

```
set access-rule type outgoing position <position> [ action <action> ] [ log <log>] [ source <source> ] [ source-negate <source-negate> ] [ destination <destination> ] [ destination-negate <destination-negate> ] [ service <service> ] [ service-negate <service-negate> ] [ disabled <disabled> ] [ comment <comment> ] [ hours-range-enabled { true hours-range-from <hours-range-from> hours-range-to <hours-range-to> | false } ] [ { position <position> | position-above <position-above> | position-below <position-below> } ] [ name <name> ] [ { [ application-name <application-name> ] | [ application-id <application-id>] } ] [ application-negate <application-negate> ] [ limit-application-download { true limit <limit> | false } ] [ limit-application-upload { true limit <limit> | false } ]
```

```
set access-rule type outgoing name <name>[ action <action> ] [ log <log> ] [ source <source> ] [ source-negate <source-negate> ] [ destination <destination> ] [ destination-negate <destination-negate> ] [ service <service> ] [ service-negate <service-negate> ] [ disabled <disabled> ] [ comment <comment> ] [ hours-range-enabled { true hours-range-from <hours-range-from> hours-range-to <hours-range-to> | false } ] [ { position <position> | position-above <position-above> | position-below <position-below> } ] [ name <name> ] [ { [ application-name <application-name> ] | [ application-id <application-id> ] } ] [ application-negate <application-negate> ] [ limit-application-download { true limit <limit> | false } ] [ limit-application-upload { true limit <limit> | false } ]
```

Parameters

Parameter	Description
action	The action taken when there is a match on the rule Options: block, accept, ask, inform, block-inform
application-id	Applications or web sites that are accepted or blocked
application-name	Applications or web sites that are accepted or blocked

Parameter	Description
application-negate	If true, the rule accepts or blocks all applications but the selected application Type: Boolean (true/false)
comment	Description of the rule Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
destination	Network object that is the target of the connection
destination-negate	If true, the destination is all traffic except what is defined in the destination field Type: Boolean (true/false)
disabled	Indicates if the rule is disabled Type: Boolean (true/false)
hours-range-enabled	If true, time is configured Type: Boolean (true/false)
hours-range-from	Time in the format HH:MM Type: A time format hh:mm
hours-range-to	Time in the format HH:MM Type: A time format hh:mm
limit	Applications traffic upload limit (in kbps) Type: A number with no fractional part (integer)
limit-application-download	If true, download is limited Type: Boolean (true/false)
limit-application-upload	If true, upload is limited Type: Boolean (true/false)
log	Defines which logging method to use: None - do not log, Log - Create log, Alert - log with alert, Account - account rule Options: none, log, alert, account
name	name Type: A string of alphanumeric characters without space between them
position	The order of the rule in comparison to other manual rules Type: Decimal number

Parameter	Description
position-above	The order of the rule in comparison to other manual rules Type: Decimal number
position-below	The order of the rule in comparison to other manual rules Type: Decimal number
service	The network service object that the rule should match to
service-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)
source	Network object or user group that initiates the connection
source-negate	If true, the source is all traffic except what is defined in the source field Type: Boolean (true/false)

Example

```
set access-rule type outgoing position 2 action block log none source
TEXT source-negate true destination TEXT destination-negate true
service TEXT service-negate true disabled true comment "This is a
comment." hours-range-enabled true hours-range-from 23:20 hours-range-
to 23:20 position 2 name word application-name hasOne application-
negate true limit-application-download true limit 100 limit-
application-upload true limit 5
```

```
set access-rule type outgoing name word action block log none source
TEXT source-negate true destination TEXT destination-negate true
service TEXT service-negate true disabled true comment "This is a
comment." hours-range-enabled true hours-range-from 23:20 hours-range-
to 23:20 position 2 name word application-name hasOne application-
negate true limit-application-download true limit 100 limit-
application-upload true limit 5
```

show access-rule type outgoing

Description

Shows a firewall access rule in the outgoing (clear) traffic Rule Base according to name or position.

Syntax

```
show access-rule type outgoing name <name>
show access-rule type outgoing position <position>
```

Parameters

Parameter	Description
name	name Type: A string of alphanumeric characters without space between them
position	The order of a manual rule in comparison to other manual rules Type: Decimal number

Example

```
show access-rule type outgoing position 2
show access-rule type outgoing name word
```

access-rule type incoming-internal-and-vpn

Commands relevant for firewall access rule to the incoming/internal/VPN traffic Rule Base.

add access-rule type incoming-internal-and-vpn

Description

Adds a new firewall access rule to the incoming/internal/VPN traffic Rule Base.

Syntax

```
add access-rule type incoming-internal-and-vpn [ action <action> ] [
log <log> ] [ source <source> ] [ source-negate <source-negate> ] [
destination <destination> ] [ destination-negate <destination-negate> ]
[ service <service> ] [ service-negate <service-negate> ] [ disabled
<disabled> ] [ comment <comment>] [ hours-range-enabled { true hours-
range-from <hours-range-from> hours-range-to <hours-range-to> | false }
] [ { position <position> | position-above <position-above> | position-
below <position-below>} ] [ name <name> ] [ vpn <vpn> ]
```

Parameters

Parameter	Description
action	The action taken when there is a match on the rule Options: block, accept, ask, inform, block-inform
comment	Description of the rule Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
destination	Network object that is the target of the connection
destination-negate	If true, the destination is all traffic except what is defined in the destination field Type: Boolean (true/false)
disabled	Indicates if the rule is disabled Type: Boolean (true/false)
hours-range-enabled	If true, time is configured Type: Boolean (true/false)
hours-range-from	Time in the format HH:MM Type: A time format hh:mm
hours-range-to	Time in the format HH:MM Type: A time format hh:mm

Parameter	Description
log	Defines which logging method to use: None - do not log, Log - Create log, Alert - log with alert, Account - account rule Options: none, log, alert, account
name	name Type: A string of alphanumeric characters without space between them
position	The order of the rule in comparison to other manual rules Type: Decimal number
position-above	The order of the rule in comparison to other manual rules Type: Decimal number
position-below	The order of the rule in comparison to other manual rules Type: Decimal number
service	The network service object that the rule should match to
service-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)
source	Network object or user group that initiates the connection
source-negate	If true, the source is all traffic except what is defined in the source field Type: Boolean (true/false)
vpn	Indicates if traffic is matched on encrypted traffic only or all traffic Type: Boolean (true/false)

Example

```
add access-rule type incoming-internal-and-vpn action block log none
source TEXT source-negate true destination TEXT destination-negate true
service TEXT service-negate true disabled true comment "This is a
comment." hours-range-enabled true hours-range-from 23:20 hours-range-
to 23:20 position 2 name word vpn true
```

delete access-rule type incoming-internal-and-vpn

Description

Deletes an existing firewall access rule to the incoming/internal/VPN traffic Rule Base by rule name or rule position.

Syntax

```
delete access-rule type incoming-internal-and-vpn name <name>
```

```
delete access-rule type incoming-internal-and-vpn position <position>
```

Parameters

Parameter	Description
name	Name Type: A string of alphanumeric characters without space between them
position	The order of the rule in comparison to other manual rules Type: Decimal number

Example

```
delete access-rule type incoming-internal-and-vpn name word
```

```
delete access-rule type incoming-internal-and-vpn position 2
```

set access-rule type incoming-internal-and-vpn

Description

Configures an existing firewall access rule to the incoming/internal/VPN traffic Rule Base by position or name.

Syntax

```
set access-rule type incoming-internal-and-vpn position <position> [
action <action>] [ log <log> ] [ source <source> ] [ source-negate
<source-negate> ] [ destination <destination> ] [ destination-negate
<destination-negate> ] [ service <service> ] [ service-negate <service-
negate> ] [ disabled <disabled> ] [ comment <comment> ] [ hours-range-
enabled { true hours-range-from <hours-range-from> hours-range-to
<hours-range-to> | false } ] [ { position <position> | position-above
<position-above> | position-below <position-below> } ] [ name <name> ]
[ vpn <vpn>]
```

```
set access-rule type incoming-internal-and-vpn name <name> [ action
<action> ] [ log <log> ] [ source <source> ] [ source-negate <source-
negate> ] [ destination <destination> ] [ destination-negate
<destination-negate>] [ service <service> ] [ service-negate <service-
negate> ] [ disabled <disabled> ] [ comment <comment> ] [ hours-range-
enabled { true hours-range-from <hours-range-from> hours-range-to
<hours-range-to> | false } ] [ { position <position> | position-above
<position-above> | position-below <position-below> } ] [ name <name> ]
[ vpn <vpn> ]
```

Parameters

Parameter	Description
action	The action taken when there is a match on the rule Options: block, accept, ask, inform, block-inform
comment	Description of the rule Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
destination	Network object that is the target of the connection
destination-negate	If true, the destination is all traffic except what is defined in the destination field Type: Boolean (true/false)
disabled	Indicates if the rule is disabled Type: Boolean (true/false)

Parameter	Description
hours-range-enabled	If true, time is configured Type: Boolean (true/false)
hours-range-from	Time in the format HH:MM Type: A time format hh:mm
hour-range-to	Time in the format HH:MM Type: A time format hh:mm
log	Defines which logging method to use: None - do not log, Log - Create log, Alert - log with alert, Account - account rule Options: none, log, alert, account
name	name Type: A string of alphanumeric characters without space between them
position	The order of the rule in comparison to other manual rules Type: Decimal number
position-above	The order of the rule in comparison to other manual rules Type: Decimal number
position-below	The order of the rule in comparison to other manual rules Type: Decimal number
service	The network service object that the rule should match to
service-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)
source	Network object or user group that initiates the connection
source-negate	If true, the source is all traffic except what is defined in the source field Type: Boolean (true/false)
vpn	Indicates if traffic is matched on encrypted traffic only or all traffic Type: Boolean (true/false)

Example

```
set access-rule type incoming-internal-and-vpn position 2 action block
log none source TEXT source-negate true destination TEXT destination-
negate true service TEXT service-negate true disabled true comment
"This is a comment." hours-range-enabled true hours-range-from 23:20
hours-range-to 23:20 position 2 name word vpn true
```

```
set access-rule type incoming-internal-and-vpn name word action block
log none source TEXT source-negate true destination TEXT destination-
negate true service TEXT service-negate true disabled true comment
"This is a comment." hours-range-enabled true hours-range-from 23:20
hours-range-to 23:20 position 2 name word vpn true
```

show access-rule type incoming-internal-and-vpn

Description

Shows a firewall access rule in the incoming/internal/VPN traffic Rule Base according to position or name..

Syntax

```
show access-rule type incoming-internal-and-vpn position <position>
```

```
show access-rule type incoming-internal-and-vpn name <name>
```

Parameters

Parameter	Description
position	The order of a manual rule in comparison to other manual rules Type: Decimal number
name	name Type: A string of alphanumeric characters without space between them

Example

```
show access-rule type incoming-internal-and-vpn position 2
```

```
show access-rule type incoming-internal-and-vpn name word
```

additional-hw-settings

Relevant commands for additional hardware settings.

set additional-hw-settings

Description

Configures various hardware settings.

Syntax

```
set additional-hw-settings [ reset-timeout <reset-timeout> ]
```

Parameters

Parameter	Description
reset-timeout	Indicates the amount of time (in seconds) that you need to press and hold the factory defaults button on the back panel to restore to the factory defaults image Type: A number with no fractional part (integer)

Example

```
set additional-hw-settings reset-timeout 15
```

show additional-hw-settings

Description

Shows advanced hardware related setings.

Syntax

```
show additional-hw-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show additional-hw-settings
```

additional-management-settings

Commands relevant for additional management settings.

set additional-management-settings

Description

Configure additional management settings.

Syntax

```
set additional-management-settings advanced-settings install-temporary-
policy-to-storage <advanced-settings install-temporary-policy-to-
storage>
```

Parameters

Parameter	Description
advanced-settings install-temporary-policy- to-storage	Indicates whether the temporary policy installation files will be saved to the storage partition Type: Boolean (true/false)

Example

```
set additional-management-settings advanced-settings install-temporary-
policy-to-storage true
```

show additional-management-settings

Description

Show the additional management settings that were configured.

Syntax

```
show additional-management-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show additional-management-settings
```

ad-server

Relevant commands for ad server

add ad-server

Description

Adds a new Active Directory server object.

Syntax

```
add ad-server domain <domain> ipv4-address <ipv4-address> username
<username> password <password> user-dn <user-dn> use-branch-path { true
branch-path <branch-path> | false }
```

When you fill the branch-path field, you can add multiple branches by chaining them into a single string with a semi-colon separator between them: `branch1path;branch2path;branch3path`

Parameters

Parameter	Description
branch-path	The branch of the domain to be used Type: An LDAP DN
domain	Domain name Type: Host name
ipv4-address	Domain controller IP address
password	The user's password Type: A string that contains alphanumeric and special characters
use-branch-path	Select only if you want to use only part of the user database defined in the Active Directory Type: Boolean (true/false)
user-dn	FQDN of the user Type: An LDAP DN
username	A user name with administrator privileges to communicate with the AD server Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces

Example

```
add ad-server domain myHost.com ipv4-address 192.168.1.1 username admin
password a(&7Ba user-dn cn=John\ Doe,dc=example,dc=com use-branch-path
true branch-path cn=John\ Doe,dc=example,dc=com
```

delete ad-server

Description

Deletes an existing Active Directory server object.

Syntax

```
delete ad-server <domain>
```

Parameters

Parameter	Description
domain	Domain name Type: Host name

Example

```
delete ad-server myHost.com
```

set ad-server

Description

Configures an existing Active Directory server object.

Syntax

```
set ad-server <domain> [ ipv4-address <ipv4-address> ] [ username
<username>
```

```
] [ password <password> ] [ user-dn <user-dn> ] [ use-branch-path { true
[ branch-path <branch-path> ] | false } ]
```

When you fill the branch-path field, you can add multiple branches by chaining them into a single string with a semi-colon separator between them: `branch1path;branch2path;branch3path`

Parameters

Parameter	Description
branch-path	The branch of the domain to be used Type: An LDAP DN
domain	Domain name Type: Host name
ipv4-address	Domain controller IP address
password	The user's password Type: A string that contains alphanumeric and special characters
use-branch-path	Select only if you want to use only part of the user database defined in the Active Directory Type: Boolean (true/false)
user-dn	FQDN of the user Type: An LDAP DN
username	A user name with administrator privileges to communicate with the AD server Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces

Example

```
set ad-server myHost.com ipv4-address 192.168.1.1 username admin
password a(&7Ba user-dn cn=John\ Doe,dc=example,dc=com use-branch-path
true branch-path cn=John\ Doe,dc=example,dc=com
```

show ad-server

Description

Shows settings of a configured Active Directory server object.

Syntax

```
show ad-server <domain>
```

Parameters

Parameter	Description
domain	Domain name Type: Host name

Example

```
show ad-server myHost.com
```

show ad-servers

Description

Shows settings of all configured AD server objects.

Syntax

```
show ad-servers
```

Parameters

Parameter	Description
n/a	

Example

```
show ad-servers
```

address-range

Relevant commands for address range.

add address-range

Description

Adds a new IP address range object.

Syntax

```
add address-range name <name> start-ipv4 <start-ipv4> end-ipv4 <end-
ipv4> [ dhcp-exclude-ip-addr <dhcp-exclude-ip-addr> ]
```

Parameters

Parameter	Description
dhcp-exclude-ip-addr	Indicates if the object's IP address(es) is excluded from internal DHCP daemon Options: on, off
end-ipv4	The end of the IP range
name	Network Object name Type: String
start-ipv4	The beginning of the IP range

Example

```
add address-range name TEXT start-ipv4 192.168.1.1 end-ipv4 192.168.1.1
dhcp-exclude-ip-addr on
```

delete address-range

Description

Deletes an existing address range object.

Syntax

```
delete address-range <name>
```

Parameters

Parameter	Description
name	Network Object name Type: String

Example

```
delete address-range TEXT
```

set address-range

Description

Configures an existing IP address range object.

Syntax

```
set address-range <name> [ name <name> ] [ start-ipv4 <start-ipv4> ] [
end-ipv4 <end-ipv4> ] [ dhcp-exclude-ip-addr <dhcp-exclude-ip-addr> ]
```

Parameters

Parameter	Description
dhcp-exclude-ip-addr	Indicates if the object's IP address(es) is excluded from internal DHCP daemon Options: on, off
end-ipv4	The end of the IP range
name	Network Object name Type: String
start-ipv4	The beginning of the IP range

Example

```
set address-range TEXT name TEXT start-ipv4 192.168.1.1 end-ipv4
192.168.1.1 dhcp-exclude-ip-addr on
```

show address-range

Description

Shows settings of a configured IP address range object.

Syntax

```
show address-range <name>
```

Parameters

Parameter	Description
name	Network Object name Type: String

Example

```
show address-range TEXT
```

show address-ranges

Description

Shows settings of all configured IP address range objects.

Syntax

```
show address-ranges
```

Parameters

Parameter	Description
n/a	

Example

```
show address-ranges
```

admin-access

Relevant commands for admin access.

add admin access

Description

Adds a specific IPv4 address or a network IPv4 address from which the administrator can remotely access the appliance.

Syntax

```
add admin-access-ipv4-address
{single-ipv4-address|network-ipv4-address} <ip_addr> {subnet-mask
<netmask>|mask-length <mask_length>}
```

Parameters

Parameter	Description
`ip_addr`	IPv4 address
`mask_length`	Interface mask length, a value between 1 - 32
`netmask`	Interface IPv4 address subnet mask

Return Value

0 on success, 1 on failure

Example

```
add admin-access-ipv4-address network-ipv4-address 1.1.1.1 subnet-mask
255.255.255.0
```

set admin-access

Description

Configures various parameters for administrator access to the device via web/SSH.

Syntax

```
set admin-access [ interfaces { Wireless access <access> | VPN access
<access> | LAN access <access> | any access { allow | block } | WAN
access <access> } ] [ web-access-port <web-access-port> ] [ ssh-access-
port <ssh-access-port> ] [ support-weak-tls-version <support-weak-tls-
version> ] [ allowed-ipv4-addresses <allowed-ipv4-addresses> ]
```

Parameters

Parameter	Description
access	Enable administrator access from the Internet (clear traffic from external interfaces) Type: Boolean (true/false)
allowed-ipv4-addresses	Administrator access permissions policy for source IP addresses Options: any, from-ip-list, any-except-internet
ssh-access-port	SSH Port Type: Port number
support-weak-tls-version	For security reasons, it is highly recommended never to change this parameter's value. Support of TLSv1.0 will be added back to the administration portal to allow connectivity with old browsers (usually ones released prior to 2014). Changing the default of this parameter exposes the administration portal to at- tacks that use vulnerabilities like Heartbleed (CVE-2014-0160). Type: Boolean (true/false)
web-access-port	Web Port (HTTPS) Type: Port number

Example

```
set admin-access interfaces Wireless access true web-access-port 8080
ssh-access-port 8080 support-weak-tls-version true allowed-ipv4-
addresses any
```

show admin-access

Description

Shows settings of administrator access configuration.

Syntax

```
show admin-access
```

Parameters

Parameter	Description
n/a	

Example

```
show admin-access
```

admin-access-ip-addresses

Relevant commands for admin access IP addresses.

show admin-access-ip-addresses

Description

Show all the configured IP addresses that are permitted for administrator access to the appliance.

Syntax

```
show admin-access-ip-addresses
```

Parameters

Parameter	Description
n/a	

Example

```
show admin-access-ip-addresses
```

delete admin-access-ip-address-all

Description

Delete all the reserved IP addresses for administrator access.

Syntax

```
delete admin-access-ip-address-all
```

Parameters

Parameter	Description
n/a	

Example

```
delete admin-access-ip-address-all
```

admin-access-ipv4-address

Relevant commands for admin access IPv4 addresses.

add admin-access-ipv4-address

Adds a specific IPv4 address or an IPv4 address network and mask from which the administrator can remotely access the appliance according to configuration.

add admin-access-ipv4-address

Description

Adds a specific IPv4 address from which the administrator can remotely access the appliance according to configuration.

Syntax

```
add admin-access-ipv4-address single-ipv4-address <single-ipv4-address>
```

Parameters

Parameter	Description
single-ipv4-address	IP address Type: IP address

Example

```
add admin-access-ipv4-address single-ipv4-address 192.168.1.1
```

add admin-access-ipv4-address

Description

Adds an IPv4 address network and mask from which the administrator can remotely access the appliance according to configuration.

Syntax

```
add admin-access-ipv4-address network-ipv4-address <network-ipv4-
address>{ subnet-mask <subnet-mask> | [ mask-length <mask-length> ] }
```

Parameters

Parameter	Description
mask-length	Subnet mask length Type: A string that contains numbers only
network-ipv4-address	IP address Type: IP address
subnet-mask	Subnet mask Type: Subnet mask

Example

```
add admin-access-ipv4-address network-ipv4-address 192.168.1.1 subnet-
mask 255.255.255.0
```

delete admin-access-ipv4-address

Description

Deletes a specific IPv4 address or an IPv4 network and subnet from which the administrator can remotely access the appliance according to configuration.

Syntax

```
delete admin-access-ipv4-address <ipv4-address>
```

Parameters

Parameter	Description
ipv4-address	IP address Type: IP address

Example

```
delete admin-access-ipv4-address 192.168.1.1
```

show admin-access-ipv4-addresses

Description

Shows allowed IP addresses for admin access.

Syntax

```
show admin-access-ipv4-addresses
```

Parameters

Parameter	Description
n/a	

Example

```
show admin-access-ipv4-addresses
```

delete admin-access-ipv4-address-all

Description

Deletes all configured IPv4 addresses from which the administrator can remotely access the appliance according to configuration.

Syntax

```
delete admin-access-ipv4-address-all
```

Parameters

Parameter	Description
n/a	

Example

```
delete admin-access-ipv4-address-all
```

administrator

Relevant commands for admininstrators.

add administrator

Description

Adds a new user who can access the administration web portal and SSH.

Syntax

```
add administrator username <username> [ password-hash <password-hash> ]
permission <permission>
```

Parameters

Parameter	Description
password-hash	Virtual field used for calculating a hashed password Type: An encrypted password
permission	The administrator role and permissions Options: read-write, readonly, networking
username	Indicates the administrator user name Type: A string that contains [A-Z], [0-9], and '_' characters

Example

```
add administrator username admin password-hash TZXPLs20bN0RA permission
read-write
```

delete administrator

Description

Deletes an existing defined administrator. The system will not allow deletion of the last administrator.

Syntax

```
delete administrator username <username>
```

Parameters

Parameter	Description
username	Indicates the administrator user name Type: A string that contains [A-Z], [0-9], and '_' characters

Example

```
delete administrator username admin
```

set administrator

Configures an existing user with administrator privileges.

set administrator

Description

Configures a new password for an existing administrator. You will be prompted to add a new password following this command (this command cannot be used in a script).

Syntax

```
set administrator username <username> password
```

Parameters

Parameter	Description
username	Indicates the administrator user name Type: A string that contains [A-Z], [0-9], and '_' characters

Example

```
set administrator username admin password
```

set administrator

Description

Configures an existing administrator's permission level and password (by hash).

Syntax

```
set administrator username <username> permission <permission> [
password-hash <password-hash> ]
```

Parameters

Parameter	Description
password-hash	Virtual field used for calculating a hashed password Type: An encrypted password
permission	The administrator role and permissions Options: read-write, readonly, networking
username	Indicates the administrator user name Type: A string that contains [A-Z], [0-9], and '_' characters

Example

```
set administrator username admin permission read-write password-hash
TZXPLs20bN0RA
```

set administrators

Configure users with administrator privileges through a RADIUS server.

set administrators

Description

Configures users with administrator privileges through a RADIUS server.

Syntax

```
set administrators radius-auth { true [ use-radius-groups { true

radius-groups <radius-groups> | false } ] [ permission <permission> ] |
false

}
```

Parameters

Parameter	Description
permission	Administrators role Options: read-write, readonly, networking
radius-auth	Administrators RADIUS authentication Type: Boolean (true/false)
radius-groups	RADIUS groups for authentication. Example: RADIUS-group1, RADIUS-class2 Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_', ',' and space characters
use-radius-groups	Use RADIUS groups for authentication Type: Boolean (true/false)

Example

```
set administrators radius-auth true use-radius-groups true radius-
groups My group permission read-write
```

show administrator

Description

Shows settings of an existing user with administrator privileges.

Syntax

```
show administrator username <username>
```

Parameters

Parameter	Description
username	Indicates the administrator user name Type: A string that contains [A-Z], [0-9], and '_' characters

Example

```
show administrator username admin
```

show administrators

Shows settings of all users with administrator privileges.

show administrators

Description

Shows settings of all users with administrator privileges.

Syntax

```
show administrators
```

Parameters

Parameter	Description
n/a	

Example

```
show administrators
```

show administrators

Description

Shows advanced settings of all users with administrator privileges.

Syntax

```
show administrators advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show administrators advanced-settings
```

administrators radius-auth

Relevant commands for administrator radius authentication.

set administrators radius-auth

Description

Configure the administrator role on the RADIUS.

Syntax

```
set administrators radius-auth <enable/disable> use-radius-roles
<true|false>
```

Parameters

Parameter	Description
n/a	

Example

```
set administrators radius-auth enable use-radius-roles true
```

set administrators radius-auth (legacy mode)

Description

Use the default role for all RADIUS users.text.

Syntax

```
set administrators radius-auth <enable/disable> use-radius-roles false
permission <readonly/read-write/networking> [use-radius-groups <group_
name>]
```

Parameters

Parameter	Description
admin role	■ Read Only ■ Read-Write ■ Networking
group_name	The name of the radius group

Example

```
set administrators radius-auth enable use-radius-roles false permission
networking [use-radius-groups <group_name>]
```

show administrators radius-auth

Description

Shows RADIUS related settings for users with administrator privileges.

Syntax

```
show administrators radius-auth
```

Parameters

Parameter	Description
n/a	

Example

```
show administrators radius-auth
```

administrators roles-settings

Commands relevant for configuring administrator roles

set administrators roles-settings

Description

Configure settings for administrator roles.

Syntax

```
set administrators roles-settings customize-roles { true [roles-conf <roles-
conf> ] | false }
```

Parameters

Parameter	Description
customize-roles	Customize administrators roles permissions Type: Boolean (true/false)
roles-conf	The configuration of administrator roles in base64 format. To get the right configuration, contact Check Point Support. Type: base64

Example

```
set administrators roles-settings customize-roles true roles-conf base64
```

show administrators roles-settings

Description

Show settings for administrator roles.

Syntax

```
show administrators roles-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show administrators roles-settings
```

administrator session-settings

Relevant commands for administrator session settings.

set administrator session-settings

Description

Configures session settings for administrators. The settings are global for all administrators.

Syntax

```
set administrator session-settings [ lockout-enable <lockout-enable> ]
[ max-lockout-attempts <max-lockout-attempts> ] [ lock-period <lock-
period> ] [ inactivity-timeout <inactivity-timeout> ] [ password-
complexity-level <password-complexity-level> ] [ password-expiration-
timeout <password-expiration-timeout> ]
```

Parameters

Parameter	Description
inactivity-timeout	Allowed web interface session idle time before automatic logout is executed (in minutes) Type: A number with no fractional part (integer)
lock-period	Once locked out, the administrator will be unable to login for this long Type: A number with no fractional part (integer)
lockout-enable	Limit administrators login failure attempts Options: on, off
max-lockout-attempts	The maximum number of consecutive login failure attempts before the administrator is locked out Type: A number with no fractional part (integer)
password-complexity-level	Set of additional restrictions on administrator passwords, according to the selected mode Options: low, high
password-expiration-timeout	Number of days before administrator is required to change his password. Takes effect only if password complexity level is set to 'high' Type: A number with no fractional part (integer)

Example

```
set administrator session-settings lockout-enable on max-lockout-
attempts 5 lock-period 5 inactivity-timeout 5 password-complexity-level
low password-expiration-timeout 5
```

show administrator session-settings

Description

Shows session settings for users with administrator privileges.

Syntax

```
show administrator session-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show administrator session-settings
```

show adsl statistics

Description

Shows statistics regarding the DSL internet connection (applicable on appliance models with DSL).

Syntax

```
show adsl statistics
```

Parameters

Parameter	Description
n/a	

Example

```
show adsl statistics
```

aggressive-aging

Relevant commands for aggressive aging.

set aggressive-aging

Configures aggressive aging feature's behavior. Aggressive Aging is designed to optimize how the device is dealing with a large connection number by aggressively reducing the timeout of existing connections when necessary.

set aggressive-aging

Description

Configures aggressive aging default reduced timeouts.

Syntax

```
set aggressive-aging [ icmp-timeout <icmp-timeout> ] [ icmp-timeout-
enable <icmp-timeout-enable> ] [ other-timeout <other-timeout> ] [
other-timeout-enable <other-timeout-enable> ] [ pending-timeout
<pending-timeout> ] [ pending-timeout-enable <pending-timeout-enable> ]
[ tcp-end-timeout <tcp-end-timeout> ] [ tcp-end-timeout-enable <tcp-
end-timeout-enable> ] [ tcp-start-timeout <tcp-start-timeout> ] [ tcp-
start-timeout-enable <tcp-start-timeout-enable> ] [ tcp-timeout <tcp-
timeout> ] [ tcp-timeout-enable <tcp-timeout-enable> ] [ udp-timeout
<udp-timeout> ] [ udp-timeout-enable <udp-timeout-enable> ] [ general
<general>] [ log <log> ] [ connt-limit-high-watermark-pct <connt-limit-
high-watermark-pct> ] [ connt-mem-high-watermark-pct <connt-mem-high-
watermark-pct> ] [ memory-conn-status <memory-conn-status> ]
```

Parameters

Parameter	Description
connt-limit-high- watermark-pct	Connection table percentage limit Type: A number with no fractional part (integer)
connt-mem-high- watermark-pct	Memory consumption percentage limit Type: A number with no fractional part (integer)
general	Enable aggressive aging of connections Type: Boolean (true/false)
icmp-timeout	ICMP connections reduced timeout Type: A number with no fractional part (integer)
icmp-timeout-enable	Enable reduced timeout for ICMP connections Type: Boolean (true/false)
log	Tracking options for aggressive aging Options: log, none
memory-conn-status	Choose when aggressive aging timeouts are enforced Options: both, connections, memory

Parameter	Description
other-timeout	Other IP protocols reduced timeout Type: A number with no fractional part (integer)
other-timeout-enable	Enable reduced timeout for non TCP/UDP/ICMP connections Type: Boolean (true/false)
pending-timeout	Pending Data connections reduced timeout Type: A number with no fractional part (integer)
pending-timeout- enable	Enable reduced timeout for non TCP/UDP/ICMP connections Type: Boolean (true/false)
tcp-end-timeout	TCP termination reduced timeout Type: A number with no fractional part (integer)
tcp-end-timeout- enable	Enable reduced timeout for TCP termination Type: Boolean (true/false)
tcp-start-timeout	TCP handshake reduced timeout Type: A number with no fractional part (integer)
tcp-start-timeout- enable	Enable reduced timeout for TCP handshake Type: Boolean (true/false)
tcp-timeout	TCP session reduced timeout Type: A number with no fractional part (integer)
tcp-timeout-enable	Enable reduced timeout for TCP session Type: Boolean (true/false)
udp-timeout	UDP connections reduced timeout Type: A number with no fractional part (integer)
udp-timeout-enable	Enable reduced timeout for UDP connections Type: Boolean (true/false)

Example

```
set aggressive-aging icmp-timeout 30 icmp-timeout-enable true other-
timeout 30 other-timeout-enable true pending-timeout 30 pending-
timeout-enable true tcp-end-timeout 3600 tcp-end-timeout-enable true
tcp-start-timeout 3600 tcp-start-timeout-enable true tcp-timeout 3600
tcp-timeout-enable true udp-timeout 3600 udp-timeout-enable true
general true log log connt-limit-high-watermark-pct 80 connt-mem-high-
watermark-pct 80 memory-conn-status both
```

set aggressive-aging

Description

Configures aggressive aging advanced settings.

Syntax

```
set aggressive-aging advanced-settings connections [ other-timeout-
enable <other-timeout-enable> ] [ connt-limit-high-watermark-pct
<connt-limit-high-watermark-pct> ] [ tcp-start-timeout-enable <tcp-
start-timeout-enable> ] [ icmp-timeout-enable <icmp-timeout-enable> ] [
general <general> ] [ tcp-timeout-enable <tcp-timeout-enable> ] [ tcp-
timeout <tcp-timeout> ] [ tcp-start-timeout <tcp-start-timeout> ] [
udp-timeout-enable <udp-timeout-enable> ] [ udp-timeout <udp-timeout> ]
[ pending-timeout-enable <pending-timeout-enable>] [ log <log> ] [
connt-mem-high-watermark-pct <connt-mem-high-watermark-pct> ] [ tcp-
end-timeout-enable <tcp-end-timeout-enable> ] [ icmp-timeout <icmp-
timeout> ] [ tcp-end-timeout <tcp-end-timeout> ] [ memory-conn-status
<memory-conn-status> ] [ pending-timeout <pending-timeout> ] [ other-
timeout <other-timeout> ]
```

Parameters

Parameter	Description
n/a	

Example

```
set aggressive-aging advanced-settings connections other-timeout-enable
true connt-limit-high-watermark-pct -1000000 tcp-start-timeout-enable
true icmp-timeout-enable true general true tcp-timeout-enable true tcp-
timeout -1000000 tcp-start-timeout -1000000 udp-timeout-enable true
udp-timeout -1000000 pending-timeout-enable true log log connt-mem-
high-watermark-pct -1000000 tcp-end-timeout-enable true icmp-timeout -
1000000 tcp-end-timeout -1000000 memory-conn-status both pending-
timeout -1000000 other-timeout -1000000
```

show aggressive-aging

Shows aggressive aging settings.

show aggressive-aging

Description

Shows aggressive aging settings.

Syntax

```
show aggressive-aging
```

Parameters

Parameter	Description
n/a	

Example

```
show aggressive-aging
```

show aggressive-aging

Description

Shows aggressive aging advanced settings.

Syntax

```
show aggressive-aging advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show aggressive-aging advanced-settings
```

antispam

Relevant commands for Anti-Spam Software Blade and settings.

set antispam

Configures policy for Anti-Spam blade.

set antispam

Description

Configures the policy for Anti-Spam blade.

Syntax

```
set antispam [ mode <mode> ] [ detection-method <detection-method> ] [
log <log> ] [ action-spam-email-content <action-spam-email-content> ] [
flag-subject-stamp <flag-subject-stamp> ] [ detect-mode <detect-mode> ]
[ specify-suspected-spam-settings { true [ suspected-spam-log
<suspected-spam-log> ] [ action-suspected-spam-email-content <action-
suspected-spam-email-content> ] [ flag-suspected-spam-subject-stamp
<flag-suspected-spam-subject-stamp> ] | false } ]
```

Parameters

Parameter	Description
action-spam-email-content	Action to be used upon spam detection in email content: block, flag-header, flag-subject Options: block, flag-header, flag-subject
action-suspected- spam-email-content	Action to be used upon suspected spam detection in email content: block, flag-header, flag-subject Options: block, flag-header, flag-subject
detect-mode	Detect-Only mode: on, off Type: Boolean (true/false)
detection-method	Type of spam detection: Either Sender's IP address or both Sender's IP address and content based detection Options: email-content, sender-ipaddr-reputation-only
flag-subject-stamp	Text to add to spam emails' subject (depends on action chosen for detected spam) Type: A string of alphanumeric characters with space between them
flag-suspected-spam-subject-stamp	Text to add to suspected spam emails subject (depends on action chosen for detected spam) Type: A string of alphanumeric characters with space between them
log	Tracking options for spam emails: log, alert or none Options: none, log, alert

Parameter	Description
mode	Anti-Spam blade mode: on, off Options: on, off
specify-suspected- spam-settings	Handle suspected spam emails differently from spam emails Type: Boolean (true/false)
suspected-spam-log	Tracking options for suspected spam emails: log, alert or none Options: none, log, alert

Example

```
set antispam mode on detection-method email-content log none action-
spam-email-content block flag-subject-stamp several words detect-mode
true specify-suspected-spam-settings true suspected-spam-log none
action-suspected-spam-email-content block flag-suspected-spam-subject-
stamp several words
```

set antispam

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

```
set antispam advanced-settings ip-rep-fail-open <ip-rep-fail-open>
```

Parameters

Parameter	Description
n/a	

Example

```
set antispam advanced-settings ip-rep-fail-open true
```

set antispam

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

```
set antispam advanced-settings email-size-scan <email-size-scan>
```

Parameters

Parameter	Description
n/a	

Example

```
set antispam advanced-settings email-size-scan 1024
```

set antispam

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

```
set antispam advanced-settings scan-outgoing <scan-outgoing>
```

Parameters

Parameter	Description
n/a	

Example

```
set antispam advanced-settings scan-outgoing true
```

set antispam

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

```
set antispam advanced-settings spam-engine-timeout <spam-engine-
timeout>
```

Parameters

Parameter	Description
n/a	

Example

```
set antispam advanced-settings spam-engine-timeout 15
```

set antispam

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

```
set antispam advanced-settings allow-mail-track <allow-mail-track>
```

Parameters

Parameter	Description
n/a	

Example

```
set antispam advanced-settings allow-mail-track none
```

set antispam

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

```
set antispam advanced-settings transparent-proxy <transparent-proxy>
```

Parameters

Parameter	Description
n/a	

Example

```
set antispam advanced-settings transparent-proxy true
```

set antispam

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

```
set antispam advanced-settings ip-rep-timeout <ip-rep-timeout>
```

Parameters

Parameter	Description
n/a	

Example

```
set antispam advanced-settings ip-rep-timeout 15
```

set antispam

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

```
set antispam advanced-settings spam-engine-all-mail-track
```

<spam-engine-all-mail-track>

Parameters

Parameter	Description
n/a	

Example

```
set antispam advanced-settings spam-engine-all-mail-track none
```

show antispam

Shows the configured policy for the Anti-Spam blade.

show antispam

Description

Shows the configured policy for the Anti-Spam blade.

Syntax

```
show antispam
```

Parameters

Parameter	Description
n/a	

Example

```
show antispam
```

show antispam

Description

Shows the advanced settings in the configured policy for the Anti-Spam blade.

Syntax

```
show antispam advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show antispam advanced-settings
```

antispam allowed-sender

add antispam allowed-sender

Adds a new Anti-Spam "allow" exception.

add antispam allowed-sender

Description

Adds a new Anti-Spam "allow" exception for a specific IP address.

Syntax

```
add antispam allowed-sender ipv4-addr <ipv4-addr>
```

Parameters

Parameter	Description
ipv4-addr	Anti-Spam allowed IP address Type: IP address

Example

```
add antispam allowed-sender ipv4-addr 192.168.1.1
```

add antispam allowed-sender

Description

Adds a new Anti-Spam "allow" exception for a sender email or domain.

Syntax

```
add antispam allowed-sender sender-or-domain <sender-or-domain>
```

Parameters

Parameter	Description
sender-or-domain	Anti-Spam allowed domain or sender Type: A domain or email address

Example

```
add antispam allowed-sender sender-or-domain myEmail@mail.com
```

delete antispam allowed-sender

Deletes an existing Anti-Spam "allow" exception.

delete antispam allowed-sender

Description

Deletes all existing Anti-Spam "allow" exceptions.

Syntax

```
delete antispam allowed-sender all
```

Parameters

Parameter	Description
n/a	

Example

```
delete antispam allowed-sender all
```

delete antispam allowed-sender

Description

Deletes an existing Anti-Spam "allow" exception for sender's email or domain.

Syntax

```
delete antispam allowed-sender sender-or-domain <sender-or-domain>
```

Parameters

Parameter	Description
sender-or-domain	Anti-Spam allowed domain or sender Type: A domain name or email address

Example

```
delete antispam allowed-sender sender-or-domain myEmail@mail.com
```

delete antispam allowed-sender

Description

Deletes an existing Anti-Spam "allow" exception for a specific IPv4 address.

Syntax

```
delete antispam allowed-sender ipv4-addr <ipv4-addr>
```

Parameters

Parameter	Description
ipv4-addr	Anti-Spam allowed IP address Type: IP address

Example

```
delete antispam allowed-sender ipv4-addr 192.168.1.1
```

show antispam allowed-senders

Description

Shows the "allowed" exceptions for the Anti-Spam blade.

Syntax

```
show antispam allowed-senders
```

Parameters

Parameter	Description
n/a	

Example

```
show antispam allowed-senders
```

antispam blocked-sender

add antispam blocked-sender

Adds a new Anti-Spam "block" exception.

add antispam blocked-sender

Description

Adds a new Anti-Spam "block" exception for a specific IP address.

Syntax

```
add antispam blocked-sender ipv4-addr <ipv4-addr>
```

Parameters

Parameter	Description
ipv4-addr	Anti-Spam blocked IP address Type: IP address

Example

```
add antispam blocked-sender ipv4-addr 192.168.1.1
```

add antispam blocked-sender

Description

Adds a new Anti-Spam "block" exception for a sender email or domain.

Syntax

```
add antispam blocked-sender sender-or-domain <sender-or-domain>
```

Parameters

Parameter	Description
sender-or-domain	Anti-Spam blocked domain or sender Type: A domain name or email address

Example

```
add antispam blocked-sender sender-or-domain myEmail@mail.com
```

delete antispam blocked-sender

Deletes an existing Anti-Spam "block" exception.

delete antispam blocked-sender

Description

Deletes all existing Anti-Spam "block" exceptions.

Syntax

```
delete antispam blocked-sender all
```

Parameters

Parameter	Description
n/a	

Example

```
delete antispam blocked-sender all
```

delete antispam blocked-sender

Description

Deletes an existing Anti-Spam "block" exception for sender's email or domain.

Syntax

```
delete antispam blocked-sender sender-or-domain <sender-or-domain>
```

Parameters

Parameter	Description
sender-or-domain	Anti-Spam blocked domain or sender Type: A domain name or email address

Example

```
delete antispam blocked-sender sender-or-domain myEmail@mail.com
```

delete antispam blocked-sender

Description

Deletes an existing Anti-Spam "block" exception for a specific IPv4 address.

Syntax

```
delete antispam blocked-sender ipv4-addr <ipv4-addr>
```

Parameters

Parameter	Description
ipv4-addr	Anti-Spam blocked IP address Type: IP address

Example

```
delete antispam blocked-sender ipv4-addr 192.168.1.1
```

show antispam blocked-senders

Description

Shows the "blocked" exceptions for the Anti-Spam blade.

Syntax

```
show antispam blocked-senders
```

Parameters

Parameter	Description
n/a	

Example

```
show antispam blocked-senders
```

application

Relevant commands for application.

add application

Adds a new custom application object (string or regular expression signature over URL).

add application

Description

Adds a new custom application object (string or regular expression signature over URL).

Syntax

```
add application application-name <application-name> category <category>
[ regex-url <regex-url> ] application-url <application-url>
```

Parameters

Parameter	Description
application-name	Application name Type: URL
application-url	Contains the URLs related to this application
category	The primary category for the application (the category which is the most relevant)
regex-url	Indicates if regular expressions are used instead of partial strings Type: Boolean (true/false)

Example

```
add application application-name http://somehost.example.com category
TEXT regex-url true application-url http://somehost.example.com
```

add application

Description

Simplified method for adding a new custom application object (string over URL)

Syntax

add application-url <*application-url*>

Parameters

Parameter	Description
application-url	Application URL

Example

```
add application-url http://somehost.example.com
```

delete application

Deletes an existing custom application object (string or regular expression signature over URL).

delete application

Description

Deletes an existing custom application object by application ID.

Syntax

```
delete application application-id <application-id>
```

Parameters

Parameter	Description
application-id	The ID of the application Type: A number with no fractional part (integer)

Example

```
delete application application-id 1000000
```

delete application

Description

Deletes an existing custom application object by application name.

Syntax

```
delete application application-name <application-name>
```

Parameters

Parameter	Description
application-name	Application name Type: URL

Example

```
delete application application-name http://somehost.example.com
```

find application

Description

Find an application by name (or partial string) to view further details regarding it.

Syntax

```
find application <application-name>
```

Parameters

Parameter	Description
application-name	Application or group name Type: String

Example

```
find application TEXT
```

set application

Configures an existing custom application object.

set application

Description

Adds a URL to an existing custom application object by name.

Syntax

```
set application application-name <application-name> add url <url>
```

Parameters

Parameter	Description
application-name	Application name Type: URL
url	Application URL

Example

```
set application application-name http://somehost.example.com add url
http://somehost.example.com
```

set application

Description

Removes a URL from an existing custom application object by name.

Syntax

```
set application application-name <application-name>remove url <url>
```

Parameters

Parameter	Description
application-name	Application name Type: URL
url	Application URL

Example

```
set application application-name http://somehost.example.com remove url
http://somehost.example.com
```

set application

Description

Adds a URL to an existing custom application object by ID.

Syntax

```
set application application-id <application-id> add url <url>
```

Parameters

Parameter	Description
application-id	The ID of the application Type: A number with no fractional part (integer)
url	Application URL

Example

```
set application application-id 12345678 add url
http://somehost.example.com
```

set application

Description

Removes a URL from an existing custom application object by ID.

Syntax

```
set application application-id <application-id> remove url <url>
```

Parameters

Parameter	Description
application-id	The ID of the application Type: A number with no fractional part (integer)
url	Application URL

Example

```
set application application-id 12345678 remove url
http://somehost.example.com
```

set application

Description

Adds a category to an existing custom application object by name.

Syntax

```
set application application-name <application-name> add category
<category>
```

Parameters

Parameter	Description
application-name	Application name Type: URL
category	Category name

Example

```
set application application-name http://somehost.example.com add
category TEXT
```

set application

Description

Removes a category from an existing custom application object by name.

Syntax

```
set application application-name <application-name> remove category
<category>
```

Parameters

Parameter	Description
application-name	Application name Type: URL
category	Category name

Example

```
set application application-name http://somehost.example.com remove
category TEXT
```

set application

Description

Adds a category to an existing custom application object by ID.

Syntax

```
set application application-id <application-id> add category <category>
```

Parameters

Parameter	Description
application-id	The ID of the application Type: A number with no fractional part (integer)
category	Category name

Example

```
set application application-id 12345678 add category TEXT
```

set application

Description

Removes a category from an existing custom application object by ID.

Syntax

```
set application application-id <application-id> remove category
<category>
```

Parameters

Parameter	Description
application-id	The ID of the application Type: A number with no fractional part (integer)
category	Category name

Example

```
set application application-id 12345678 remove category TEXT
```

set application

Description

Configures an existing custom application by ID.

Syntax

```
set application application-id <application-id> [ category <category> ]
[ regex-url <regex-url> ]
```

Parameters

Parameter	Description
application-id	The ID of the application Type: A number with no fractional part (integer)
category	The primary category for the application (the category which is the most relevant)
regex-url	Indicates if regular expressions are used instead of partial strings Type: Boolean (true/false)

Example

```
set application application-id 12345678 category TEXT regex-url true
```

set application

Description

Configures an existing custom application by name.

Syntax

```
set application application-name <application-name> [ category
<category> ] [ regex-url <regex-url>]
```

Parameters

Parameter	Description
application-name	Application name Type: URL
category	The primary category for the application (the category which is the most relevant)
regex-url	Indicates if regular expressions are used instead of partial strings Type: Boolean (true/false)

Example

```
set application application-name http://somehost.example.com category
TEXT regex-url true
```

show application

Shows details for a specific application in the Application Control database.

show application

Description

Shows details for a specific application in the Application Control database by application name.

Syntax

```
show application application-name <application-name>
```

Parameters

Parameter	Description
application-name	Application or group name Type: String

Example

```
show application application-name TEXT
```

show application

Description

Shows details for a specific application in the Application Control database by application ID.

Syntax

```
show application application-id <application-id>
```

Parameters

Parameter	Description
application-id	The ID of the application or the group Type: A number with no fractional part (integer)

Example

```
show application application-id 12345678
```

show applications

Description

Shows details of all applications.

Syntax

```
show applications
```

Parameters

Parameter	Description
n/a	

Example

```
show applications
```

application-control

set application-control

Description

Configures the default policy for the Application Control and URL filtering blades.

Syntax

```
set application-control [ mode <mode>] [ url-flitering-only <url-
flitering-only>] [ block-security-categories <block-security-
categories>] [ block-inappropriate-content <block-inappropriate-
content> ] [ block-other-undesired-applications <block-other-undesired-
applications> ] [ block-file-sharing-applications <block-file-sharing-
applications> ] [ limit-bandwidth { true [ limit-upload { true set-
limit <set-limit> | false } ] [ limit-download { true set-limit <set-
limit> | false } ] | false } ]
```

Parameters

Parameter	Description
block-file-sharing-applications	Block file sharing using torrents and peer-to-peer applications Type: Boolean (true/false)
block-inappropriate-content	Control content by blocking Internet access to websites with inappropriate content such as sex, violence, weapons, gambling, and alcohol Type: Boolean (true/false)
block-other-undesired-applications	Manually add and block applications or categories of URLs to a group of undesired applications Type: Boolean (true/false)
block-security-categories	Block applications and URLs that can be a security risk and are categorized as spyware, phishing, botnet, spam, anonymizer, or hacking Type: Boolean (true/false)
limit-bandwidth	Indicates if applications that use a lot of bandwidth are limited (also used for QoS) Type: Boolean (true/false)
limit-download	If true, traffic for downloading is limited to the value in maxLimitedDownload Type: Boolean (true/false)
limit-upload	If true, traffic for uploading is limited to the value in maxLimitedDownload Type: Boolean (true/false)

Parameter	Description
mode	Applications & URLs mode - true for on, false for off Type: Boolean (true/false)
set-limit	The limit, in kbps, for downloading Type: A number with no fractional part (integer)
url-flitering-only	Indicates if enable URL Filtering and detection only mode is enabled Type: Boolean (true/false)

Example

```
set application-control mode true url-flitering-only true block-
security-categories true block-inappropriate-content true block-other-
undesired-applications true block-file-sharing-applications true limit-
bandwidth true limit-upload true set-limit 5 limit-download true set-
limit 100
```

show application-control

Description

Shows the configured policy for the Application Control blade

Syntax

```
show application-control
```

Parameters

Parameter	Description
n/a	

Example

```
show application-control
```

show application-control other-undesired-applications

Description

Shows the content of the custom "Other Undesired Applications" group. This group can be chosen to be blocked by default by the Application Control policy.

Syntax

```
show application-control other-undesired-applications
```

Parameters

Parameter	Description
n/a	

Example

```
show application-control other-undesired-applications
```

application-control-engine-settings

set application-control-engine-settings

Configures Application Control blade's advanced engine settings.

set application-control-engine-settings

Description

Configures Application Control blade's advanced engine settings.

Syntax

```
set application-control-engine-settings advanced-settings fail-mode
<fail-mode>
```

Parameters

Parameter	Description
n/a	

Example

```
set application-control-engine-settings advanced-settings fail-mode
allow-all-requests
```

set application-control-engine-settings

Description

Configures Application Control blade's advanced engine settings.

Syntax

```
set application-control-engine-settings advanced-settings block-
requests-when-web-service-unavailable <block-requests-when-web-service-
unavailable>
```

Parameters

Parameter	Description
n/a	

Example

```
set application-control-engine-settings advanced-settings block-
requests-when-web-service-unavailable true
```

set application-control-engine-settings

Description

Configures Application Control blade's advanced engine settings.

Syntax

```
set application-control-engine-settings advanced-settings enforce-safe-search <enforce-safe-search>
```

Parameters

Parameter	Description
n/a	

Example

```
set application-control-engine-settings advanced-settings enforce-safe-search true
```

set application-control-engine-settings

Description

Configures Application Control blade's advanced engine settings.

Syntax

```
set application-control-engine-settings advanced-settings web-site-
categorization-mode <web-site-categorization-mode>
```

Parameters

Parameter	Description
n/a	

Example

```
set application-control-engine-settings advanced-settings web-site-
categorization-mode background
```

set application-control-engine-settings

Description

Configures Application Control blade's advanced engine settings.

Syntax

```
set application-control-engine-settings advanced-settings track-browse-
time
```

<track-browse-time>

Parameters

Parameter	Description
n/a	

Example

```
set application-control-engine-settings advanced-settings track-browse-
time true
```

set application-control-engine-settings

Description

Configures Application Control blade's advanced engine settings.

Syntax

```
set application-control-engine-settings advanced-settings http-
referrer-identification <http-referrer-identification>
```

Parameters

Parameter	Description
n/a	

Example

```
set application-control-engine-settings advanced-settings http-
referrer-identification true
```

set application-control-engine-settings

Description

Configures Application Control blade's advanced engine settings.

Syntax

```
set application-control-engine-settings advanced-settings categorize-
cached-and-translated-pages <categorize-cached-and-translated-pages>
```

Parameters

Parameter	Description
n/a	

Example

```
set application-control-engine-settings advanced-settings categorize-
cached-and-translated-pages true
```

show application-control-engine-settings

Description

Shows advanced settings of the Application Control blade.

Syntax

```
show application-control-engine-settings advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show application-control-engine-settings advanced-settings
```

application-group

add application-group

Description

Adds a new group object for applications.

Syntax

```
add application-group name <name>
```

Parameters

Parameter	Description
name	Application group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - . &) characters without spaces

Example

```
add application-group name users
```

delete application-group

Deletes an existing group object of applications.

delete application-group

Description

Deletes an existing group object of applications by group object name.

Syntax

```
delete application-group name <name>
```

Parameters

Parameter	Description
name	Application group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - . &) characters without spaces

Example

```
delete application-group name users
```

delete application-group

Description

Deletes an existing group object of applications by group object ID.

Syntax

```
delete application-group application-group-id <application-group-id>
```

Parameters

Parameter	Description
application-group-id	The ID of the application group Type: A number with no fractional part (integer)

Example

```
delete application-group application-group-id 12345678
```

set application-group

Configures an existing application group object.

set application-group

Description

Adds an application to an existing application group object by application's name.

Syntax

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

Parameters

Parameter	Description
application-name	Application or group name
name	Application group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - . &) characters without spaces

Example

```
set application-group name users add application-name hasMany
```

set application-group

Description

Removes an application from an existing application group object by application's name.

Syntax

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

Parameters

Parameter	Description
application-name	Application or group name
name	Application group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - . &) characters without spaces

Example

```
set application-group name users remove application-name hasMany
```

set application-group

Description

Adds an application to an existing application group object by application's ID.

Syntax

```
set application-group name <name> add application-id <application-id>
```

Parameters

Parameter	Description
application-id	The ID of the application or the group
name	Application group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - . &) characters without spaces

Example

```
set application-group name users add application-id hasMany
```

set application-group

Description

Removes an application from an existing application group object by application's ID.

Syntax

```
set application-group name <name> remove application-id <application-
id>
```

Parameters

Parameter	Description
application-id	The ID of the application or the group
name	Application group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - . &) characters without spaces

Example

```
set application-group name users remove application-id hasMany
```

set application-group

Description

Adds an application to an existing application group object by application's name using group object's ID.

Syntax

```
set application-group application-group-id <application-group-id> add
application-name <application-name>
```

Parameters

Parameter	Description
application-group-id	The ID of the application group Type: A number with no fractional part (integer)
application-name	Application or group name

Example

```
set application-group application-group-id 12345678 add application-
name hasMany
```

set application-group

Description

Removes an application from an existing application group object by application's name using group object's ID.

Syntax

```
set application-group application-group-id <application-group-id>
remove application-name <application-name>
```

Parameters

Parameter	Description
application-group-id	The ID of the application group Type: A number with no fractional part (integer)
application-name	Application or group name

Example

```
set application-group application-group-id 12345678 remove application-
name hasMany
```

set application-group

Description

Adds an application to an existing application group object by application's ID using group object's ID.

Syntax

```
set application-group application-group-id <application-group-id> add
application-id <application-id>
```

Parameters

Parameter	Description
application-group-id	The ID of the application group Type: A number with no fractional part (integer)
application-id	The ID of the application or the group

Example

```
set application-group application-group-id 12345678 add application-id
hasMany
```

set application-group

Description

Removes an application from an existing application group object by application's ID using group object's ID.

Syntax

```
set application-group application-group-id <application-group-id>
remove application-id <application-id>
```

Parameters

Parameter	Description
application-group-id	The ID of the application group Type: A number with no fractional part (integer)
application-id	The ID of the application or the group

Example

```
set application-group application-group-id 12345678 remove application-
id hasMany
```

show application-group

shows the configuration of the Application group objects.

show application-group

Description

Shows the configuration of a specific application group object by ID.

Syntax

```
show application-group application-group-id <application-group-id>
```

Parameters

Parameter	Description
application-group-id	The ID of the application group Type: A number with no fractional part (integer)

Example

```
show application-group application-group-id 12345678
```

show application-group

Description

Shows the configuration of a specific application group object by name.

Syntax

```
show application-group name <name>
```

Parameters

Parameter	Description
name	Application group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - . &) characters without spaces

Example

```
show application-group name users
```

show application-groups

Description

Shows the configuration of all specific application group objects.

Syntax

```
show application-groups
```

Parameters

Parameter	Description
n/a	

Example

```
show application-groups
```

antispoofing

set antispoofing

Description

Configures the activation of the IP address Anti-Spoofing feature.

Syntax

```
set antispoofing advanced-settings global-activation <global-
activation>
```

Parameters

Parameter	Description
n/a	

Example

```
set antispoofing advanced-settings global-activation true
```

show antispoofing

Description

Shows the configuration for IP addresses Anti-Spoofing functionality.

Syntax

```
show antispoofing advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show antispoofing advanced-settings
```

backup settings

Description

Creates a backup file that contains the current settings for the appliance and saves them to a file. The file is saved to either a USB device or TFTP server. You can use these options when the backup file is created:

- Specific file name (The default file name contains the current image and a date and time stamp)
- Password encryption
- Backup policies
- Add a comment to the file

Syntax

```
backup settings to {usb|tftp server <serverIP>} [filename <filename>]
[file-encryption {off|on password <pass>}] [backup-policy {on|off}]
[add-comment <comment>]
```

Parameters

Parameter	Description
`comment`	Comment that is added to the file.
`filename`	Name of the backup file.
`pass`	Password for the file. Alphanumeric and special characters are allowed.
`serverIP`	IPv4 address of the TFTP server.

Return Value

0 on success, 1 on failure

Example

```
backup settings to usb file-encryption on password admin backup-policy
on add-comment check_point_new_configuration
```

Output

Success prints OK. Failure shows an appropriate error message.

Comments

When saving the backup file to a USB device, the backup settings command fails if there are two USB devices connected to the appliance.

show backup settings

Description

Shows previous backup information of the appliance's settings.

`show backup-settings-log` shows the log file of previous backup settings operations.

Syntax

```
show backup-settings-{log|info {from tftp server <server> filename
<file>|from usb filename <file>}}
```

Parameters

Parameter	Description
`server`	IP address or host name of the TFTP server
`file`	Name of backup file

Example

```
show backup-settings-log
```

```
show backup-settings-info from usb filename backup
```

Output

Success shows backup settings information. Failure shows an appropriate error message.

blade-update-schedule

set blade-update-schedule

Configures schedule for Software Blade updates.

set blade-update-schedule

Description

Configures schedule forSoftware Blades updates.

Syntax

```
set blade-update-schedule [ schedule-ips <schedule-ips> ] [ schedule-
anti-bot <schedule-anti-bot> ] [ schedule-anti-virus <schedule-anti-
virus> ] [ schedule-appi <schedule-appi> ] [ recurrence { daily time
<time>| weekly day-of-week <day-of-week>time  <time> | hourly hour-
interval <hour-interval> | monthly day-of-month <day-of-month> time
<time> } ]
```

Parameters

Parameter	Description
day-of-month	If the update occurs monthly, this is the day in which it occurs Type: A number with no fractional part (integer)
day-of-week	If the update occurs weekly, this is the weekday in which it occurs Options: sunday, monday, tuesday, wednesday, thursday, friday, saturday
hour-interval	If the update occurs hourly, this indicates the hour interval between each update Type: A number with no fractional part (integer)
recurrence	The recurrence of the updates - hourly, daily, weekly or monthly Type: Press TAB to see available options
schedule-anti-bot	Indicates if Anti-Bot blade is automatically updated according to configured schedule Type: Boolean (true/false)
schedule-anti-virus	Indicates if Anti-Virus blade is automatically updated according to configured schedule Type: Boolean (true/false)
schedule-appi	Indicates if Application Control blade is automatically updated according to configured schedule Type: Boolean (true/false)
schedule-ips	Indicates if IPS blade is automatically updated according to configured schedule Type: Boolean (true/false)

Parameter	Description
time	The hour of the update (Format: HH:MM in 24 hour clock) Type: A time format hh:mm

Example

```
set blade-update-schedule schedule-ips true schedule-anti-bot true
schedule-anti-virus true schedule-appi true recurrence daily time 23:20
```

set blade-update-schedule

Description

Configures advanced settings for Software Blade updates.

Syntax

```
set blade-update-schedule advanced-settings max-num-of-retries <max-num-of-retries>
```

Parameters

Parameter	Description
n/a	

Example

```
set blade-update-schedule advanced-settings max-num-of-retries 10
```

set blade-update-schedule

Description

Configures advanced settings for Software Blade updates.

Syntax

```
set blade-update-schedule advanced-settings timeout-until-retry
<timeout-until-retry>
```

Parameters

Parameter	Description
n/a	

Example

```
set blade-update-schedule advanced-settings timeout-until-retry 10
```

show blade-update-schedule

Shows the configuration of Software Blade updates schedule.

show blade-update-schedule

Description

Shows the configuration of Software Blade updates schedule

Syntax

```
show blade-update-schedule
```

Parameters

Parameter	Description
n/a	

Example

```
show blade-update-schedule
```

show blade-update-schedule

Description

Shows advanced settings of Software Blade updates schedule.

Syntax

```
show blade-update-schedule advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show blade-update-schedule advanced-settings
```

bookmark

add bookmark

Description

Adds a new bookmark link that will appear for VPN remote access users in the SNX VPN remote access landing page.

Syntax

```
add bookmark label <label> url <url> [ tooltip <tooltip> ] [ type
<type> ] [ is-global <is-global> ] [ user-name <user-name> ] [ password
<password> ] [ screen-width <screen-width> ] [ screen-height <screen-
height> ]
```

Parameters

Parameter	Description
is-global	Indicates if the bookmark will be displayed for all remote access users Type: Boolean (true/false)
label	Text for the bookmark in the SSL Network Extender portal Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
password	The password for remote desktop connection Type: A string that contains alphanumeric and special characters
screen-height	The height of the screen when the bookmark is remote desktop Type: A number with no fractional part (integer)
screen-width	The width of the screen when the bookmark is remote desktop Type: A number with no fractional part (integer)
tooltip	Tooltip for the bookmark in the SSL Network Extender portal Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
type	The type of the bookmark - link or remote desktop connection Options: link, rdp
url	Bookmark URL - should start with `http://` or `https://` for a bookmark of type link Type: URL
user-name	The user name for remote desktop connection Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces

Example

```
add bookmark label myLabel url http://www.checkpoint.com/ tooltip "This
is a comment." type link is-global true user-name admin password a(&7Ba
screen-width 1920 screen-height 1080
```

delete bookmark

Deletes an existing bookmark link that appears in the SNX VPN remote access landing page.

delete bookmark

Description

Deletes an existing bookmark link by label.

Syntax

```
delete bookmark label <label>
```

Parameters

Parameter	Description
label	Text for the bookmark in the SSL Network Extender portal Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @

Example

```
delete bookmark label myLabel
```

delete bookmark

Description

Deletes all existing bookmark links.

Syntax

```
delete bookmark all
```

Parameters

Parameter	Description
n/a	

Example

```
delete bookmark all
```

set bookmark

Description

Configures an existing bookmark shown to users in the SNX landing page.

Syntax

```
set bookmark [ label <label> ] [ new-label <new-label> ] [ url <url> ]
[ tooltip <tooltip> ] [ type <type> ] [ is-global <is-global> ] [ user-
name <user-name> ] [ password <password> ] [ screen-width <screen-
width> ] [ screen-height <screen-height> ]
```

Parameters

Parameter	Description
is-global	Indicates if the bookmark will be displayed for all remote access users Type: Boolean (true/false)
label	Text for the bookmark in the SSL Network Extender portal Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
new-label	Text for the bookmark in the SSL Network Extender portal Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
password	The password for remote desktop connection Type: A string that contains alphanumeric and special characters
screen-height	The height of the screen when the bookmark is remote desktop Type: A number with no fractional part (integer)
screen-width	The width of the screen when the bookmark is remote desktop Type: A number with no fractional part (integer)
tooltip	Tooltip for the bookmark in the SSL Network Extender portal Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
type	The type of the bookmark - link or remote desktop connection Options: link, rdp
url	Bookmark URL - should start with http:// or https:// for a bookmark of type link Type: URL

Parameter	Description
user-name	The user name for remote desktop connection Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces

Example

```
set bookmark label myLabel new-label myNewLabel url
http://www.checkpoint.com/ tooltip myToolTip type link is-global true
user-name admin password a(&7Ba screen-width 1920 screen-height 1080
```

show bookmark

Description

Shows the configuration of a bookmark defined to be shown to users when connecting to the SNX portal using remote access VPN.

Syntax

```
show bookmark label <label>
```

Parameters

Parameter	Description
label	Text for the bookmark in the SSL Network Extender portal Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @

Example

```
show bookmark label myLabel
```

show bookmarks

Description

Shows all bookmarks defined to be shown to users when connecting to the SNX portal using remote access VPN.

Syntax

```
show bookmarks
```

Parameters

Parameter	Description
n/a	

Example

```
show bookmarks
```

bridge

add bridge

Description

Adds a new bridge.

Syntax

```
add bridge [ name <name> ]
```

Parameters

Parameter	Description
name	Bridge name Type: A bridge name should be br0-9

Example

```
add bridge name br7
```

delete bridge

Description

Deletes an existing bridge.

Syntax

```
delete bridge <name>
```

Parameters

Parameter	Description
name	Bridge name Type: A bridge name should be br0-9

Example

```
delete brdige br7
```

set bridge

Configures an existing bridge interface.

set bridge

Description

Configures an existing bridge interface.

Syntax

```
set bridge <name> stp <stp>
```

Parameters

Parameter	Description
name	Bridge name Type: A bridge name should be br0-9
stp	Spanning Tree Protocol mode Options: on, off

Example

```
set bridge br7 stp on
```

set bridge

Description

Adds an existing network/interface to an existing bridge.

Syntax

```
set bridge <name> add member <member>
```

Parameters

Parameter	Description
member	Network name
name	Bridge name Type: A bridge name should be br0-9

Example

```
set bridge br7 add member My_Network
```

set bridge

Description

Removes an existing network/interface from an existing bridge.

Syntax

```
set bridge <name> remove member <member>
```

Parameters

Parameter	Description
member	Network name
name	Bridge name Type: A bridge name should be br0-9

Example

```
set bridge br7 remove member My_Network
```

show bridge

Description

Shows configuration and statistics of a defined bridge.

Syntax

```
show bridge <name>
```

Parameters

Parameter	Description
name	Bridge name Type: A bridge name should be br0-9

Example

```
show bridge br7
```

show bridges

Description

Shows details of all defined bridges.

Syntax

```
show bridges
```

Parameters

Parameter	Description
n/a	

Example

```
show bridges
```

show clock

Description

Shows current system date and time.

Syntax

```
show clock
```

Parameters

Parameter	Description
n/a	

Example

```
show clock
```

Output

Success shows date and time. Failure shows an appropriate error message.

cloud-deployment

set cloud-deployment

Description

Configures different settings for zero-touch deployment. Command is relevant to preset files.

Syntax

```
set cloud-deployment [ cloud-url <cloud-url> ] [ gateway-name <gateway-
name>
```

```
] [ template <template> ] [ container <container> ]
```

Parameters

Parameter	Description
cloud-url	The DNS or IP address through which the device will connect to the cloud service Type: URL
container	Container Type: String
gateway-name	The appliance name used to identify the gateway Type: A string that contains [A-Z], [0-9] and '-' characters
template	Template Type: String

Example

```
set cloud-deployment cloud-url http://www.checkpoint.com/ gateway-name
My-appliance template TEXT container TEXT
```

show cloud-deployment

Description

Shows the configuration of cloud management connection.

Syntax

```
show cloud-deployment
```

Parameters

Parameter	Description
n/a	

Example

```
show cloud-deployment
```

cloud-notifications

These commands are relevant for Cloud notifications

set cloud-notification

Description

Turn on/off a specific notification type.

Syntax

```
set cloud-notification <notification-type> mode <mode>
```

Parameters

Parameter	Description
notification-type	Describes the notification type including: ■ license-expired ■ license-about-to-expire ■ license-activated ■ infected-device ■ malicious-file-blocked ■ malicious-file-downloaded ■ firmware-upgrade-available ■ new-device ■ system-up ■ unexpected-reboot ■ primary-internet-up ■ secondary-internet-up ■ malicious-mail-blocked ■ malicious-mail-received ■ reconnected-device
mode	Enable sending the chosen cloud notification type.

Example

```
set cloud-notification license-expired mode on
```

show cloud-notifications

Description

Show mode for all types of notifications

Syntax

```
show cloud-notifications
```

Parameters

Parameter	Description
n/a	

Example

```
show cloud-notifications
```

send cloud-report

Description

Force sending a report to Cloud Services.

Syntax

```
send cloud-report type <type>
```

Parameters

Parameter	Description
type	The report type Options: top-last-hour, top-last-day, top-last-week, top-last-month, 3d

Example

```
send cloud-report type top-last-hour
```

cloud-services

reconnect cloud-services

Description

Force a manual reconnection to Cloud Services.

Syntax

```
reconnect cloud-services
```

Parameters

Parameter	Description
n/a	

Example

```
reconnect cloud-services
```

set cloud-services

Configures settings for cloud/SMP management connection.

set cloud-services

Description

Configures settings for cloud/SMP management connection.

Syntax

```
set cloud-services [ { [ activation-key <activation-key> ] | [ [
service-center <service-center> ] [ gateway-id <gateway-id> ] [
registration-key <registration-key> ] ] } ] [ confirm-untrusted-
certificate <confirm-untrusted-certificate> ] [ mode <mode> ]
```

Parameters

Parameter	Description
activation-key	A key received from the Cloud Services provider which is used to initialize the connection to the Cloud Services Type: String
confirm-untrusted-certificate	Is the service center URL is a trusted certificate Type: Boolean (true/false)
gateway-id	Gateway id (in the format <gateway name>.<portal name>). This is not needed if an activation-key was configured. Type: cloudGwName
mode	Indicates if the device is managed by a cloud service Options: off, on
registration-key	Registration key that acts as a password when connecting to the cloud service for the first time. This is not needed if an activation-key was configured. Type: A registration key
service-center	The DNS or IP address through which the device will connect to the cloud service for the first time. This is not needed if an activation-key was configured. Type: URL

Example

```
set cloud-services activation-key TEXT confirm-untrusted-certificate
true mode off
```

set cloud-services

Description

Configures advanced settings for cloud/SMP management connection.

Syntax

```
set cloud-services advanced-settings cloud-management-configuration [
smp-login <smp-login> ] [ show-mgmt-server-details-on-login <show-mgmt-
server-details-on-login> ]
```

Parameters

Parameter	Description
n/a	

Example

```
set cloud-services advanced-settings cloud-management-configuration
smp-login true show-mgmt-server-details-on-login true
```

show cloud-services

Description

Shows advanced settings of cloud management connection.

Syntax

```
show cloud-services advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show cloud-services advanced-settings
```

show cloud-services connection-details

Description

Shows connection details for cloud management connection.

Syntax

```
show cloud-services connection-details
```

Parameters

Parameter	Description
n/a	

Example

```
show cloud-services connection-details
```

cloud-services-firmware-upgrade

set cloud-services-firmware-upgrade

Configure settings for the "firmware upgrade" Cloud Services.

set cloud-services-firmware-upgrade

Description

Configures settings for the "firmware upgrade" Cloud Services.

Syntax

```
set cloud-services-firmware-upgrade [ activate <activate> ] frequency {
immediately-when-available | daily time <time> | monthly day-of-month
<day-of-month> time <time> | weekly day-of-week <day-of-week> time
<time> }
```

Parameters

Parameter	Description
activate	Enable auto firmware upgrades. Upgrades may occur immediately or be scheduled according to a predefined frequency Type: Boolean (true/false)
day-of-month	Choose the desired day of the month Type: A number with no fractional part (integer)
day-of-week	Choose the desired day of week Options: sunday, monday, tuesday, wednesday, thursday, friday, saturday
frequency	Indicates the preferred time to perform upgrade once a new firmware is detected Type: Press TAB to see available options
time	The hour of the upgrade (Format: HH:MM in 24 hour clock) Type: A time format hh:mm

Example

```
set cloud-services-firmware-upgrade activate true frequency
immediately-when-available
```

set cloud-services-firmware-upgrade

Description

Configures advanced settings for the "firmware upgrade" Cloud Services.

Syntax

```
set cloud-services-firmware-upgrade advanced-settings max-num-of-retries
```

<max-num-of-retries>

Parameters

Parameter	Description
n/a	

Example

```
set cloud-services-firmware-upgrade advanced-settings max-num-of-retries 15
```

set cloud-services-firmware-upgrade

Description

Configures advanced settings for the "firmware upgrade" Cloud Services.

Syntax

```
set cloud-services-firmware-upgrade advanced-settings timeout-until-
retry
```

<timeout-until-retry>

Parameters

Parameter	Description
n/a	

Example

```
set cloud-services-firmware-upgrade advanced-settings timeout-until-
retry 15
```

show cloud-services-firmware-upgrade

Shows configuration of the "Firmware Upgrade" Cloud Services.

show cloud-services-firmware-upgrade

Description

Shows configuration of the "Firmware Upgrade" Cloud Services.

Syntax

```
show cloud-services-firmware-upgrade
```

Parameters

Parameter	Description
n/a	

Example

```
show cloud-services-firmware-upgrade
```

show cloud-services-firmware-upgrade

Description

Shows advanced settings of the "Firmware Upgrade" Cloud Services.

Syntax

```
show cloud-services-firmware-upgrade advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show cloud-services-firmware-upgrade advanced-settings
```

show cloud-service managed-blades

Description

Shows the currently managed blades by the cloud management.

Syntax

```
show cloud-services managed-blades
```

Parameters

Parameter	Description
n/a	

Example

```
show cloud-services managed-blades
```

show cloud-services managed-services

Description

Shows the currently managed services by the cloud management.

Syntax

```
show cloud-services managed-services
```

Parameters

Parameter	Description
n/a	

Example

```
show cloud-services managed-services
```

fetch cloud-services policy

Description

Fetch configuration now from your Cloud Services Security Management Server.

Syntax

```
fetch cloud-services policy
```

Parameters

Parameter	Description
n/a	

Example

```
fetch cloud-services policy
```

show cloud-services status

Description

Shows the current status of the cloud management connection.

Syntax

```
show cloud-services status
```

Parameters

Parameter	Description
n/a	

Example

```
show cloud-services status
```

show commands

Description

Shows all available CLI commands.

Syntax

```
show commands
```

Parameters

Parameter	Description
n/a	

Example

```
show commands
```

cphaprob

Description

Defines and manages the critical cluster member properties of the appliance. When a critical process fails, the appliance is considered to have failed.

Syntax

```
cphaprob [-i[a]] [-d <device>] [-s {ok|init|problem}] [-f <file>] [-p]
[register|unregister|report|list|state|if]
```

Parameters

Parameter	Description
`register`	Registers *<appliance>* as a critical process.
`-a`	Lists all devices in the cluster.
`-d <device>`	The name of the device as it appears in the output of the cphaprob list.
`-p`	The configuration change is permanent and applies after the appliance reboots.
`-t <timeout>`	If *<device>* fails to contact ClusterXL in *<timeout>* seconds, *<device>* is considered to have failed. To disable this parameter, enter the value 0.
`-s`	Status to be reported. ok - *<appliance>* is alive init - *<appliance>* is initializing problem - *<appliance>* has failed
`-f <file> register`	Option to automatically register several appliances. The file defined in the *<file>* field should contain the list of appliances with these parameters: ■ *<device>* ■ *<timeout>* ■ Status
`unregister`	Unregisters *<device>* as a critical process.
`report`	Reports the status of the *<device>* to the gateway.

Parameter	Description
`list`	Displays that state of: -i - Internal (as well as external) devices, such as interface check and High Availability initialization. -e - External devices, such as devices registered by the user or outside the kernel. For example, fwd, sync, filter. -ia - All devices, including those used for internal purposes, such as note initialization and load-balance configuration.
`state`	Displays the state of all the gateways in the High Availability configuration.
`if`	Displays the state of interfaces.

Example

```
cphaprob -d $process -t 0 -s ok -p register
```

Output

Success prints OK. Failure shows an appropriate error message.

These are some typical scenarios for the cphaprob command.

Argument	Description
`cphaprob -d` *`<device>`* `-t` *`<timeout(sec)>`* `-s` *`<ok|init|problem>`* `[-p] register`	Register *<device>* as a critical process, and add it to the list of devices that must be running for the cluster member to be considered active.
`cphaprob -f <file> register`	Register all the user defined critical devices listed in *<file>*.
`cphaprob -d` *`<device>`* `[-p] unregister`	Unregister a user defined *<device>* as a critical process. This means that this device is no longer considered critical.
`cphaprob -a unregister`	Unregister all the user defined *<device>*.
`cphaprob -d` *`<device>`* `-s` *`<ok|init|problem>`* `report`	Report the status of a user defined critical device to ClusterXL.
`cphaprob [-i[a]] [-e] list`	View the list of critical devices on a cluster member, and of all the other machines in the cluster.
`cphaprob state`	View the status of a cluster member, and of all the other members of the cluster.
`cphaprob [-a] if`	View the state of the cluster member interfaces and the virtual cluster interfaces.

Examples

```
cphaprob -d <device> -t <timeout(sec)> -s <ok|init|problem> [-p]
register
cphaprob -f <file> register
cphaprob -d <device> [-p] unregister
cphaprob -a unregister
cphaprob -d <device> -s <ok|init|problem> report
cphaprob [-i[a]] [-e] list
cphaprob state
cphaprob [-a] if
```

cphastop

Description

Disables High Availability on the appliance. Running `cphastop`on an appliance that is a cluster member stops the appliance from passing traffic. State synchronization also stops.

Syntax

```
cphastop
```

Parameters

Parameter	Description
`n/a`	

Return Value

0 on success, 1 on failure

Example

```
cphastop
```

Output

Success prints `OK`. Failure shows an appropriate error message.

cpinfo

Description

Creates a Check Point Support Information (CPinfo) file on a machine at the time of execution.

The files is saved to a USB drive or TFTP server.

The CPinfo output file enables Check Point's support engineers to analyze setups from a remote location.

Syntax

```
cpinfo {to-tftp <ipaddr>|to-usb}
```

Parameters

Parameter	Description
`ipaddr`	IPv4 address

Return Value

0 on success, 1 on failure

Example

```
cpinfo to-usb
```

Output

Success prints `Creating cpinfo.txt file`. Failure shows an appropriate error message.

cpstart

Start all Check Point processes and applications running on a machine.

Description

Starts firewall services.

Syntax

```
cpstart
```

Parameters

Parameter	Description
n/a	

Return Value

0 on success, 1 on failure

Example

```
cpstart
```

Output

Success shows `Starting CP products....` Failure shows an appropriate error message.

cpstat

Description

Shows Check Point statistics for applications.

Syntax

```
cpstat [-p <port>] [-s <SICname>] [-f <flavor>] [-o <polling>] [-c
<count>] [-e <period>] [-x] [-j] [-d] application_flag <flag>
```

Parameters

Parameter	Description
`-p <port>`	Port number of the server. The default is the standard server port (18192).
`-s <SICname>`	Secure Internal Communication (SIC) name of the server.
`-f <flavor>`	The flavor of the output (as it appears in the configuration file). The default is the first flavor found in the configuration file.
`-o <polling>`	Polling interval (seconds) specifies the pace of the results. The default is 0, meaning the results are shown only once.
`-c <count>`	Specifies how many times the results are shown. The default is 0, meaning the results are repeatedly shown.
`-e <period>`	Specifies the interval (seconds) over which 'statistical' olds are computed. Ignored for regular olds.
`-x`	XML output mode
`-j`	Json output mode
`-d`	Debug mode.

Parameter	Description

<flag>	One of these applications is displayed:
	One of the following:
	`fw`- Firewall component of the Security Gateway
	`vpn`- VPN component of the Security Gateway
	`fg`- QoS (formerly FloodGate-1)
	`ha`- ClusterXL (High Availability)
	`os`- OS Status
	`mg`- for the Security Management Server
	`persistency`- for historical status values
	`polsrv`
	`uas`
	`svr`
	`cpsemd`
	`cpsead`
	`asm`
	`ls`
	`ca`

Return Value

0 on success, 1 on failure

Example

```
cpstat -c 3 -o 3 fw
```

Output

Success shows `OK`. Failure shows an appropriate error message.

The following flavors can be added to the application flags:

- `fw`- "default", "interfaces", "all", "policy", "perf", "hmem", "kmem", "inspect", "cookies", "chains", "fragments", "totals", "ufp", "http", "ftp", "telnet", "rlogin", "smtp", "pop3", "sync"
- `vpn`- "default", "product", "IKE", "ipsec", "traffic", "compression", "accelerator", "nic", "statistics", "watermarks", "all"
- `fg`- "all"
- `ha`- "default", "all"

- `os`- "default", "ifconfig", "routing", "memory", "old_memory", "cpu", "disk", "perf", "multi_cpu", "multi_disk", "all", "average_cpu", "average_memory", "statistics"
- `mg`- "default"
- `persistency`- "product", "Tableconfig", "SourceConfig"
- `polsrv`- "default", "all"
- `uas`- "default"
- `svr`- "default"
- `cpsemd`- "default"
- `cpsead`- "default"
- `asm`- "default", "WS"
- `ls`- "default"
- `ca`- "default", "crl", "cert", user", "all"

cpstop

Description

Stops firewall services and terminates all Check Point processes and applications running on the appliance.

Syntax

```
cpstop
```

Parameters

Parameter	Description
`n/a`	

Return Value

0 on success, 1 on failure

Example

```
cpstop
```

Output

Success shows `Uninstalling Security Policy....` Failure shows an appropriate error message.

cpwd_admin

Description

The `cpwd_admin` utility can be used to verify if a process is running and to stop and start a process if necessary.

Syntax

```
cpwd_admin {del <name>|detach <name>|list|kill|exist|start_monitor|stop_
monitor|
monitor_list}
```

Parameters

Parameter	Description
`del`	Deletes process
`detach`	Detaches process
`list`	Print status of processes
`kill`	Stops cpWatchDog
`exist`	Checks if cpWatchDog is running
`start_monitor`	cpwd starts monitoring this machine
`stop_monitor`	cpwd stops monitoring this machine
`monitor_list`	Displays list of monitoring processes
`name`	Name of process

Return Value

0 on success, 1 on failure

Example

```
cpwd_admin start_monitor
```

Output

Success shows `OK`. Failure shows an appropriate error message.

date

set date

Configures the device's date and time.

set date

Description

Manually configure the device's date.

Syntax

```
set date <date>
```

Parameters

Parameter	Description
date	Date in the format YYYY-MM-DD Type: A date format yyyy-mm-dd

Example

```
set date 2000-01-01
```

set date

Description

Manually configure the device's time.

Syntax

```
set time <time>
```

Parameters

Parameter	Description
time	Time in the format HH:MM Type: A time format hh:mm

Example

```
set time 23:20
```

set date

Description

Manually configure the device's time zone.

Syntax

```
set timezone <timezone>
```

Parameters

Parameter	Description
timezone	Timezone location

Example

```
set timezone GMT-11:00(Midway-Island)
```

set date

Description

Configures if the daylight savings will be changed automatically.

Syntax

```
set timezone-dst automatic <timezone-dst automatic>
```

Parameters

Parameter	Description
timezone-dst automatic	Automatic adjustment clock for daylight saving changes flag Options: on, off

Example

```
set timezone-dst automatic on
```

show date

Shows date and time.

show date

Description

Shows current date of the appliance.

Syntax

```
show date
```

Parameters

Parameter	Description
n/a	

Example

```
show date
```

show date

Description

Shows current time of the appliance.

Syntax

```
show time
```

Parameters

Parameter	Description
n/a	

Example

```
show time
```

show date

Description

Shows current time zone of the appliance.

Syntax

```
show timezone
```

Parameters

Parameter	Description
n/a	

Example

```
show timezone
```

show date

Description

Shows current daylight savings configuration of the appliance.

Syntax

```
show timezone-dst
```

Parameters

Parameter	Description
n/a	

Example

```
show timezone-dst
```

restore default-settings

Description

Restores the default settings of the appliance without affecting the software image. All the custom user settings for the appliance are deleted.

Syntax

```
restore default-settings [preserve-sic {yes|no}|preserve-license
{yes|no}|force {yes|no}]
```

Parameters

Parameter	Description
`preserve-sic`	Select whether to preserve your current SIC settings.
`preserve-license`	Select whether to preserve your current license.
`force`	Skip the confirmation question.

Return Value

0 on success, 1 on failure

Example

```
restore default-settings preserve-sic yes
```

Comments

The appliance automatically reboots after the default settings are restored.

dhcp-relay

set dhcp-relay

Description

Configures advanced settings for DHCP Relay functionality.

Syntax

```
set dhcp-relay advanced-settings use-internal-ip-addrs-as-source <use-
internal-ip-addrs-as-source>
```

Parameters

Parameter	Description
n/a	

Example

```
set dhcp-relay advanced-settings use-internal-ip-addrs-as-source true
```

show dhcp-relay

Description

Shows advanced settings for DHCP relay.

Syntax

```
show dhcp-relay advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show dhcp-relay advanced-settings
```

show dhcp servers

Description

Shows configuration for all DHCP servers.

Syntax

```
show dhcp servers
```

Parameters

Parameter	Description
n/a	

Example

```
show dhcp servers
```

dhcp server interface

delete dhcp server interface

Description

Deletes the configured exclude range from the DHCP server settings of a specific network/interface.

Syntax

```
delete dhcp server interface <name> exclude-range
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
delete dhcp server interface My_Network exclude-range
```

set dhcp server interface

Configures DHCP server settings.

set dhcp server interface

Description

Configures a custom DHCP option.

Syntax

```
set dhcp server interface <cliName> custom-option name <custom-option
name> type <type> tag <tag> data <data>
```

Parameters

Parameter	Description
cliName	cliName Type: virtual
custom-option name	Set the name of the object Type: A string that contains alphanumeric characters or hyphen
data	Set the desired value of the object Type: String
tag	Select a unique tag for the object Type: A number with no fractional part (integer)
type	Select the appropriate type to store your object Options: string, int8, int16, int32, uint8, uint16, uint32, boolean, ipv4-address, ipv4-address-array, hex-string

Example

```
set dhcp server interface LAN1 custom-option name MyOption type string
tag 43 data TEXT
```

set dhcp server interface

Description

Configures if a DHCP server is active or not on an existing network/interface.

Syntax

```
set dhcp server interface <name> { disable | enable }
```

Parameters

Parameter	Description
dhcp	Use DHCP Server with a specified IP address range Options: off, on, relay
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set dhcp server interface My_Network off
```

set dhcp server interface

Description

Configures DHCP relay functionality on an existing network/interface.

Syntax

```
set dhcp server interface <name> relay relay-to <relay relay-to> { [
secondary <secondary> ] | [ relay-secondary <relay-secondary> ] }
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
relay relay-to	Enter the DHCP server IP address Type: IP address
relay-secondary	This field is deprecated. Please use field 'secondary'
secondary	Enter the secondary DHCP server IP address Type: IP address

Example

```
set dhcp server interface My_Network relay relay-to 192.168.1.1
secondary 192.168.1.1
```

set dhcp server interface

Description

Configures an IP address pool for a DHCP server on an existing network/interface.

Syntax

```
set dhcp server interface <name> include-ip-pool <include-ip-pool>
```

Parameters

Parameter	Description
include-ip-pool	DHCP range Type: A range of IP addresses
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set dhcp server interface My_Network include-ip-pool 192.168.1.1-
192.168.1.10
```

set dhcp server interface

Description

Configures the default gateway provided by a DHCP server on an existing network/interface.

Syntax

```
set dhcp server interface <name> default-gateway <default-gateway>
```

Parameters

Parameter	Description
default-gateway	A virtual field calculated by the values of the fields: dhcpGwMode & dhcpGw
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set dhcp server interface My_Network default-gateway auto
```

set dhcp server interface

Description

Configures the WINS mode provided by a DHCP server on an existing network/interface.

Syntax

```
set dhcp server interface <name> wins-mode <wins-mode>
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
wins-mode	Configure the WINS Server

Example

```
set dhcp server interface My_Network wins-mode auto
```

set dhcp server interface

Description

Configures the WINS servers IP addresses provided by a DHCP server on an existing network/interface.

Syntax

```
set dhcp server interface <name> wins primary <wins primary> [
secondary <secondary> ]
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
secondary	Configure the IP address for the second WINS server
wins primary	Configure the IP address for the first WINS server

Example

```
set dhcp server interface My_Network wins primary 192.168.1.1 secondary
192.168.1.1
```

set dhcp server interface

Description

Configures the lease time used by a DHCP server on an existing network/interface.

Syntax

```
set dhcp server interface <name> lease-time <lease-time>
```

Parameters

Parameter	Description
lease-time	Configure the timeout in hours for a single device to retain a dynamically acquired IP address
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set dhcp server interface My_Network lease-time 30
```

set dhcp server interface

Description

Configures the domain used by a DHCP server on an existing network/interface.

Syntax

```
set dhcp server interface <name> domain <domain>
```

Parameters

Parameter	Description
domain	The domain name of the DHCP
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set dhcp server interface My_Network domain myHost.com
```

set dhcp server interface

Description

Configures the NTP servers used by a DHCP server on an existing network/interface.

Syntax

```
set dhcp server interface <name> ntp <ntp> [ secondary <secondary> ]
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
ntp	Configure the first NTP (Network Time Protocol) server to be distributed to DHCP client
secondary	Configure the second NTP (Network Time Protocol) server to be distributed to DHCP client

Example

```
set dhcp server interface My_Network ntp 192.168.1.1 secondary
192.168.1.1
```

set dhcp server interface

Description

Configures the TFTP server used by a DHCP server on an existing network/interface.

Syntax

```
set dhcp server interface <name> tftp <tftp>
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
tftp	Configure TFTP server to be distributed to DHCP client

Example

```
set dhcp server interface My_Network tftp 192.168.1.1
```

set dhcp server interface

Description

Configures the TFTP bootfile used by a DHCP server on an existing network/interface.

Syntax

```
set dhcp server interface <name> file <file>
```

Parameters

Parameter	Description
file	Configure TFTP bootfile to be distributed to DHCP client
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set dhcp server interface My_Network file word
```

set dhcp server interface

Description

Configures the Call Manager servers used by a DHCP server on an existing network/interface.

Syntax

```
set dhcp server interface <name> callmgr <callmgr> [ secondary
<secondary> ]
```

Parameters

Parameter	Description
callmgr	Configure the first Call manager server to be distributed to DHCP client
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
secondary	Configure the second Call manager server to be distributed to DHCP client

Example

```
set dhcp server interface My_Network callmgr 192.168.1.1 secondary
192.168.1.1
```

set dhcp server interface

Description

Configures the X-Windows display manager server used by a DHCP server on an existing network/interface.

Syntax

```
set dhcp server interface <name> xwin-display-mgr <xwin-display-mgr>
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
xwin-display-mgr	Configure X-Windows display manager to be distributed to DHCP client

Example

```
set dhcp server interface My_Network xwin-display-mgr 192.168.1.1
```

set dhcp server interface

Description

Configures the Avaya Manager server used by a DHCP server on an existing network/interface.

Syntax

```
set dhcp server interface <name>avaya-voip <avaya-voip>
```

Parameters

Parameter	Description
avaya-voip	Configure Avaya IP phone to be distributed to DHCP client
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set dhcp server interface My_Network avaya-voip 192.168.1.1
```

set dhcp server interface

Description

Configures the Nortel Manager server used by a DHCP server on an existing network/interface.

Syntax

```
set dhcp server interface <name> nortel-voip <nortel-voip>
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
nortel-voip	Configure Nortel IP phone to be distributed to DHCP client

Example

```
set dhcp server interface My_Network nortel-voip 192.168.1.1
```

set dhcp server interface

Description

Configures the Thomson Manager server used by a DHCP server on an existing network/interface.

Syntax

```
set dhcp server interface <name> thomson-voip <thomson-voip>
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
thomson-voip	Configure Thomson IP phone to be distributed to DHCP client

Example

```
set dhcp server interface My_Network thomson-voip 192.168.1.1
```

set dhcp server interface

Description

Configures the DNS servers provided by a DHCP server on an existing network/interface. In automatic mode the device will provide its own IP address when configured as DNS proxy, and the DNS servers it is configured with otherwise.

Syntax

```
set dhcp server interface <name> dns { none | manual [ primary
<primary> ] [ secondary <secondary> ] [ tertiary <tertiary> ] | auto }
```

Parameters

Parameter	Description
dns	Configure the DNS Server
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
primary	Configure the IP address for the first DNS server
secondary	Configure the IP address for the second DNS server
tertiary	Configure the IP address for the third DNS server

Example

```
set dhcp server interface My_Network dns none
```

set dhcp server interface

Description

Configures the primary DNS server provided by a DHCP server on an existing network/interface in manual mode.

Syntax

```
set dhcp server interface <name> dns primary <dns primary>
```

Parameters

Parameter	Description
dns primary	Configure the IP address for the first DNS server
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set dhcp server interface My_Network dns primary 192.168.1.1
```

set dhcp server interface

Description

Configures the secondary DNS server provided by a DHCP server on an existing network/interface in manual mode.

Syntax

```
set dhcp server interface <name> dns secondary <dns secondary>
```

Parameters

Parameter	Description
dns secondary	Configure the IP address for the second DNS server
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set dhcp server interface My_Network dns secondary 192.168.1.1
```

set dhcp server interface

Description

Configures the tertiary DNS server provided by a DHCP server on an existing network/interface in manual mode.

Syntax

```
set dhcp server interface <name> dns tertiary <dns tertiary>
```

Parameters

Parameter	Description
dns tertiary	Configure the IP address for the third DNS server
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set dhcp server interface My_Network dns tertiary 192.168.1.1
```

set dhcp server interface

Description

Removes a custom DHCP option from a DHCP server on an existing network/interface.

Syntax

```
set dhcp server interface <name> remove custom-option <custom-option>
```

Parameters

Parameter	Description
custom-option	Set the name of the object
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set dhcp server interface My_Network remove custom-option MyOption
```

show dhcp server interface

Shows configuration of DHCP servers.

show dhcp server interface

Description

Shows the configuration of a DHCP server configured on a specific interface/network.

Syntax

```
show dhcp server interface <name>
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
show dhcp server interface My_Network
```

show dhcp server interface

Description

Shows the IP address pool of a DHCP server configured on a specific interface/network.

Syntax

```
show dhcp server interface <name> ip-pool
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
show dhcp server interface My_Network ip-pool
```

show diag

Description

Shows information about your appliance, such as the current firmware version and additional details.

Syntax

```
show diag
```

Parameters

Parameter	Description
`n/a`	

Example

```
show diag
```

Output

Current system information.

show disk usage

Description

Shows the file system space used and space available.

Syntax

```
show disk-usage [-h|-m|-k]
```

Parameters

Parameter	Description
-h	Human readable (e.g. 1K 243M 2G)
-m	1024*1024 blocks
-k	1024 blocks

Example

```
show disk-usage-h
```

Output

Current file system space used and space available.

dns

delete dns

Deletes configured DNS settings.

delete dns

Description

Deletes configured primary DNS.

Syntax

```
delete dns [ primary ipv4-address ]
```

Parameters

Parameter	Description
n/a	

Example

```
delete dns primary ipv4-address
```

delete dns

Description

Deletes configured secondary DNS.

Syntax

```
delete dns [ secondary ipv4-address ]
```

Parameters

Parameter	Description
n/a	

Example

```
delete dns secondary ipv4-address
```

delete dns

Description

Deletes configured tertiary DNS.

Syntax

```
delete dns [ tertiary ipv4-address ]
```

Parameters

Parameter	Description
n/a	

Example

```
delete dns tertiary ipv4-address
```

delete dns

Description

Deletes configured domain name of the appliance.

Syntax

```
delete domainname
```

Parameters

Parameter	Description
n/a	

Example

```
delete domainname
```

set dns

Configures the DNS and domain settings for the device.

set dns

Description

Configures the DNS settings for the device.

Syntax

```
set dns [ primary ipv4-address <primary ipv4-address> ] [ secondary
ipv4-address <secondary ipv4-address> ] [ tertiary ipv4-address
<tertiary ipv4-address> ]
```

Parameters

Parameter	Description
primary ipv4-address	First global DNS IP address Type: IP address
secondary ipv4- address	Second global DNS IP address Type: IP address
tertiary ipv4-address	Third global DNS IP address Type: IP address

Example

```
set dns primary ipv4-address 192.168.1.1 secondary ipv4-address
192.168.1.1 tertiary ipv4-address 192.168.1.1
```

set dns

Description

Configures the DNS mode for the device. It can either use manually configured DNS servers or use the DNS servers provided to him by the active internet connection from his ISP.

Syntax

```
set dns mode <mode>
```

Parameters

Parameter	Description
mode	Status of appliance using global DNS servers Options: global, internet

Example

```
set dns mode global
```

set dns

Description

Configures the DNS proxy mode. DNS proxy allows treating the configured network objects as a hosts list which the device can translate from hostname to IP address for local networks.

Syntax

```
set dns proxy { on [ resolving <resolving> ] | off }
```

Parameters

Parameter	Description
proxy	Relay DNS requests from internal network clients to the DNS servers defined above Type: Press TAB to see available options
resolving	Use network objects as a hosts list to translate names to their IP addresses Options: on, off

Example

```
set dns proxy on resolving on
```

set dns

Description

Configures the domain settings for the device.

Syntax

```
set domainname <domainname>
```

Parameters

Parameter	Description
domainname	Identification string that defines a realm of administrative autonomy, authority, or control in the Internet Type: A FQDN

Example

```
set domainname somehost.example.com
```

show dns

Shows configuration for DNS and domain name.

show dns

Description

Shows configuration for DNS.

Syntax

```
show dns
```

Parameters

Parameter	Description
n/a	

Example

```
show dns
```

show dns

Description

Shows configuration for domain name.

Syntax

```
show domainname
```

Parameters

Parameter	Description
n/a	

Example

```
show domainname
```

dsl

set dsl advanced-settings global-settings

Description

Set DSL configuration parameters.

Syntax

```
set dsl advanced-settings global-settings [ ginp <ginp> ] [ sra <sra> ]
```

Parameters

Parameter	Description
ginp	Enhanced Impulse Noise Protection
sra	Enables Seamless Rate Adaption

Example

```
set dsl advanced-settings global-settings ginp downstream-and-upstream
sra true
```

set dsl advanced-settings standards

Description

Set DSL standard related configuration parameters.

Syntax

```
set dsl advanced-settings standards [ vdsl2 <true|false> ] [ dmt <
true|false > ] [ adsl-lite < true|false > ] [ adsl2 < true|false > ] [
adsl2plus < true|false > ] [ t1413 < true|false > ] [ annex-m <
true|false > [ annex-l < true|false > ] [ vdsl-8a < true|false > ] [
vdsl-8b < true|false > ] [ vdsl-8c < true|false > ] [ vdsl-8d <
true|false > ] [ vdsl-12a < true|false >] [ vdsl-12b < true|false >] [
vdsl-17a < true|false >] [ vdsl-us0 < true|false > ]
```

Parameters

Parameter	Description
vdsl2	Supports ITU G.993.2 VDSL2 standard.
dmt	Supports ITU G.992.1 ADSL (G.dmt) standard.
adsl-lite	Supports ITU G.992.2 ADSL Lite (G.lite) standard.
adsl2	Supports ITU G.992.3 ADSL2 standard.
adsl2plus	Supports ITU G.992.5 Annex M ADSL2+M standard.
t1413	Supports ANSI T1.413-1998 Issue 2 ADSL.
annex-m	In an Annex A appliance: Combined with supported ADSL2+ it specifies support for Annex M ADSL2+. In an Annex B appliance: Combined with supported ADSL2 it specifies support for Annex J ADSL2.
annex-l	Combined with enabled ADSL2 (G.992.3) specifies support for Annex L.
vdsl-8a	Supports VDSL Profile 8a.
vdsl-8b	Supports VDSL Profile 8b.
vdsl-8c	Supports VDSL Profile 8c.
vdsl-8d	Supports VDSL Profile 8d.
vdsl-12a	Supports VDSL Profile 12a.
vdsl-12b	Supports VDSL Profile 12b.

Parameter	Description
vdsl-17a	Supports VDSL Profile 17a.
vdsl-us0	Enables usage of first upstream band in VDSL2.

Example

```
set dsl advanced-settings standards adsl2plus false
```

show dsl advanced-setting

Description

Show all DSL advanced settings parameters.

Syntax

```
show dsl advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show dsl advanced-settings
```

Sample Output

```
adsl2plus: true
vdsl-8d: true
vdsl-8c: true
vdsl-8b: true
annex-m: false
t1413: true
vdsl-17a: true
adsl-lite: true
vdsl2: true
annex-l: false
vdsl-12b: true
adsl2: true
dmt: true
ginp: disabled
sra: false
vdsl8a: true
vdsl-us0: true
vdsl-12a: true
```

show dsl statistics

Description

Show DSL statistics.

Syntax

```
show dsl statistics
```

Parameters

Parameter	Description
tpstc	Indicates the TPS-TC layer. Possible values: ATM, PTM.
mode	Indicates the negotiated DSL mode. Example for a value: VDSL Annex B.
status	Indicates the status of DSL connection synchronization. Example values: Showtime, G.994.
bitrate-up	Indicates the upstream DSL bit rate.
bitrate-down	Indicates the downstream DSL bit rate.
vendor	4 hexa digits representing the vendor of the DSL chip in the peer DSLAM/MSAG (i.e. IFTN, BDCM) + 4 hex digits representing the firmware version of the vendor.
power-up	Indicates the appliance transmission power (dBm).
hec-up	Indicates the number of HEC errors counted by the peer DSLAM/MSAG.
attn-up	Indicates the upstream attenuation (dB).
attn-down	Indicates the attenuation of the power from the peer DSLAM/MSAG to the appliance (dB).
rs-down	Indicates the number of RS words that were received by the appliance in the downstream.
rs-corrected-down	Indicates the number of RS words that were corrected by the appliance in the downstream.
rs-up	Indicates the number of RS words that were received by the peer DSLAM/MSAG in the upstream.
rs-corrected-up	Indicates the number of RS words that were corrected by the peer DSLAM/MSAG in the upstream.

Parameter	Description
hec-up	Indicates the number of HEC errors counted by the peer DSLAM/MSAG.
hec-down	Indicates the number of HEC errors counted by the appliance.
total-cells-up	Indicates the number of 53 bytes (cells in the case of ATM) that were transmitted by the appliance.
total-cells-down	Indicates the number of 53 bytes (cells in the case of ATM) that were received by the appliance.
configured-sra	Indicates the seamless rate adaptation (SRA) that was configured in the appliance. Possible values: On, Off.
configured-trellis	Indicates whether trellis was enabled in the appliance configuration. Possible values: On, Off.
configured-ginp	Indicates the upstream/downstream on/off for the configured Enhanced Impulse response. Possible values: Off/Off, Off/On, On/Off, On/On
configured-bitswap	Indicates the upstream/downstream on/off for the Bit Swap configured in the appliance. Possible values: On, Off.
vectoring	Indicates the vectoring status. Possible values: 0: Vectoring Training State. 1: Showtime vectoring state, idle, not reporting errors. 2: Initial showtime vector mode state, transition to full factoring when the peer sends a vectoring configuration message. 3: Vectoring state where error samples are being reported upon peer request. 4: Vectoring is disabled. 5: DSLAM/MSAG doesn't support vectoring.

Example

```
show dsl statistics
```

Sample Output

```
snr-down: 8.7
configured-ginp: Off/Off
power-up: 7.6
rs-corrected-down: 421298
rs-corrected-up: 208
configured-sra: Off
rs-up: 1610329207
configured-trellis: On
total-cells-down: 2609810117
snr-up: 15.4
tpstc: PTM
bitrate-up: 5024
vectoring: 5 (DSLAM is not a vectored DSLAM)
vendor: IFTN:0xb206
status: Showtime
rs-down: 2127995393
mode: VDSL2 Annex B
hec-up: 0
bitrate-down: 48470
training: Showtime
power-down: 7.7
total-cells-up: 0
hec-down: 0
attn-down: 25.9
attn-up: 0.0
configured-bitswap: Off
```

dynamic-dns

set dynamic-dns

Configures a persistent domain name for the device.

set dynamic-dns

Description

Configures a persistent domain name for the device.

Syntax

```
set dynamic-dns { is_active } provider <provider> password <password>
user
```

<user> domain *<domain>*

Parameters

Parameter	Description
domain	The domain name (sometimes called host name) within your account that the device will use Type: A FQDN
is-active	Is the DDNS service active Type: Boolean (enable/disable)
password	The password of the account Type: A string that contains alphanumeric and special characters
provider	Select the DDNS provider that you have already set up an account with Options: no-ip.com, DynDns
user	The user name of the account Type: DynDns provider: begins with a letter and have 2-25 alphanumeric char acters. no-ip.com provider: length is 6-15 characters and contains only a-z, 0-9, -, _

Example

```
set dynamic-dns enable provider no-ip.com password a(&7Ba user myUser17
```

set dynamic-dns

Description

Configure advanced settings for the DDNS service.

Syntax

```
set dynamic-dns advanced-settings iterations <iterations>
```

Parameters

Parameter	Description
n/a	

Example

```
set dynamic-dns advanced-settings iterations 15
```

show dynamic-dns

Shows configuration for DDNS service.

show dynamic-dns

Description

Shows configuration for DDNS service.

Syntax

```
show dynamic-dns
```

Parameters

Parameter	Description
n/a	

Example

```
show dynamic-dns
```

show dynamic-dns

Description

Shows advanced settings for DDNS service.

Syntax

```
show dynamic-dns advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show dynamic-dns advanced-settings
```

dynamic objects

Manages dynamic objects on the appliance. The `dynamic_objects` command specifies an IP address to which the dynamic object is resolved.

First, define the dynamic object in the SmartDashboard. Then create the same object with the CLI (-n argument). After the new object is created on the gateway with the CLI, you can use the dynamic_objects command to specify an IP address for the object.

Any change you make to dynamic objects' ranges are applied immediately to the objects. It is not necessary to reinstall the policy.

Description

Manages dynamic objects on the appliance.

Syntax

```
dynamic_objects -o <object> [-r <fromIP> <toIP> ...] [-a] [-d] [-l] [-n
<object> ] [-c] [-do <object>]
```

Parameters

Parameter	Description
`-o`	Name of the dynamic object that is being configured.
`-r`	Defines the range of IP addresses that are being configured for this object.
`-a`	Adds range of IP addresses to the dynamic object.
`-d`	Deletes range of IP addresses from the dynamic object.
`-l`	Lists dynamic objects that are used on the appliance.
`-n`	Creates a new dynamic object.
`-c`	Compare the objects in the dynamic objects file and in objects.
`-do`	Deletes the dynamic object.
<object>	Name of dynamic object.
<fromIP>	Starting IPv4 address.
<toIP>	Ending IPv4 address.

Example

```
dynamic_objects -n sg80gw -r 190.160.1.1 190.160.1.40 -a
```

Output

Success shows `Operation completed successfully`. Failure shows an appropriate error message.

exit

Description

Exits from the shell.

Syntax

```
exit
```

Parameters

Parameter	Description
n/a	

Example

```
exit
```

set expert password

Description

Sets the initial password or password hash for the expert shell

Syntax

```
set expert {password|password-hash} { <pass>| <pass_hash>}
```

Parameters

Parameter	Description
pass	Password using alphanumeric and special characters
pass_hash	Password MD5 string representation

Example

```
set expert password-hash $1$fGT7pGX6$oo9LUBJTkLOGKLhjRQ2rw1
```

Output

Success shows `OK`. Failure shows an appropriate error message.

Comments

To generate a password-hash, you can use this command on any Check Point SMB Appliance gateway (as an expert user).

```
cryptpw -a md5 <password string>
```

fetch certificate

Description

Establishes a SIC connection with the Security Management Server and fetches the certificate. You fetch the certificate from a specific appliance with the `gateway-name` parameter.

Syntax

```
fetch certificate mgmt-ipv4-address <ip_addr> [gateway-name <gw_name>]
```

Parameters

Parameter	Description
`ip_addr`	Management IPv4 address
`gw_name`	Appliance/Module name

Example

```
fetch certificate mgmt-ipv4-address 192.168.1.100 gateway-name SMB_
Appliance
```

Output

Success shows `OK`. Failure shows an appropriate error message.

fetch policy

Description

Fetches a policy from the Security Management Server with IPv4 address *<ip_addr>* or from the local gateway.

Syntax

```
fetch policy {local|mgmt-ipv4-address <ip_addr>}
```

Parameters

Parameter	Description
`ip_addr`	IPv4 address of the Security Management Server.

Return Value

0 on success, 1 on failure

Example

```
fetch policy mgmt-ipv4-address 192.168.1.100
```

Output

Success shows `Done`. Failure shows an appropriate error message.

fw commands

The fw commands are used for working with various aspects of the firewall. All `fw`commands are executed on the Check Point Security Gateway. For more about the `fw`commands, see the *Command Line Interface (CLI) Reference Guide*.

fw commands can be found by typing `fw [TAB]` at a command line. For some of the CLI commands, you can enter the `-h` parameter to display all the relevant arguments and parameters. These commands are:

fw command	Explanation
`fw accel [-h]`	Turn acceleration on/off
`fw activation [-h]`	Activate license
`fw avload [-h]`	Load Anti-Virussignatures to kernel
`fw ctl [args]`	Control kernel
`fw debug [-h]`	Turn debug output on or off
`fw fetch`	Fetch last policy
`fw fetchdefault [-h]`	Fetch default policy
`fw fetchlocal [-h]`	Fetch local policy
`fw monitor [-h]`	Monitor Check Point Appliance traffic
`fw pull_cert`	Pull certificate from internal CA
`fw sfwd`	fw daemon
`fw sic_init [-h]`	Initialize SIC
`fw sic_reset [-h]`	Reset SIC
`fw sic_test`	Test SIC with management
`fw stat [-h]`	Display policy installation status of the gateway. (Command is provided for backward compatibility.)
`fw tab [-h]`	Display kernel-table content
`fw unloadlocal`	Unload local policy

`fw ver [-k]`	Display version

fw policy

set fw policy

Configures the default policy for the Firewall blade

set fw policy

Description

Configures the default policy for the Firewall blade.

Syntax

```
set fw policy [ mode <mode> ] [ track-allowed-traffic <track-allowed-
traffic>
```

```
] [ track-blocked-traffic <track-blocked-traffic> ]
```

Parameters

Parameter	Description
mode	Current mode for firewall policy
track-allowed-traffic	Indicates if accepted connections are logged Options: none, log
track-blocked-traffic	Indicates if blocked connections are logged Options: none, log

Example

```
set fw policy mode off track-allowed-traffic none track-blocked-traffic
none
```

set fw policy

Description

Configures advanced settings for the default policy of the Firewall blade.

Syntax

```
set fw policy advanced-settings blocked-packets-action <blocked-
packets-action>
```

Parameters

Parameter	Description
n/a	

Example

```
set fw policy advanced-settings blocked-packets-action auto
```

set fw policy

Description

Configures advanced settings for the default policy of the Firewall blade.

Syntax

```
set fw policy advanced-settings log-implied-rules <log-implied-rules>
```

Parameters

Parameter	Description
n/a	

Example

```
set fw policy advanced-settings log-implied-rules true
```

show fw policy

Shows the configured policy for the Firewall blade.

show fw policy

Description

Shows the configured policy for the Firewall blade.

Syntax

```
show fw policy
```

Parameters

Parameter	Description
n/a	

Example

```
show fw policy
```

show fw policy

Description

Shows advanced settings for the Firewall blade.

Syntax

```
show fw policy advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show fw policy advanced-settings
```

show fw policy

Description

Shows the configuration for customizable messages shown to users upon actions.

Syntax

```
show fw policy user-check { block | ask | accept }
```

Parameters

Parameter	Description
user-check	Activity message type Type: Press TAB to see available options

Example

```
show fw policy user-check block
```

set fw policy user-check accept

Description

Configures a customizable "accept" message shown to users upon match on browser based traffic.

Syntax

```
set fw policy user-check accept [ body <body> ] [ fallback-action
<fallback-action> ] [ frequency <frequency> ] [ subject <subject> ] [
title <title> ]
```

Parameters

Parameter	Description
body	The informative text that appears in the APPI 'Accept' user message Type: A string that contains only printable characters
fallback-action	Indicates the action to take when an 'Accept' user message cannot be displayed Options: block, accept
frequency	Indicates how often is the APPI 'Accept' user message is being presented to the same user Options: day, week, month
subject	The subject of an APPI 'Accept' user message Type: A string that contains only printable characters
title	The title of an APPI 'Accept' user message Type: A string that contains only printable characters

Example

```
set fw policy user-check accept body My Network fallback-action block
frequency day subject My Network title My Network
```

set fw policy user-check ask

Description

Configures a customizable "ask" message shown to users upon match on browser based traffic.

Syntax

```
set fw policy user-check ask [ body <body> ] [ confirm-text <confirm-
text>
```

```
] [ fallback-action <fallback-action> ] [ frequency <frequency> ] [
subject <subject> ] [ title <title> ] [ reason-displayed <reason-
displayed> ]
```

Parameters

Parameter	Description
body	The informative text that appears in the APPI 'Ask' user message Type: A string that contains only printable characters
confirm-text	This text appears next to the 'ignore warning' checkbox of an APPI 'Ask' user message Type: A string that contains only printable characters
fallback-action	The action that is performed when the 'Ask' message cannot be shown Options: block, accept
frequency	Indicates how often is the APPI 'Ask' user message is being presented to the same user Options: day, week, month
reason-displayed	Indicates if the user must enter a reason for ignoring this message in a designated text dialog Type: Boolean (true/false)
subject	The subject of an APPI 'Ask' user message Type: A string that contains only printable characters
title	The title of an APPI 'Ask' user message Type: A string that contains only printable characters

Example

```
set fw policy user-check ask body My Network confirm-text My Network
fallback-action block frequency day subject My Network title My Network
reason-displayed true
```

set fw policy user-check block

Description

Configures a customizable "block" message shown to users upon match on browser based traffic.

Syntax

```
set fw policy user-check block [ body <body> ] [ redirect-url
<redirect-url>
```

```
] [ subject <subject> ] [ title <title> ] [ redirect-to-url <redirect-to-
url>]
```

Parameters

Parameter	Description
body	The informative text that appears in the APPI 'Block' user message Type: A string that contains only printable characters
redirect-to-url	Indicates if the user will be redirected to a custom URL in case of a 'Block' action Type: Boolean (true/false)
redirect-url	Indicates the URL to redirect the user in case of a 'Block' action if configured to do so. The URL to redirect the user in case of a 'Block' action. Redirection happens only if this functionality is turned on Type: urlWithHttp
subject	The subject of an APPI 'Block' user message Type: A string that contains only printable characters
title	The title of an APPI 'Block' user message Type: A string that contains only printable characters

Example

```
set fw policy user-check block body My Network redirect-url urlWithHttp
subject My Network title My Network redirect-to-url true
```

set fw policy user-check block-device

Description

User Check is a customizable message shown to users upon match, and allows to 'ask' the user for the desired action. In this case, to block a particular device.

Syntax

```
set fw policy user-check block-device [ body <body> ] [ subject
<subject> ] [ title <title>
```

Parameters

Parameter	Description
body	The informative text that appears in the 'Block Device' user message. Type: A string that contains only printable characters
subject	The subject of the 'Block Device' user message Type: A string that contains only printable characters
title	The title of the 'Block Device' user message Type: A string that contains only printable characters

Example

```
set fw policy user-check block-device body My Network subject My
Network title My Network
```

set fw policy user-check block-infected-device

Description

User Check is a customizable message shown to users upon match, and allows to 'ask' the user for the desired action. In this case, to block an infected device.

Syntax

```
set fw policy user-check block-infected-device [ body <body> ] [
subject <subject> ] [ title <title> ]
```

Parameters

Parameter	Description
body	The informative text that appears in the 'Block Infected Device' user message Type: A string that contains only printable characters
subject	The subject of the 'Block Infected Device' user message Type: A string that contains only printable characters
title	The title of the 'Block Infected Device' user message Type: A string that contains only printable characters

Example

```
set fw policy user-check block-infected-device body My Network subject
My Network title My Network
```

global-radius-conf

set global-radius-conf

Description

Configure the NAS IP\IPv6 address for RADIUS server authentication.

NAS IP\IPv6 address indicates the identifying IP Address of the NAS which is requesting authentication of the user, and should be unique to the NAS within the scope of the RADIUS server.

Syntax

```
set global-radius-conf [ nas-ip-address <nas-ip-address> ] [ nasIPV6
<nasIPV6> ]
```

Parameters

Parameter	Description
nas-ip-address	Nas ip address Type: IP address
nasIPV6	nasIPV6 Type: ipv6addr

Example

```
set global-radius-conf nas-ip-address 192.168.1.1 nasIPV6 ipv6addr
```

show global-radius-conf

Description

Configure the NAS IP\IPv6 address for RADIUS server authentication.

Syntax

```
show global-radius-conf
```

Parameters

Parameter	Description
n/a	

Example

```
show global-radius-conf
```

group

add group

Description

Adds a new group of network objects.

Syntax

```
add group name <name> [ comments <comments> ] [ member <member> ]
```

Parameters

Parameter	Description
comments	Comments and explanation about the Network Object group Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
member	An association field to the contained network objects
name	Network Object group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
add group name myObject_17 comments "This is a comment." member TEXT
```

delete group

Description

Deletes an existing group object of network objects.

Syntax

```
delete group <name>
```

Parameters

Parameter	Description
name	Network Object group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
delete group myObject_17
```

set group

Configures an existing network objects group.

set group

Description

Configures an existing network objects group.

Syntax

```
set group <name> [ new-name <new-name> ] [ comments <comments> ]
```

Parameters

Parameter	Description
comments	Comments and explanation about the Network Object group Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
name	Network Object group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces
new-name	Network Object group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
set group myObject_17 new-name myObject_17 comments "This is a
comment."
```

set group

Description

Removes all members from an existing network objects group.

Syntax

```
set group <name> remove-all members
```

Parameters

Parameter	Description
name	Network Object group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
set group myObject_17 remove-all members
```

set group

Description

Adds an existing network object to an existing network objects group.

Syntax

```
set group <name> add member <member>
```

Parameters

Parameter	Description
member	Network Object name
name	Network Object group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
set group myObject_17 add member TEXT
```

set group

Description

Removes an existing network object from an existing network objects group.

Syntax

```
set group <name> remove member <member>
```

Parameters

Parameter	Description
member	Network Object name
name	Network Object group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
set group myObject_17 remove member TEXT
```

show group

Description

Shows the contents of a network object group.

Syntax

```
show group <name>
```

Parameters

Parameter	Description
name	Network Object group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
show group myObject_17
```

show groups

Description

Shows the contents of all network object groups.

Syntax

```
show groups
```

Parameters

Parameter	Description
n/a	

Example

```
show groups
```

host

add host

Description

Adds a new network host object that can be used for resolving when the device acts as a DNS proxy, and also DHCP settings for this object (exclude/reserve IP address).

Syntax

```
add host name <name> [ dhcp-exclude-ip-addr { on [ dhcp-reserve-ip-
addr-to-mac { on [ mac-addr <mac-addr> ] [ reserve-mac-address
<reserve-mac-address> ] | off } ] [ mac-reserved-in-dhcp { on [ mac-
addr <mac-addr> ] [ reserve-mac-address <reserve-mac-address> ] | off }
] | off } ] [ dns-resolving <dns-resolving> ] ipv4-address <ipv4-
address>
```

Parameters

Parameter	Description
dhcp-exclude-ip-addr	Indicates if the object's IP address(es) is excluded from internal DHCP daemon Type: Press TAB to see available options
dhcp-reserve-ip-addr- to-mac	Indicates if the IP address is reserved in internal DHCP daemon Type: Press TAB to see available options
dns-resolving	Indicates if the name of the server/network object will be used as a hostname for internal DNS service Type: Boolean (true/false)
ipv4-address	The beginning of the IP range
mac-addr	MAC address of the Network Object Type: MAC address
mac-reserved-in-dhcp	This field is deprecated. Please use field 'dhcp-reserve-ip-addr-to-mac'
name	Network Object name Type: String
reserve-mac-address	This field is deprecated. Please use field 'mac-addr'

Example

```
add host name TEXT dhcp-exclude-ip-addr on dhcp-reserve-ip-addr-to-mac
on mac-addr 00:1C:7F:21:05:BE reserve-mac-address 00:1C:7F:21:05:BE
mac-reserved-in-dhcp on mac-addr 00:1C:7F:21:05:BE reserve-mac-address
00:1C:7F:21:05:BE dns-resolving true ipv4-address 192.168.1.1
```

delete host

Description

Deletes an existing network host object.

Syntax

```
delete host <name>
```

Parameters

Parameter	Description
name	Network Object name Type: String

Example

```
delete host TEXT
```

set host

Description

Configures an existing network object/host.

Syntax

```
set host <name> [ name <name> ] [ dhcp-exclude-ip-addr { on [ dhcp-
reserve-ip-addr-to-mac { on [ mac-addr <mac-addr> ] [ reserve-mac-
address <reserve-mac-address> ] | off } ] [ mac-reserved-in-dhcp { on [
mac-addr <mac-addr> ] [ reserve-mac-address <reserve-mac-address> ] |
off } ] | off } ] [ exclude-from-dhcp { on [ dhcp-reserve-ip-addr-to-
mac { on [ mac-addr <mac-addr>] [ reserve-mac-address <reserve-mac-
address> ] | off } ] [ mac-reserved-in-dhcp { on [ mac-addr <mac-addr>
] [ reserve-mac-address <reserve-mac-address> ] | off } ] | off } ] [
dns-resolving <dns-resolving>] [ ipv4-address <ipv4-address> ]
```

Parameters

Parameter	Description
dhcp-exclude-ip-addr	Indicates if the object's IP address(es) is excluded from internal DHCP daemon Type: Press TAB to see available options
dhcp-reserve-ip-addr-to-mac	Indicates if the IP address is reserved in internal DHCP daemon Type: Press TAB to see available options
dns-resolving	Indicates if the name of the server/network object will be used as a hostname for internal DNS service Type: Boolean (true/false)
exclude-from-dhcp	This field is deprecated. Please use field 'dhcp-reserve-ip-addr-to-mac'
ipv4-address	The beginning of the IP range
mac-addr	MAC address of the Network Object Type: MAC address
mac-reserved-in-dhcp	This field is deprecated. Please use field 'dhcp-reserve-ip-addr-to-mac'
name	Network Object name Type: String
reserve-mac-address	This field is deprecated. Please use field 'mac-addr'

Example

```
set host TEXT name TEXT dhcp-exclude-ip-addr on dhcp-reserve-ip-addr-
to-mac on mac-addr 00:1C:7F:21:05:BE reserve-mac-address
00:1C:7F:21:05:BE mac-reserved-in-dhcp on mac-addr 00:1C:7F:21:05:BE
reserve-mac-address 00:1C:7F:21:05:BE exclude-from-dhcp on dhcp-
reserve-ip-addr-to-mac on mac-addr 00:1C:7F:21:05:BE reserve-mac-
address 00:1C:7F:21:05:BE mac-reserved-in-dhcp on mac-addr
00:1C:7F:21:05:BE reserve-mac-address 00:1C:7F:21:05:BE dns-resolving
true ipv4-address 192.168.1.1
```

show host

Description

Shows the configuration of an existing network object.

Syntax

```
show host <name>
```

Parameters

Parameter	Description
name	Network Object name Type: String

Example

```
show host TEXT
```

show hosts

Description

Shows the configuration of all existing network objects.

Syntax

```
show hosts
```

Parameters

Parameter	Description
n/a	

Example

```
show hosts
```

hotspot

set hotspot

Configures hotspot settings.

set hotspot

Description

Configures hotspot settings.

Syntax

```
set hotspot [ require-auth <require-auth> ] [ auth-mode <auth-mode> ] [
allowed-group <allowed-group> ] [ timeout <timeout> ] [ portal-title
<portal-title> ] [ portal-msg <portal-msg> ] [ show-terms-of-use <show-
terms-of-use> ] [ terms-of-use <terms-of-use> ] [ redirect-after-auth
<redirect-after-auth> ] [ redirect-after-auth-url <redirect-after-auth-
url> ]
```

Parameters

Parameter	Description
allowed-group	Indicates the specific user group that can authenticate through the hotspot when auth-mode is set to allow-specific-group Type: A string of alphanumeric characters without space between them
auth-mode	Allow access to a specific user group only or all users Options: allow-all, allow-specific-group
portal-msg	The message shown in hotspot portal Type: A string that contains only printable characters
portal-title	The title of the hotspot portal Type: A string that contains only printable characters
redirect-after-auth	Indicates if after the user accepts terms or authenticate in the hotspot portal the user will be redirected to a configured external URL instead of the originally requested URL Options: on, off
redirect-after-auth-url	Redirect the user to the following URL after the user accepts terms or authenticate in the hotspot portal Type: urlWithHttp
require-auth	Indicates if user authentication is required Type: Boolean (true/false)
show-terms-of-use	Indicates if a terms and conditions link will be shown in the hotspot portal Options: on, off

Parameter	Description
terms-of-use	Indicates the When users will click the terms and conditions text shown in the hotspot portal Type: A string that contains only printable characters
timeout	Time, in minutes, untill the hotspot session expires Type: A number with no fractional part (integer)

Example

```
set hotspot require-auth true auth-mode allow-all allowed-group word
timeout 15 portal-title My Network portal-msg My Network show-terms-of-
use on terms-of-use My Network redirect-after-auth on redirect-after-
auth-url urlWithHttp
```

set hotspot

Description

Adds an existing network object as an exception for hotspot portal.

Syntax

```
set hotspot add exception <exception>
```

Parameters

Parameter	Description
exception	Network object name

Example

```
set hotspot add exception TEXT
```

set hotspot

Description

Removes an existing network object from being an exception to hotspot portal.

Syntax

```
set hotspot remove exception <exception>
```

Parameters

Parameter	Description
exception	Network object name

Example

```
set hotspot remove exception TEXT
```

set hotspot

Description

Configures advanced hotspot settings.

Syntax

```
set hotspot advanced-settings activation <activation>
```

Parameters

Parameter	Description
n/a	

Example

```
set hotspot advanced-settings activation on
```

set hotspot

Description

Configures advanced hotspot settings.

Syntax

```
set hotspot advanced-settings prevent-simultaneous-login <prevent-simultaneous-login>
```

Parameters

Parameter	Description
n/a	

Example

```
set hotspot advanced-settings prevent-simultaneous-login true
```

show hotspot

Shows hotspot configuration.

show hotspot

Description

Shows hotspot configuration.

Syntax

```
show hotspot
```

Parameters

Parameter	Description
n/a	

Example

```
show hotspot
```

show hotspot

Description

Shows hotspot advanced settings configuration.

Syntax

```
Shows hotspot advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
Shows hotspot advanced-settings
```

https-categorization

set https-categorization

Configures HTTPS categorization settings (categorization does not require a full SSL inspection mechanism).

set https-categorization

Description

Configures advanced HTTPS categorization settings.

Syntax

```
set https-categorization advanced-settings validate-cert-expiration
<validate-cert-expiration>
```

Parameters

Parameter	Description
n/a	

Example

```
set https-categorization advanced-settings validate-cert-expiration
true
```

set https-categorization

Description

Configures advanced HTTPS categorization settings.

Syntax

```
set https-categorization advanced-settings validate-unreachable-crl
<validate-unreachable-crl>
```

Parameters

Parameter	Description
n/a	

Example

```
set https-categorization advanced-settings validate-unreachable-crl
true
```

set https-categorization

Description

Configures advanced HTTPS categorization settings.

Syntax

```
set https-categorization advanced-settings validate-crl <validate-crl>
```

Parameters

Parameter	Description
n/a	

Example

```
set https-categorization advanced-settings validate-crl true
```

show https-categorization

Description

Shows configuration for HTTPS categorization feature.

Syntax

```
show https-categorization advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show https-categorization advanced-settings
```

interface

add interface

Adds a new virtual interface.

add interface

Description

Adds a new 802.1q tag-based VLAN over an existing physical interface.

Syntax

```
add interface <assignment> vlan <vlan>
```

Parameters

Parameter	Description
assignment	The switch or bridge which the object belongs to Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
vlan	Enter a number that is the virtual identifier Type: A number with no fractional part (integer)

Example

```
add interface My_Network vlan 12
```

add interface

Description

Adds a new numbered/unnumbered Virtual Tunnel Interface (VTI) to be used for Route-based VPN purposes.

Syntax

```
add vpn tunnel <vpn tunnel> type { unnumbered peer <peer> internet-
connection <internet-connection> | numbered local <local> remote
<remote> peer <peer> }
```

Parameters

Parameter	Description
internet-connection	The local interface for unnumbered VTI
local	Enter the IP address of the interface Type: IP address
peer	Remote peer name as defined in the VPN community. You must define the two peers in the VPN community before you can define the VTI. The Peer ID is an alpha-numeric character string. Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces
remote	Defines the remote peer IPv4 address, used at the peer gateway's point-to-point virtual interface (numbered VTI only) Type: IP address
type	The type of VTI: Numbered VTI that uses a specified, static IPv4 addresses for local and remote connections, or unnumbered VTI that uses the interface and the remote peer name to get addresses Type: Press TAB to see available options
vpn tunnel	A number identifying the Virtual Tunnel Interface (VTI) Type: A number with no fractional part (integer)

Example

```
add vpn tunnel 12 type unnumbered peer site17 internet-connection My
connection
```

delete interface

Description

Deletes an existing virtual interface.

Syntax

```
delete interface <name>
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
delete interface My_Network
```

set interface

Configures local networks/interfaces.

set interface

Description

Configures local networks/interfaces.

Syntax

```
set interface <name> ipv4-address <ipv4-address> { subnet-mask <subnet-
mask> default-gw <default-gw> [ dns-primary <dns-primary> [ dns-
secondary <dns-secondary> [ dns-tertiary <dns-tertiary> ] ] ] | mask-
length <mask-length> default-gw <default-gw> [ dns-primary <dns-
primary> [ dns-secondary <dns-secondary> [ dns-tertiary <dns-tertiary>
] ] ] }
```

Parameters

Parameter	Description
default-gw	Default gateway Type: IP address
dns-primary	First DNS server IP address Type: IP address
dns-secondary	Second DNS server IP address Type: IP address
dns-tertiary	Third DNS server IP address Type: IP address
ipv4-address	The IP address Type: IP address
mask-length	Subnet mask length Type: A string that contains numbers only
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
subnet-mask	Subnet mask Type: Subnet mask

Example

```
set interface My_Network ipv4-address 192.168.1.100 subnet-mask
255.255.255.0 default-gw 192.168.1.1 dns-primary 192.168.1.1 dns-
secondary 192.168.1.2 dns-tertiary 192.168.1.3
```

set interface

Description

Configures IP address for local networks/interfaces.

Syntax

```
set interface <name> ipv4-address <ipv4-address>{ mask-length <mask-
length> | subnet-mask <subnet-mask> }
```

Parameters

Parameter	Description
ipv4-address	Enter the IP address of the interface Type: IP address
mask-length	Represents the network's mask length Type: A string that contains numbers only
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
subnet-mask	Enter the Subnet mask of the specified network Type: A subnet mask, or 255.255.255.255

Example

```
set interface My_Network ipv4-address 192.168.1 mask-length 20
```

set interface

Description

Configures a physical interface to be unassigned from existing networks.

Syntax

```
set interface <name> unassigned
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set interface LAN2 unassigned
```

set interface

Description

Configures monitor mode on an existing local network/interface.

Syntax

```
set interface <name> monitor-mode
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set interface My_Network monitor-mode
```

set interface

Description

Configures advanced settings on an existing local network/interface.

Syntax

```
set interface <name>[ mac-address-override <mac-address-override> ] [
exclude-from-dns-proxy <exclude-from-dns-proxy> ]
```

Parameters

Parameter	Description
exclude-from-dns- proxy	Exclude from DNS proxy Options: on, off
mac-address-override	Override default MAC address Type: MAC address
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set interface My_Network mac-address-override 00:1C:7F:21:05:BE
exclude-from-dns-proxy on
```

set interface

Description

Configures networking settings on an existing local network/interface.

Syntax

```
set interface <name> [ auto-negotiation <auto-negotiation> ] [ mtu
<mtu> ] [ link-speed <link-speed>]
```

Parameters

Parameter	Description
auto-negotiation	Enable this option in order to manually configure the link speed of the interface. Options: on, off
link-speed	Configure the link speed of the interface manually Options: 10/full, 10/half, 100/full, 100/half
mtu	Configure the Maximum Transmission Unit size for an interface Type: A number with no fractional part (integer)
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set interface My_Network auto-negotiation on mtu 1460 link-speed
10/full
```

set interface

Description

Enable/disable an existing local network/interface.

Syntax

```
set interface <name> state <state>
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
state	The mode of the network - enabled or disabled Options: on, off

Example

```
set interface My_Network state on
```

set interface

Description

Configures a description for an existing local network/interface.

Syntax

```
set interface <name> [ description <description> ]
```

Parameters

Parameter	Description
description	Description Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set interface My_Network description "This is a comment."
```

set interface

Description

Configures automatic access policy for an existing local network/interface. This feature is relevant when the device is locally managed.

Syntax

```
set interface <name> [ lan-access <lan-access> ] [ lan-access-track
<lan-access-track>
```

Parameters

Parameter	Description
lan-access	Local networks will be accessible from this network once this option is enabled Options: block, accept
lan-access-track	Traffic from this network to local networks will be logged once this option is enabled Options: none, log
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set interface My_Network lan-access block lan-access-track none
```

set interface

Description

Configure hotspot functionality for an existing local network/interface.

Syntax

```
set interface <name> hotspot <hotspot>
```

Parameters

Parameter	Description
hotspot	Redirect users to the Hotspot portal before allowing access from this interface Options: on, off
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set interface My_Network hotspot on
```

show interface

Description

Shows configuration and details of local networks.

Syntax

```
show interface <name> [ all ]
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
show interface My_Network all
```

show interfaces

Description

Shows the list of defined local networks.

Syntax

```
show interfaces
```

Parameters

Parameter	Description
n/a	

Example

```
show interfaces
```

show interfaces all

Description

Shows details of all defined local networks.

Syntax

```
show interfaces all
```

Parameters

Parameter	Description
n/a	

Example

```
show interfaces all
```

internal-certificates-conf

Configure settings for internal certificates.

add internal-certificate

Description

Add an internal certificate.

Syntax

```
add internal-certificate certificate-name <certificate-name> p12-password <p12-
password> url <url> [ less secure <less-secure> ]
```

Parameters

Parameter	Description
certificate-name	Informal representation for the Certificate Type: String
Less-secure	Allow connections to SSL sites without certificates. Only applied over SFTP. Type: Boolean (true/false)
P12-password	PKCS#12 Password, PKCS #12 defines an archive file format for storing many cryptography objects as a single file Type: A registration key
url	Download the certificate file from this URL. The URL format should be (s)ftp://name:passwd@machine.domain:port/full_path_to_file Type: ftpUrl

Example

```
add internal-certificate certificate-name TEXT p12-password QWEDFRGH4 url ftpUrl
less-secure true
```

delete internal-certificate

Description

Delete an internal certificate.

Syntax

```
delete internal-certificate name <name>
```

Parameters

Parameter	Description
name	Name of the internal certificate Type: String

Example

```
delete internal-certificate name TEXT
```

show internal-certificate

Description

Show an internal certificate.

Syntax

```
show internal-certificate name <name>
```

Parameters

Parameter	Description
name	Name of the internal certificate Type: String

Example

```
show internal-certificate name TEXT
```

show internal-certificates

Description

Show all internal certificates.

Syntax

```
show internal-certificates
```

Parameters

Parameter	Description
n/a	

Example

```
show internal-certificates
```

ips engine-settings

set ips engine-settings

set ips engine-settings

Description

Configures advanced IPS engine settings. This command configures if and when IPS will deactivate upon high resource consumption of the device.

Syntax

```
set ips engine-settings [ protection-scope <protection-scope> ] [
bypass-under-load { true [ bypass-track <bypass-track>] [ gateway-load-
thresholds [ cpu-usage-low-watermark <cpu-usage-low-watermark>] [ cpu-
usage-high-watermark <cpu-usage-high-watermark> ] [ memory-usage-low-
watermark <memory-usage-low-watermark> ] [ memory-usage-high-watermark
<memory-usage-high-watermark> ] [ threshold-detection-delay <threshold-
detection-delay> ] ] | false } ]
```

Parameters

Parameter	Description
bypass-track	Indicates how the appliance will track events where the bypass mechanism is activated/deactivated Options: none, log, alert
bypass-under-load	Indicates if the IPS engine will move to bypass mode if the appliance is under heavy load Type: Boolean (true/false)
protection-scope	Indicates if the IPS blade will protect internal networks only or protect all networks (including external networks) Options: protect-internal-hosts-only, perform-ips-inspection-on-all-traffic

Example

```
set ips engine-settings protection-scope protect-internal-hosts-only
bypass-under-load true bypass-track none gateway-load-thresholds cpu-
usage-low-watermark 75 cpu-usage-high-watermark 80 memory-usage-low-
watermark 75 memory-usage-high-watermark 80 threshold-detection-delay
90
```

set ips engine-settings

Description

Configures advanced IPS engine settings. This command configures a legacy error page shown in some legacy IPS HTTP protections.

Syntax

```
set ips engine-settings advanced-settings AboutConfigIPSErrorPageConfig
[ status-code-desc <status-code-desc> ] [ show-error-code <show-error-
code> ] [ logo-url <logo-url> ] [ send-detailed-status-code <send-
detailed-status-code>
```

```
] [ enable-logo-url <enable-logo-url> ]
```

Parameters

Parameter	Description
n/a	

Example

```
set ips engine-settings advanced-settings AboutConfigIPSErrorPageConfig
status-code-desc "This is a comment." show-error-code true logo-url
http://www.checkpoint.com/ send-detailed-status-code true enable-logo-
url true
```

set ips engine-settings

Description

Configures advanced IPS engine settings. This command configures a legacy error page shown in some legacy IPS HTTP protections.

Syntax

```
set ips engine-settings advanced-settings AboutConfigIPSErrorPage [
send-error-code <send-error-code>] [ error-page-for-supported-web-
protections <error-page-for-supported-web-protections> ] [ url <url> ]
```

Parameters

Parameter	Description
n/a	

Example

```
set ips engine-settings advanced-settings AboutConfigIPSErrorPage send-
error-code true error-page-for-supported-web-protections do-not-show
url http://www.checkpoint.com/
```

show ips engine-settings

Shows engine settings for the IPS blade.

show ips engine-settings

Description

Shows engine settings for the IPS blade.

Syntax

```
show ips engine-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show ips engine-settings
```

show ips engine-settings

Description

Shows advanced engine settings for the IPS blade.

Syntax

```
show ips engine-settings advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show ips engine-settings advanced-settings
```

interface-loopback

add interface-loopback

Description

Adds a new loopback interface (A fixed interface in the system that is commonly used for dynamic routing purposes).

Syntax

```
add interface-loopback ipv4-address <ipv4-address> { mask-length <mask-
length> | subnet-mask <subnet-mask> }
```

Parameters

Parameter	Description
ipv4-address	Enter the IP address of the interface Type: IP address
mask-length	Represents the network's mask length Type: A string that contains numbers only
subnet-mask	Enter the Subnet mask of the specified network Type: A subnet mask, or 255.255.255.255

Example

```
add interface-loopback ipv4-address 192.168.1.1 mask-length 20
```

delete interface-loopback

Description

Deletes an existing configured loopback interface.

Syntax

```
delete interface-loopback <name>
```

Parameters

Parameter	Description
name	Network name Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
delete interface-loopback My_Network
```

internet

set internet

Description

Configures advanced settings for internet connectivity.

Syntax

```
set internet advanced-settings reset-sierra-usb-on-lsi-event <reset-sierra-usb-on-lsi-event>
```

Parameters

Parameter	Description
n/a	

Example

```
set internet advanced-settings reset-sierra-usb-on-lsi-event true
```

show internet

Description

Shows advanced settings for configured internet

Syntax

```
show internet advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show internet advanced-settings
```

internet-connection

add internet-connection

Adds a new internet connection.

add internet-connection (physical interface)

Description

Adds a new internet connection using an existing physical interface (multiple internet connection can engage in High Availability/Load Sharing).

WAN

Syntax for DHCP

```
add internet-connection name <name> interface WAN type dhcp
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
interface	Interface name Type: Press TAB to see available options
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
type	Connection type Type: Press TAB to see available options
vlan-id	VLAN ID Type: A number with no fractional part (integer)

Syntax for Static IP

```
add internet-connection name <name> interface WAN type static default-gw <default-gw> ipv4-address <ipv4-address> mask-length <mask-length>
```

```
add internet-connection name <name> interface WAN type static default-gw <default-gw> ipv4-address <ipv4-address> subnet-mask <subnet-mask> { dns-primary <dns-primary>dns-secondary <dns-secondary> dns-tertiary <dns-tertiary>} { use-connection-as-vlan vlan-id <vlan-id>} { conn-test-timeout <conn-test-timeout>}
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
interface	Interface name Type: Press TAB to see available options
default-gw	WAN default gateway (in the advanced section of PPTP and l2TP) Type: IP address
dns-primary	First DNS server IP address Type: IP address
dns-secondary	Second DNS server IP address Type: IP address
dns-tertiary	Third DNS server IP address Type: IP address
ipv4-address	IP address field (for static IP and bridge settings) Type: IP address
mask-length	Subnet mask length Type: A string that contains numbers only
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
subnet-mask	Subnet mask Type: A subnet mask, or 255.255.255.255
type	Connection type Type: Press TAB to see available options
vlan-id	VLAN ID Type: A number with no fractional part (integer)

Syntax for L2TP

```
add internet-connection name <name> interface WAN type l2tp server
<server> password-hash <password-hash>
```

```
add internet-connection name <name> interface WAN type l2tp server
<server> password <password> username <username> { local-ipv4-address
<local-ipv4-address> wan-ipv4-address <wan-ipv4-address> wan-mask-
length <wan-mask-length>
```

```
add internet-connection name <name>interface WAN type l2tp server
<server> password <password> username <username> { local-ipv4-address
<local-ipv4-address> wan-ipv4-address <wan-ipv4-address> wan-subnet-
mask <wan-mask-length> default-gw <default-gw>} { is-unnumbered-pppoe
<is-unnumbered-pppoe>local-ipv4-address <local-ipv4-address>}
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
interface	Interface name Type: Press TAB to see available options
default-gw	WAN default gateway (in the advanced section of PPTP and l2TP) Type: IP address
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once Type: Boolean (true/false)
local-ipv4-address	Local tunnel IP address or Auto for automatic Type: An IP address, or 'auto'
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
password	Password for PPP connection settings Type: internetPassword
password-hash	The hash of the user password Type: passwordHash
server	Server IP address Type: IP address
type	Connection type Type: Press TAB to see available options

Parameter	Description
username	User name for PPP connection settings Type: A string that contains all printable characters but a single or double quote- like characters. Usually *<username>@<ISP>*
vlan-id	VLAN ID Type: A number with no fractional part (integer)
wan-ipv4-address	Wan IP address wrapper Type: An IP address, or 'auto'
wan-mask-length	WAN subnet mask length Type: A string that contains numbers only
wan-subnet-mask	WAN subnet mask (in the advanced section) Type: Subnet mask

Syntax for PPPoE

```
add internet-connection name < name> interface WAN type pppoe username
<username> password-hash <password-hash>
```

```
add internet-connection name <name> interface WAN type pppoe username
<username> password <password-hash> { is-unnumbered-pppoe <is-
unnumbered-pppoe> local-ipv4-address <local-ipv4-address> }
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
interface	Interface name Type: Press TAB to see available options
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once Type: Boolean (true/false)
local-ipv4-address	Local tunnel IP address or Auto for automatic Type: An IP address, or 'auto'
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters

Parameter	Description
password	Password for PPP connection settings Type: internetPassword
password-hash	The hash of the user password Type: passwordHash
type	Connection type Type: Press TAB to see available options
username	User name for PPP connection settings Type: A string that contains all printable characters but a single or double quote- like characters. Usually *<username>@<ISP>*
vlan-id	VLAN ID Type: A number with no fractional part (integer)

Syntax for PPTP

```
add internet-connection name <name> interface WAN type pptp server
<server> password-hash <password-hash>
```

```
command_synadd internet-connection name <name> interface WAN type
pptpserver <server> password <password > username <username> { { local-
ipv4-address <local-ipv4-address> wan-ipv4-address <wan-ipv4-address>
wan-mask-length <wan-mask-length>tax
```

```
add internet-connection name <name> interface WAN type pptp server
<server> password <password> username <username> { local-ipv4-address
<local-ipv4-address> wan-ipv4-address <wan-ipv4-address> wan-subnet-
mask <wan-subnet-mask> default-gw <default-gw>} { is-unnumbered-pppoe
<is-unnumbered-pppoe> local-ipv4-address <local-ipv4-address>}
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
interface	Interface name Type: Press TAB to see available options
default-gw	

Parameter	Description
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once Type: Boolean (true/false)
local-ipv4-address	Local tunnel IP address or Auto for automatic Type: An IP address, or 'auto'
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
password	Password for PPP connection settings Type: internetPassword
password-hash	The hash of the user password Type: passwordHash
server	Server IP address Type: IP address
type	Connection type Type: Press TAB to see available options
username	User name for PPP connection settings Type: A string that contains all printable characters but a single or double quote- like characters. Usually *<username>@<ISP>*
vlan-id	VLAN ID Type: A number with no fractional part (integer)
wan-ipv4-address	Wan IP address wrapper Type: An IP address, or 'auto'
wan-mask-length	WAN subnet mask length Type: A string that contains numbers only
wan-subnet-mask	WAN subnet mask (in the advanced section) Type: Subnet mask

ADSL

Syntax for EoA

```
add internet-connection name <name> interface ADSL type eoa
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
encapsulation	Encapsulation type for the ADSL connection Options: llc, vcmux
interface	Interface name Type: Press TAB to see available options
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
standard	The ADSL standard to use Options: multimode, t1413, glite, gdmt, adsl2, adsl2+
type	Connection type Type: Press TAB to see available options
vci	VCI value for the ADSL connection Type: A number between 0 and 65535
vpi	VPI value for the ADSL connection Type: A number between 0 and 255

Syntax for PPPoA

```
add internet-connection name <name> interface ADSL type pppoa username
<username> password-hash <password-hash>
```

```
add internet-connection name <name>interface ADSL type  pppoa username
<username> password <password>{ encapsulation <encapsulation> is-
unnumbered-pppoe <is-unnumbered-pppoe> local-ipv4-address <local-ipv4-
address> vci <vci> vpi <vpi> }
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)

Parameter	Description
encapsulation	Encapsulation type for the ADSL connection Options: llc, vcmux
interface	Interface name Type: Press TAB to see available options
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once Type: Boolean (true/false)
local-ipv4-address	Local tunnel IP address or Auto for automatic Type: An IP address, or 'auto'
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
password	Password for PPP connection settings Type: internetPassword
password-hash	The hash of the user password Type: passwordHash
type	Connection type Type: Press TAB to see available options
username	User name for PPP connection settings Type: A string that contains all printable characters but a single or double quote- like characters. Usually *<username>@<ISP>*
vci	VCI value for the ADSL connection Type: A number between 0 and 65535
vpi	VPI value for the ADSL connection Type: A number between 0 and 255

Syntax for PPPoE

```
add internet-connection name <name> interface ADSL type pppoe username
<username> password-hash <password-hash>
```

```
add internet-connection name <name> interface ADSLtype pppoe username
<username> password <password> { encapsulation <encapsulation> is-
unnumbered-pppoe <is-unnumbered-pppoe> local-ipv4-address <local-ipv4-
address> vci <vci> vpi <vpi>} { encapsulation <encapsulation> vci
<vci> vpi <vpi>} { conn-test-timeout <conn-test-timeout> standard
<standard>}
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
encapsulation	Encapsulation type for the ADSL connection Options: llc, vcmux
interface	Interface name Type: Press TAB to see available options
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once Type: Boolean (true/false)
local-ipv4-address	Local tunnel IP address or Auto for automatic Type: An IP address, or 'auto'
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
password	Password for PPP connection settings Type: internetPassword
password-hash	The hash of the user password Type: passwordHash
type	Connection type Type: Press TAB to see available options
username	User name for PPP connection settings Type: A string that contains all printable characters but a single or double quote- like characters. Usually *<username>@<ISP>*
vci	VCI value for the ADSL connection Type: A number between 0 and 65535

Parameter	Description
vpi	VPI value for the ADSL connection Type: A number between 0 and 255

DSL

Syntax for IPoE Dynamic

```
add internet-connection name <name> interface DSL type ipoe-dynamic
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
encapsulation	Encapsulation type for the ADSL connection Options: llc, vcmux
interface	Interface name Type: Press TAB to see available options
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
type	Connection type Type: Press TAB to see available options
vci	VCI value for the ADSL connection Type: A number between 0 and 65535
vlan-id	VLAN ID Type: A number with no fractional part (integer)
vpi	VPI value for the ADSL connection Type: A number between 0 and 255

Syntax for IPoE Static

```
add internet-connection name <name> interface DSL type ipoe-
staticdefault-gw <default-gw> ipv4-address <ipv4-address> mask-length
<mask-length>
```

```
add internet-connection name <name> interface DSL type ipoe-static
default-gw <default-gw> ipv4-address <ipv4-address> subnet-mask VALUE {
dns-primary <dns-primary> dns-secondary <dns-secondary> dns-tertiary
<dns-tertiary> }
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
default-gw	WAN default gateway (in the advanced section of PPTP and l2TP) Type: IP address
dns-primary	First DNS server IP address Type: IP address
dns-secondary	Second DNS server IP address Type: IP address
dns-tertiary	Third DNS server IP address Type: IP address
encapsulation	Encapsulation type for the ADSL connection Options: llc, vcmux
interface	Interface name Type: Press TAB to see available options
ipv4-address	IP address field (for static IP and bridge settings) Type: IP address
mask-length	Subnet mask length Type: A string that contains numbers only
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
subnet-mask	Subnet mask Type: A subnet mask, or 255.255.255.255
type	Connection type Type: Press TAB to see available options

Parameter	Description
vci	VCI value for the ADSL connection Type: A number between 0 and 65535
vlan-id	VLAN ID Type: A number with no fractional part (integer)
vpi	VPI value for the ADSL connection Type: A number between 0 and 255

Syntax for PPPoE

```
add internet-connection name <name> interface DSL type pppoe username <username> password-hash <password-hash>
```

```
add internet-connection name <name> interface DSL type pppoe username <username> password <password> { encapsulation <encapsulation> is-unnumbered-pppoe <is-unnumbered-pppoe> local-ipv4-address <local-ipv4-address> vci <vci> vpi <vpi> } { encapsulation <encapsulation> vci <vci> vpi <vpi> } { use-connection-as-vlan vlan-id <vlan-id> } { conn-test-timeout <conn-test-timeout>}
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
encapsulation	Encapsulation type for the ADSL connection Options: llc, vcmux
interface	Interface name Type: Press TAB to see available options
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once Type: Boolean (true/false)
local-ipv4-address	Local tunnel IP address or Auto for automatic Type: An IP address, or 'auto'
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters

Parameter	Description
password	Password for PPP connection settings Type: internetPassword
password-hash	The hash of the user password Type: passwordHash
type	Connection type Type: Press TAB to see available options
username	User name for PPP connection settings Type: A string that contains all printable characters but a single or double quote- like characters. Usually *<username>@<ISP>*
vci	VCI value for the ADSL connection Type: A number between 0 and 65535
vlan-id	VLAN ID Type: A number with no fractional part (integer)
vpi	VPI value for the ADSL connection Type: A number between 0 and 255

DMZ

Syntax for DHCP

```
add internet-connection name <name> interface DMZ type dhcp
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
interface	Interface name Type: Press TAB to see available options
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters

Parameter	Description
type	Connection type Type: Press TAB to see available options
vlan-id	VLAN ID Type: A number with no fractional part (integer)

Syntax for Static IP

```
add internet-connection name <name> interface DMZ type static default-gw <default-gw> ipv4-address <ipv4-address> mask-length <mask-length>
```

```
add internet-connection name <name> interface DMZ type static default-gw <default-gw> ipv4-address <ipv4-address> subnet-mask <subnet-mask> { dns-primary <dns-primary> dns-secondary <dns-secondary> dns-tertiary <dns-tertiary>} { use-connection-as-vlan vlan-id <vlan-id>} { conn-test-timeout <conn-test-timeout>}
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
interface	Interface name Type: Press TAB to see available options
default-gw	WAN default gateway (in the advanced section of PPTP and l2TP) Type: IP address
dns-primary	First DNS server IP address Type: IP address
dns-secondary	Second DNS server IP address Type: IP address
dns-tertiary	Third DNS server IP address Type: IP address
ipv4-address	IP address field (for static IP and bridge settings) Type: IP address
mask-length	Subnet mask length Type: A string that contains numbers only

Parameter	Description
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
subnet-mask	Subnet mask Type: A subnet mask, or 255.255.255.255
type	Connection type Type: Press TAB to see available options
vlan-id	VLAN ID Type: A number with no fractional part (integer)

Syntax for L2TP

```
add internet-connection name <name> interface DMZ type l2tp server <server> password-hash <password-hash>
```

```
add internet-connection name <name> interface DMZ type l2tp server <server> password <password> username <username> { local-ipv4-address <local-ipv4-address> wan-ipv4-address <wan-ipv4-address> wan-mask-length <wan-mask-length>
```

```
add internet-connection name <name> interface DMZ type l2tp server <server> password <password> username <username> { local-ipv4-address <local-ipv4-address> wan-ipv4-address <wan-ipv4-address> wan-subnet-mask <wan-mask-length> default-gw <default-gw>} { is-unnumbered-pppoe <is-unnumbered-pppoe> local-ipv4-address <local-ipv4-address>}
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
interface	Interface name Type: Press TAB to see available options
default-gw	WAN default gateway (in the advanced section of PPTP and l2TP) Type: IP address
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once Type: Boolean (true/false)

Parameter	Description
local-ipv4-address	Local tunnel IP address or Auto for automatic Type: An IP address, or 'auto'
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
password	Password for PPP connection settings Type: internetPassword
password-hash	The hash of the user password Type: passwordHash
server	Server IP address Type: IP address
type	Connection type Type: Press TAB to see available options
username	User name for PPP connection settings Type: A string that contains all printable characters but a single or double quote- like characters. Usually *<username>@<ISP>*
vlan-id	VLAN ID Type: A number with no fractional part (integer)
wan-ipv4-address	Wan IP address wrapper Type: An IP address, or 'auto'
wan-mask-length	WAN subnet mask length Type: A string that contains numbers only
wan-subnet-mask	WAN subnet mask (in the advanced section) Type: Subnet mask

Syntax for PPPoE

```
add internet-connection name <name> interface DMZ type pppoe username
<username> password-hash <password>
```

```
add internet-connection name <name> interface DMZ type  pppoe username
<username> password <password>{ is-unnumbered-pppoe <is-unnumbered-
pppoe> local-ipv4-address <local-ipv4-address>}
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
interface	Interface name Type: Press TAB to see available options
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once Type: Boolean (true/false)
local-ipv4-address	Local tunnel IP address or Auto for automatic Type: An IP address, or 'auto'
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
password	Password for PPP connection settings Type: internetPassword
password-hash	The hash of the user password Type: passwordHash
type	Connection type Type: Press TAB to see available options
username	User name for PPP connection settings Type: A string that contains all printable characters but a single or double quote- like characters. Usually *<username>@<ISP>*
vlan-id	VLAN ID Type: A number with no fractional part (integer)

Syntax for PPTP

```
add internet-connection name <name> interface DMZ type pptp server
<server> password-hash <password-hash>
```

```
add internet-connection name <name> interface DMZ type pptp server
<server> password <password> username <username> { { local-ipv4-address
<local-ipv4-address> wan-ipv4-address <wan-ipv4-address> wan-mask-
length <wan-mask-length>
```

```
add internet-connection name <name> interface DMZ type pptp server
<server> password <password> username <username> { local-ipv4-address
<local-ipv4-address> wan-ipv4-address <wan-ipv4-address> wan-subnet-
mask <wan-subnet-mask> default-gw <default-gw>} { is-unnumbered-pppoe
<is-unnumbered-pppoe> local-ipv4-address <local-ipv4-address>}
```

Parameters

Parameter	Description
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
interface	Interface name Type: Press TAB to see available options
default-gw	WAN default gateway (in the advanced section of PPTP and l2TP) Type: IP address
dns-primary	First DNS server IP address Type: IP address
dns-secondary	Second DNS server IP address Type: IP address
dns-tertiary	Third DNS server IP address Type: IP address
encapsulation	Encapsulation type for the ADSL connection Options: llc, vcmux
ipv4-address	IP address field (for static IP and bridge settings) Type: IP address
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once Type: Boolean (true/false)
isVlan	isVlan Type: Boolean (true/false)
local-ipv4-address	Local tunnel IP address or Auto for automatic Type: An IP address, or 'auto'
mask-length	Subnet mask length Type: A string that contains numbers only

Parameter	Description
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
password	Password for PPP connection settings Type: internetPassword
password-hash	The hash of the user password Type: passwordHash
server	Server IP address Type: IP address
standard	The ADSL standard to use Options: multimode, t1413, glite, gdmt, adsl2, adsl2+
subnet-mask	Subnet mask Type: A subnet mask, or 255.255.255.255
type	Connection type Type: Press TAB to see available options
username	User name for PPP connection settings Type: A string that contains all printable characters but a single or double quote- like characters. Usually *<username>@<ISP>*
vci	VCI value for the ADSL connection Type: A number between 0 and 65535
vlan-id	VLAN ID Type: A number with no fractional part (integer)
vpi	VPI value for the ADSL connection Type: A number between 0 and 255
wan-ipv4-address	Wan IP address wrapper Type: An IP address, or 'auto'
wan-mask-length	WAN subnet mask length Type: A string that contains numbers only
wan-subnet-mask	WAN subnet mask (in the advanced section) Type: Subnet mask

Example

```
add internet-connection name My connection interface WAN true vlan-id -
1000000 type static ipv4-address 192.168.1.1 subnet-mask 255.255.255.0
default-gw 192.168.1.1 dns-primary 192.168.1.1 dns-secondary
192.168.1.1 dns-tertiary 192.168.1.1 conn-test-timeout -1000000
```

add internet-connection (3G/4G modem)

Description

Adds a new internet connection using an external 3G/4G modem connected directly to the appliance (multiple internet connection can engage in High Availability/Load Sharing).

Syntax

USB:

```
add internet-connection name <name> typeanalog use-serial-portfalse number
<number> { username <username> password-hash <password-hash>}
```

```
add internet-connection name <name> typeanalog use-serial-portfalse number
<number> { username <username> password <password> }
```

```
add internet-connection name <name> typeanalog use-serial-porttrue number
<number> { username <username> password-hash <password-hash> }
```

```
add internet-connection name <name> typeanalog use-serial-porttrue number
<number> username <username> password <password> { flow-control <flow-
control> port-speed <port-speed>} { conn-test-timeout <conn-test-
timeout>}
```

```
add internet-connection name <name> typecellular number <number> { conn-
test-timeout <conn-test-timeout> } name <name>} { apn <apn> username
<username> password-hash <password-hash> }
```

```
add internet-connection name  <name> typecellular number <number> { conn-
test-timeout <conn-test-timeout> name <name>} { apn <apn> username
<username>password <password> }
```

Parameters

Parameter	Description
apn	APN (cellular modem settings) Type: A string that contains [a-z], [0-9], '-' and '.' characters
conn-test-timeout	Connection test timeout Type: A number with no fractional part (integer)
flow-control	Flow control (serial port settings) Options: rts-cts, xon-xoff
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
number	Dialed number of the cellular modem settings Type: A sequence of numbers and #,* characters

Parameter	Description
password	Password for PPP connection settings Type: internetPassword
password-hash	The hash of the user password Type: passwordHash
port-speed	Port speed (serial port settings) Options: 9600, 19200, 38400, 57600, 115200, 230400
type	Connection type Type: Press TAB to see available options
use-serial-port	Use serial port Type: Boolean (true/false)
username	User name for PPP connection settings Type: A string that contains all printable characters but a single or double quote- like characters. Usually *<username>@<ISP>*

Example

```
add internet-connection type analog use-serial-port true number 758996
username MyUsername@MyISP password internetPassword port-speed 9600
flow-control rts-cts conn-test-timeout 50 name My connection
```

delete internet-connection

Deletes an existing internet connection or internet connection related configuration.

delete internet-connection

Description

Deletes an existing internet connection by name.

Syntax

```
delete internet-connection <name>
```

Parameters

Parameter	Description
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters

Example

```
delete internet-connection My connection
```

deleter internet-connection

Description

Deletes an existing internet connection's ping servers, configured for connection health monitoring.

Syntax

```
delete internet-connection <name> probe-icmp-servers [ first ] [ second
] [ third ]
```

Parameters

Parameter	Description
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters

Example

```
delete internet-connection My connection probe-icmp-servers first
second third
```

delete internet-connections

Description

Deletes all existing internet connections.

Syntax

```
delete internet-connections
```

Parameters

Parameter	Description
n/a	

Example

```
delete internet-connections
```

set internet-connection

Configures internet connections settings.

set internet-connection

Description

Configures an existing internet connection.

Syntax

```
set internet-connection <name>[ auto-negotiation <auto-negotiation> ] [
link-speed <link-speed> ] [ mtu <mtu>] [ mac-addr <mac-addr> ]
```

Parameters

Parameter	Description
auto-negotiation	Disable auto negotiation and manually define negotiation link speed Options: on, off
link-speed	Link speed Options: 100/full, 100/half, 10/full, 10/half
mac-addr	Default mac address wrapper Type: A MAC address or 'default'
mtu	MTU size. Select 'default' for default value. Type: A string of alphanumeric characters without space between them
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters

Example

```
set internet-connection My connection auto-negotiation on link-speed
100/full mtu word mac-addr 00:1C:7F:21:05:BE
```

set internet-connection

Description

Configures advanced settings for an existing internet connection.

Syntax

```
set internet-connection <name> connect-on-demand <connect-on-demand>
```

Parameters

Parameter	Description
connect-on-demand	Holds the status of the connect on demand feature Type: Boolean (true/false)
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters

Example

```
set internet-connection My connection connect-on-demand true
```

set internet-connection

Description

Enable/Disable an existing internet connection.

Syntax

```
set internet-connection <name> { enable | disable }
```

Parameters

Parameter	Description
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
state	Connection enabled/disabled Type: Boolean (true/false)

Example

```
set internet-connection My connection true
```

set internet-connection

Description

Configures advanced settings for an existing internet connection. Download bandwidth details allow QoS blade to run on this internet connection in locally/SMP managed mode and when managed using an LSM profile.

Syntax

```
set internet-connection <name> qos-download { true [ bandwidth
<bandwidth> ]| false }
```

Parameters

Parameter	Description
bandwidth	ISP download bandwidth Type: A number with no fractional part (integer)
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
qos-download	Enable QoS (quality of service) restriction on inbound traffic (download) Type: Boolean (true/false)

Example

```
set internet-connection My connection qos-download true bandwidth 100
```

set internet-connection

Description

Configures advanced settings for an existing internet connection. Upload bandwidth details allow QoS blade to run on this internet connection in locally/SMP managed mode and when managed using an LSM profile.

Syntax

```
set internet-connection <name> qos-upload { true [ bandwidth
<bandwidth> ] | false }
```

Parameters

Parameter	Description
bandwidth	ISP upload bandwidth Type: A number with no fractional part (integer)
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
qos-upload	Enable QoS (quality of service) restriction on outbound traffic (upload) Type: Boolean (true/false)

Example

```
set internet-connection My connection qos-upload true bandwidth 5
```

set internet-connection

Description

Configure hide NAT behavior on an existing internet connection. It is possible to disable hide-NAT from a specific internet connection.

Syntax

```
set internet-connection <name> disable-nat <disable-nat>
```

Parameters

Parameter	Description
disable-nat	Disable NAT(Network Address Translation) for traffic going through this Internet connection Type: Boolean (true/false)
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters

Example

```
set internet-connection My connection disable-nat true
```

set internet-connection

Description

Configures multiple ISP settings for an existing internet connection.

Syntax

```
set internet-connection <name> ha-priority <ha-priority> load-
balancing-weight <load-balancing-weight>
```

Parameters

Parameter	Description
ha-priority	Priority of the connection in HA Type: A number with no fractional part (integer)
load-balancing-weight	Internet connection weight for load balancing configuration Type: A number with no fractional part (integer)
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters

Example

```
set internet-connection My connection ha-priority 2 load-balancing-
weight 15
```

set internet-connection

Description

Configures advanced settings for an existing internet connection. It is possible to remove a configured internet connection from being used as a default route, making it available for traffic through manual/dynamic routing rules.

Syntax

```
set internet-connection <name> route-traffic-through-default-gateway
<route-traffic-through-default-gateway>
```

Parameters

Parameter	Description
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
route-traffic-through- default-gateway	In order to route traffic through this connection you need to add specific routes through it Type: Boolean (true/false)

Example

```
set internet-connection My connection route-traffic-through-default-
gateway true
```

set internet-connection

Description

Configures settings for an existing internet connection.

Syntax

```
set internet-connection <name>type { dhcp | pptp username <username> {
password <password> | password-hash <password-hash> } [ local-ipv4-
address <local-ipv4-address> ] [ is-unnumbered-pppoe <is-unnumbered-
pppoe> ] server <server> [ local-ipv4-address <local-ipv4-address> ] [
wan-ipv4-address <wan-ipv4-address> { wan-subnet-mask <wan-subnet-mask>
| wan-mask-length <wan-mask-length> } default-gw <default-gw> ] |
static ipv4-address <ipv4-address> { subnet-mask <subnet-mask> | mask-
length <mask-length> } default-gw <default-gw> [ dns-primary <dns-
primary> ] [ dns-secondary <dns-secondary>] [ dns-tertiary <dns-
tertiary> ] | l2tp username <username> { password <password> |
password-hash <password-hash> } [ local-ipv4-address <local-ipv4-
address>] [ is-unnumbered-pppoe <is-unnumbered-pppoe> ] server <server>
[ local-ipv4-address <local-ipv4-address> ] [ wan-ipv4-address <wan-
ipv4-address> { wan-subnet-mask <wan-subnet-mask> | wan-mask-length
<wan-mask-length> } default-gw <default-gw> ] }
```

Parameters

Parameter	Description
default-gw	Default gateway Type: IP address
dns-primary	First DNS server IP address Type: IP address
dns-secondary	Second DNS server IP address Type: IP address
dns-tertiary	Third DNS server IP address Type: IP address
ipv4-address	IP address field (for static IP and bridge settings) Type: IP address
is-unnumbered-pppoe	Unnumbered PPoE lets you manage a range of IP addresses and dial only once. Type: Boolean (true/false)

Parameter	Description
local-ipv4-address	Local tunnel IP address or Auto for automatic Type: An IP address, or 'auto'
mask-length	Subnet mask length Type: A string that contains numbers only
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
password	Password for PPP connection settings Type: internetPassword
password-hash	The hash of the user password Type: passwordHash
server	Server IP address Type: IP address
subnet-mask	Subnet mask Type: A subnet mask, or 255.255.255.255
type	Connection type Type: Press TAB to see available options
username	User name for PPP connection settings Type: A string that contains all printable characters but a single or double quote- like characters. Usually *<username>@<ISP>*
wan-ipv4-address	Wan IP address wrapper Type: An IP address, or 'auto'
wan-mask-length	WAN subnet mask length Type: A string that contains numbers only
wan-subnet-mask	WAN subnet mask (in the advanced section) Type: Subnet mask

Example

```
set internet-connection My connection type dhcp
```

set internet-connection

Description

Configures advanced settings for an existing internet connection.

Syntax

```
set internet-connection <name> type { pppoa username <username> {
password <password> | password-hash <password-hash> } [ local-ipv4-
addres <local-ipv4-address> ] [ is-unnumbered-pppoe <is-unnumbered-
pppoe> ] [ vpi <vpi> ] [ vci <vci> ] [ encapsulation <encapsulation> ]
| eoa }
```

Parameters

Parameter	Description
encapsulation	Encapsulation type for the ADSL connection Options: llc, vcmux
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once. Type: Boolean (true/false)
local-ipv4-address	Local tunnel IP address or Auto for automatic Type: An IP address, or 'auto'
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
password	Password for PPP connection or cellular modem settings Type: internetPassword
password-hash	The hash of the user password. Type: passwordHash
type	Connection type Type: Press TAB to see available options
username	User name for PPP connection or cellular modem settings Type: A string that contains all printable characters but a single or double quotelike characters. Usually *<username>@<ISP>*
vci	VCI value for the ADSL connection Type: A number between 0 and 65535

Parameter	Description
vpi	VPI value for the ADSL connection Type: A number between 0 and 255

Example

```
set internet-connection My connection type pppoe username
MyUsername@MyISP password internetPassword local-ipv4-address auto is-
unnumbered-pppoe true vpi 42 vci 42 encapsulation llc
```

set internet-connection

Description

Configures advanced settings for an existing internet connection. This command is available only for hardware that contains a DSL port.

Syntax

```
set internet-connection <name> type { pppoa [ method <method> ] [ idle-time <idle-time> ] [ standard <standard> ] | eoa [ vpi <vpi> ] [ vci <vci> ] [ encapsulation <encapsulation> ] [ wan-ipv4-address <wan-ipv4-address> { wan-subnet-mask <wan-subnet-mask> | wan-mask-length <wan-mask-length> } default-gw <default-gw> ] [ standard <standard> ] }
```

Parameters

Parameter	Description
default-gw	WAN default gateway (in the advanced section of PPTP and l2TP) Type: IP address
encapsulation	Encapsulation for the ADSL connection Options: llc, vcmux
idle-time	Disconnect idle time Type: A number with no fractional part (integer)
method	Authentication method Options: auto, pap, chap
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
standard	The ADSL standard to use Options: multimode, t1413, glite, gdmt, adsl2, adsl2+
type	Connection type Type: Press TAB to see available options
vci	VCI value for the ADSL connection Type: A number between 0 and 65535
vpi	VPI value for the ADSL connection Type: A number between 0 and 255

Parameter	Description
wan-ipv4-address	Wan IP address wrapper Type: An IP address, or 'auto'
wan-mask-length	WAN subnet mask length Type: A string that contains numbers only
wan-subnet-mask	WAN subnet mask (in the advanced section) Type: Subnet mask

Example

```
set internet-connection My connection type pppoa method auto idle-time
-1000000 standard multimode
```

set internet-connection

Description

Configures advanced settings for an existing internet connection. This command is available only for hardware that contains a DSL port.

Syntax

```
set internet-connection <name> type { pppoe [ username <username> ] [ {
password <password> | password-hash <password-hash> } ] [ [ { use-
connection-as-vlan } vlan-id <vlan-id> ] ] [ local-ipv4-address <local-
ipv4-address> ] [ is-unnumbered-pppoe <is-unnumbered-pppoe> ] [ vpi
<vpi> ] [ vci <vci> ] [ encapsulation <encapsulation> ] [ method
<method> ] [ idle-time <idle-time> ] [ standard <standard> ] | ipoe-
dynamic [ { use-connection-as-vlan } vlan-id <vlan-id> ] [ vpi <vpi>] [
vci <vci> ] [ encapsulation <encapsulation> ] | ipoe-static ipv4-
address <ipv4-address> { subnet-mask <subnet-mask> | mask-length <mask-
length> } default-gw <default-gw>[ dns-primary <dns-primary>] [ dns-
secondary <dns-secondary> ] [ dns-tertiary <dns-tertiary> ] [ { use-
connection-as-vlan } vlan-id <vlan-id> ] [ vpi <vpi> ] [ vci <vci> ] [
encapsulation <encapsulation> ] }
```

Parameters

Parameter	Description
default-gw	Default gateway Type: IP address
dns-primary	First DNS server IP address Type: IP address
dns-secondary	Second DNS server IP address Type: IP address
dns-tertiary	Third DNS server IP address Type: IP address
encapsulation	Encapsulation type for the ADSL connection Options: llc, vcmux
idle-time	Disconnect idle time Type: A number with no fractional part (integer)
ipv4-address	IP address field (for static IP and bridge settings) Type: IP address

Parameter	Description
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once Type: Boolean (true/false)
isVlan	isVlan Type: Boolean (true/false)
local-ipv4-address	Local tunnel IP address or Auto for automatic Type: An IP address, or 'auto'
mask-length	Subnet mask length Type: A string that contains numbers only
method	Authentication method Options: auto, pap, chap
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
password	Password for PPP connection settings Type: internetPassword
password-hash	The hash of the user password Type: passwordHash
standard	The ADSL standard to use Options: multimode, t1413, glite, gdmt, adsl2, adsl2+
subnet-mask	Subnet mask Type: A subnet mask, or 255.255.255.255
type	Connection type Type: Press TAB to see available options
username	User name for PPP connection settings Type: A string that contains all printable characters but a single or double quotelike characters. Usually <username>@<ISP>
vci	VCI value for the ADSL connection Type: A number between 0 and 65535

Parameter	Description
vlan-id	VLAN ID Type: A number with no fractional part (integer)
vpi	VPI value for the ADSL connection Type: A number between 0 and 255

Example

```
set internet-connection My connection type pppoe username
MyUsername@MyISP password internetPassword true vlan-id -1000000 local-
ipv4-address auto is-unnumbered-pppoe true vpi 42 vci 42 encapsulation
llc method auto idle-time -1000000 standard multimode
```

set internet-connection

Description

Configures settings for an existing internet connection.

Syntax

```
set internet-connection <name>type { cellular number <number> [
username <username> { password <password> | password-hash <password-
hash> } ] [ apn <apn> ] }
```

Parameters

Parameter	Description
apn	APN (cellular modem settings) Type: A string that contains [a-z], [0-9], '-' and '.' characters
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
number	Dialed number of the cellular modem settings Type: A sequence of numbers and #,* characters
password	Password for PPP connection or cellular modem settings Type: internetPassword
password-hash	The hash of the user password Type: passwordHash
type	Connection type Type: Press TAB to see available options
username	User name for PPP connection or cellular modem settings Type: A string that contains all printable characters but a single or double quote- like characters. Usually *<username>@<ISP>*

Example

```
set internet-connection My connection type cellular number 758996
username MyUsername@MyISP password internetPassword apn my-apn
```

set internet-connection

Description

Configures health monitoring settings for an existing internet connection.

Syntax

```
set internet-connection <name> probe-next-hop <probe-next-hop> [ probe-servers <probe-servers> ][ probing-method <probing-method> ]
```

Parameters

Parameter	Description
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
probe-next-hop	Automatically detect loss of connectivity to the default gateway Type: Boolean (true/false)
probe-servers	Monitor connection state by sending probe packets to one or more servers on the Internet Type: Boolean (true/false)
probing-method	Connection probing method Options: icmp, dns

Example

```
set internet-connection My connection probe-next-hop true probe-servers
true probing-method icmp
```

set internet-connection

Description

Configures health monitoring settings for an existing internet connection.

Syntax

```
set internet-connection < name> { probe-icmp-servers } first <first> [
second <second> ] [ third <third> ]
```

Parameters

Parameter	Description
first	First IP address for the probing method (when using connection monitoring) Type: An IP address or host name
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters
probing-method	Connection probing method Options: icmp, dns
second	Second IP address for the probing method (when using connection monitoring) Type: An IP address or host name
third	Third IP address for the probing method (when using connection monitoring) Type: An IP address or host name

Example

```
set internet-connection My connection icmp first myHost.com second
myHost.com third myHost.com
```

show internet-connection

Shows configuration and details of defined internet connections.

show internet-connection

Description

Shows configuration and details of a defined internet connection.

Syntax

```
show internet-connection <name>
```

Parameters

Parameter	Description
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters

Example

```
show internet-connection My connection
```

show internet-connection

Description

Shows configured ping servers for health monitoring of defined internet connection.

Syntax

```
show internet-connection <name> icmp-servers
```

Parameters

Parameter	Description
name	Connection name Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_' and space characters

Example

```
show internet-connection My connection icmp-servers
```

show internet-connections

Description

Shows details and configuration of all internet connections.

Syntax

```
show internet-connections
```

Parameters

Parameter	Description
n/a	

Example

```
show internet-connections
```

show internet-connections table

Description

Shows details and configuration of all internet connections in a table.

Syntax

```
show internet-connections table
```

Parameters

Parameter	Description
n/a	

Example

```
show internet-connections table
```

internet mode

set internet mode

Description

Configures multiple ISP internet connections behavior. Determines whether traffic will be distributed automatically across the defined active Internet connections according to the configured load balancing weights or use the default High Availability behavior based on priorities of each internet connection.

Syntax

```
set internet mode { load-balancing | high-availability }
```

Parameters

Parameter	Description
lb-mode	The load balancing mode Options: on, off

Example

```
set internet mode on
```

show internet mode

Description

Shows multiple internet connections mode (High Availability or Load Sharing.

Syntax

```
show internet mode
```

Parameters

Parameter	Description
n/a	

Example

```
show internet mode
```

ip-fragments-params

set ip-fragments-params

Configures how the appliance handles IP fragments.

set ip-fragments-params

Description

Configures how the appliance handles IP fragments.

Syntax

```
set ip-fragments-params advanced-settings minsize <minsize>
```

Parameters

Parameter	Description
n/a	

Example

```
set ip-fragments-params advanced-settings minsize 150
```

set ip-fragments-params

Description

Configures how the appliance handles IP fragments.

Syntax

```
set ip-fragments-params advanced-settings config [ track <track> ] [
limit <limit> ] [ advanced-state <advanced-state> ] [ timeout <timeout>
] [ pkt-cap <pkt-cap> ]
```

Parameters

Parameter	Description
n/a	

Example

```
set ip-fragments-params advanced-settings config track none limit 150
advanced-state forbid timeout 15 pkt-cap true
```

show ip-fragments-params

Description

Shows configuration of IP fragments handling.

Syntax

```
show ip-fragments-params advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show ip-fragments-params advanced-settings
```

ipv6-state

set ipv6-state

Description

Enable the IPv6 mode of the appliance.

Syntax

```
set ipv6-state
```

Parameters

Parameter	Description
n/a	

Example

```
set ipv6-state
```

show ipv6-state

Description

Show if the IPv6 mode of the appliance is enabled or disabled.

Syntax

```
show ipv6-state
```

Parameters

Parameter	Description
n/a	

Example

```
show ipv6-state
```

license

fetch license

Description

Fetches a license from one of these locations:

- Local gateway - There is an option to specify the file name with the *<file_name>* parameter.
- User Center at Check Point
- USB device - There is an option to specify the file name with the *<file_name>* parameter.

Syntax

```
fetch license {local [file <file_name>]|usercenter|usb [file <file_
name>]
```

Parameters

Parameter	Description
`file_name`	Name of the file that contains the license

Return Value

0 on success, 1 on failure

Example

```
fetch license usb file LicenseFile.xml
```

Output

Success shows `OK`. Failure shows an appropriate error message.

show license

Description

Shows current license state.

Syntax

```
show license
```

Parameters

Parameter	Description
`n/a`	

Example

```
show license
```

Output

Current license state

local-group

add local-group

Description

Adds a new group for user objects.

Syntax

```
add local-group name <name> [ comments <comments> ] [ remote-access-on
<remote-access-on> ]
```

Parameters

Parameter	Description
comments	Comments Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
name	Local group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces
remote-access-on	Indicates if the users group have remote access permissions Type: Boolean (true/false)

Example

```
add local-group name myObject_17 comments "This is a comment." remote-
access-on true
```

delete local-group

Deletes an existing group object for user objects.

delete local-group

Description

Deletes an existing group object for user objects by group object name.

Syntax

```
delete local-group name <name>
```

Parameters

Parameter	Description
name	Local group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
delete local-group name myObject_17
```

delete local-group

Description

Deletes all existing group objects for user objects.

Syntax

```
delete local-group all
```

Parameters

Parameter	Description
n/a	

Example

```
delete local-group all
```

set local-group

Configures an existing user group object.

set local-group

Description

Configures an existing user group object.

Syntax

```
set local-group name <name> [ new-name <new-name> ] [ comments
<comments> ] [ remote-access-on <remote-access-on> ]
```

Parameters

Parameter	Description
comments	Comments Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
name	Local group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces
new-name	Local group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces
remote-access-on	Indicates if the users group have remote access permissions Type: Boolean (true/false)

Example

```
set local-group name myObject_17 new-name myObject_17 comments "This is
a comment." remote-access-on true
```

set local-group

Description

Adds a bookmark to be shown in the SNX landing page to an existing user group object. This is relevant only if users in this group have VPN remote access privileges.

Syntax

```
set local-group name <name> add bookmark label <bookmark label>
```

Parameters

Parameter	Description
bookmark label	Text for the bookmark in the SSL Network Extender portal
name	Local group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
set local-group name myObject_17 add bookmark label myLabel
```

set local-group

Description

Removes a bookmark from being shown in the SNX landing page to an existing user group object. This is relevant only if users in this group have VPN remote access privileges.

Syntax

```
set local-group name <name> remove bookmark label <bookmark label>
```

Parameters

Parameter	Description
bookmark label	Text for the bookmark in the SSL Network Extender portal
name	Local group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
set local-group name myObject_17 remove bookmark label myLabel
```

show local-group

Description

Shows the content of a user group object.

Syntax

```
show local-group name <name>
```

Parameters

Parameter	Description
name	Local group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
show local-group name myObject_17
```

show local-groups

Description

Shows the content of all user group objects.

Syntax

```
show local-groups
```

Parameters

Parameter	Description
n/a	

Example

```
show local-groups
```

set local-group users

Configures an existing user group object.

set local-group users

Description

Adds a user to an existing user group object.

Syntax

```
set local-group users name <name> add user-name <user-name>
```

Parameters

Parameter	Description
name	Local group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces
user-name	User's name in the local database

Example

```
set local-group users name myObject_17 add user-name admin
```

set local-group users

Description

Removes a user from an existing user group object.

Syntax

```
set local-group users name <name> remove user-name <user-name>
```

Parameters

Parameter	Description
name	Local group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces
user-name	User's name in the local database

Example

```
set local-group users name myObject_17 remove user-name admin
```

local-user

add local-user

Description

Adds a new locally defined user object and configure its VPN remote access permissions.

Syntax

```
add local-user name <name> { password-hash <password-hash> | password
<password> } [ comments <comments> ] [ remote-access-always-on <remote-
access-always-on> ] [ is-temp-user { true expiration-date <expiration-
date> [ expiration-time <expiration-time> ] | false } ]
```

Parameters

Parameter	Description
comments	Comments Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
expiration-date	Expiration date for a temporary user in format yyyy-mm-dd Type: A date format yyyy-mm-dd
expiration-time	Expiration time for a temporary user in format HH:MM Type: A time format hh:mm
is-temp-user	Indicates if the user entry is temporary Type: Boolean (true/false)
name	User's name in the local database Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces
password	User's password in the local database Type: A string that contains alphanumeric and special characters
password-hash	User's hashed password (used for importing database) Type: An encrypted password
remote-access-always-on	Always enable remote access permission for user Type: Boolean (true/false)

Example

```
add local-user name admin password-hash TZXPLs20bN0RA comments "This is
a comment." remote-access-always-on true is-temp-user true expiration-
date 2000-01-01 expiration-time 23:20
```

delete local-user

Deletes an existing locally defined user object.

delete local-user

Description

Deletes an existing locally defined user object by user name.

Syntax

```
delete local-user name <name>
```

Parameters

Parameter	Description
name	User's name in the local database Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces

Example

```
delete local-user name admin
```

delete local-user

Description

Deletes all existing locally defined user objects by user name.

Syntax

```
delete local-user all
```

Parameters

Parameter	Description
n/a	

Example

```
delete local-user all
```

set local-user

Configures an existing user object.

set local-user

Description

Configures an existing user object.

Syntax

```
set local-user name <name> [ new-name <new-name> ] [ { password-hash
<password-hash> | password <password> } ] [ comments < comments> ] [
remote-access-always-on <remote-access-always-on> ] [ is-temp-user {
true expiration-date <expiration-date> [ expiration-time <expiration-
time>] | false } ]
```

Parameters

Parameter	Description
comments	Comments Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
expiration-date	Expiration date for a temporary user in format yyyy-mm-dd Type: A date format yyyy-mm-dd
expiration-time	Expiration time for a temporary user in format HH:MM Type: A time format hh:mm
is-temp-user	Indicates if the user entry is temporary Type: Boolean (true/false)
name	User's name in the local database Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces
new-name	User's name in the local database Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces
password	User's password in the local database Type: A string that contains alphanumeric and special characters
password-hash	User's hashed password (used for importing database) Type: An encrypted password
remote-access-always-on	Always enable remote access permission for user Type: Boolean (true/false)

Example

```
set local-user name admin new-name admin password-hash TZXPLs20bN0RA
comments "This is a comment." remote-access-always-on true is-temp-user
true expiration-date 2000-01-01 expiration-time 23:20
```

set local-user

Description

Adds a bookmark to be shown in the SNX landing page to an existing user. This is relevant only if the user has VPN remote access privileges.

Syntax

```
set local-user name <name> add bookmark label <bookmark label>
```

Parameters

Parameter	Description
bookmark label	Text for the bookmark in the SSL Network Extender portal
name	User's name in the local database Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces

Example

```
set local-user name admin add bookmark label myLabel
```

set local-user

Description

Removes a bookmark from being shown in the SNX landing page to an existing user. This is relevant only if the user has VPN remote access privileges.

Syntax

```
set local-user name <name> remove bookmark label <bookmark label>
```

Parameters

Parameter	Description
bookmark label	Text for the bookmark in the SSL Network Extender portal
name	User's name in the local database Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces

Example

```
set local-user name admin remove bookmark label myLabel
```

show local-user

Description

Shows the configuration of a locally defined user.

Syntax

```
show local-user name <name>
```

Parameters

Parameter	Description
name	User's name in the local database Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces

Example

```
show local-user name admin
```

show local-users

Description

Shows all locally defined users.

Syntax

```
show local-users
```

Parameters

Parameter	Description
n/a	

Example

```
show local-users
```

local-users expired

delete local-users expired

Description

Deletes all expired locally defined user objects from the database.

Syntax

```
delete local-users expired
```

Parameters

Parameter	Description
n/a	

Example

```
delete local-users expired
```

show local-users expired

Description

Shows all expired locally defined users.

Syntax

```
show local-users expired
```

Parameters

Parameter	Description
n.a	

Example

```
show local-users expired
```

show logs

Description

Shows system and kernel logs.

Syntax

```
show logs {system|kernel}
```

Parameters

Parameter	Description
n/a	

Example

```
show logs kernel
```

log-servers-configuration

set log-servers-configuration

Description

Configures external log servers for a locally managed device.

Syntax

```
set log-servers-configuration mgmt-server-ip-addr <mgmt-server-ip-addr>
[ log-server-ip-addr < log-server-ip-addr> ] sic-name <sic-name>
```

```
one-time-password <one-time-password> [ external-log-server-enable
<external-log-server-enable> ]
```

Parameters

Parameter	Description
external-log-server- enable	Determine if an external log server is active Type: Boolean (true/false)
log-server-ip-addr	This IP address is used if the log server is not located on the Security Management Server. Type: IP address
mgmt-server-ip-addr	This IP address is used for establishing trusted communication between the Check Point Appliance and the log server. Type: IP address
one-time-password	SIC one time password Type: A string that contains alphanumeric and special characters
sic-name	Enter the SIC name of the log server object that was defined in SmartDashboard Type: A SIC name

Example

```
set log-servers-configuration mgmt-server-ip-addr 192.168.1.1 log-
server-ip-addr 192.168.1.1 sic-name QWEDFRGH4 one-time-password a(&7Ba
external-log-server-enable true
```

show log-servers-configuration

Description

Shows external log server configuration.

Syntax

```
show log-servers-configuration
```

Parameters

Parameter	Description
n/a	

Example

```
show log-servers-configuration
```

mac-filtering-list

add mac-filtering-list

Description

Add a MAC address to the list of addresses allowed to access LAN/DMZ networks.

Syntax

```
add mac-filtering-list mac <mac>
```

Parameters

Parameter	Description
mac	MAC address to allow Type: MAC address

Example

```
add mac-filtering-list mac 00:1C:7F:21:05:BE
```

delete mac-filtering-list

Description

Delete a MAC address from the list of addresses allowed to access LAN/DMZ networks.

Syntax

```
delete mac-filtering-list mac <mac>
```

Parameters

Parameter	Description
mac	MAC address to allow Type: MAC address

Example

```
delete mac-filtering-list mac 00:1C:7F:21:05:BE
```

show mac-filtering-list

Description

Show the MAC addresses that are allowed to access LAN/DMZ networks.

Syntax

```
show mac-filtering-list
```

Parameters

Parameter	Description
n/a	

Example

```
show mac-filtering-list
```

mac-filtering-settings

set mac-filtering settings

Configure the settings for MAC filtering.

set mac-filtering-settings

Description

Configure the settings for MAC filtering.

Syntax

```
set mac-filtering-settings state <state>
```

Parameters

Parameter	Description
state	MAC filtering state Options: on, off

Example

```
set mac-filtering-settings state on
```

set mac-filtering settings

Description

Configure the settings for MAC filtering.

Syntax

```
set mac-filtering-settings advanced-settings log-activation <log-
activation>
```

Parameters

Parameter	Description
n/a	

Example

```
set mac-filtering-settings advanced-settings log-activation on
```

set mac-filtering settings

Description

Configure the settings for MAC filtering.

Syntax

```
set mac-filtering-settings advanced-settings log-interval <log-
interval>
```

Parameters

Parameter	Description
n/a	

Example

```
set mac-filtering-settings advanced-settings log-interval -1000000
```

show mac-filtering-settings

Show the settings for MAC filtering.

show mac-filtering-settings

Description

Show the settings for MAC filtering.

Syntax

```
show mac-filtering-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show mac-filtering-settings
```

show mac-filtering-settings

Description

Show the advanced settings for MAC filtering.

Syntax

```
show mac-filtering-settings advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show mac-filtering-settings advanced-settings
```

set mobile-settings

Description

Configure settings for a mobile device. In this case, for when the pairing code expires.

Syntax

```
set mobile-settings advanced-settings pairing-code-expiration <pairing-code-expiration>
```

Parameters

Parameter	Description
n/a	

Example

```
set mobile-settings advanced-settings pairing-code-expiration -1000000
```

set mobile-settings

Description

Configure settings for a mobile device.

Syntax

```
set mobile-settings advanced-settings not-cloud-server <not-cloud-
server>
```

Parameters

Parameter	Description
n/a	

Example

```
set mobile-settings advanced-settings not-cloud-server urlv6
```

show mobile-settings

Description

Show configured advanced settings for a mobile device.

Syntax

```
show mobile-settings advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show mobile-settings advanced-settings
```

mobile-settings

These commands are relevant for mobile settings.

set mobile-settings

Description

Configure settings for a mobile device. In this case, for when the pairing code expires.

Syntax

```
set mobile-settings advanced-settings pairing-code-expiration <pairing-
code-expiration>
```

Parameters

Parameter	Description
pairing-code-expiration	Number of hours until the pairing code expires.

Example

```
set mobile-settings advanced-settings pairing-code-expiration 1
```

set mobile-settings

Description

Configure settings for a mobile device.

Syntax

```
set mobile-settings advanced-settings not-cloud-server <not-cloud-
server>
```

Parameters

Parameter	Description
not-cloud-server	Notification server URL - URL for the cloud service that pushes the notifications.

Example

```
set mobile-settings advanced-settings not-cloud-server urlv6
```

show mobile-settings

Description

Show configured advanced settings for a mobile device.

Syntax

```
show mobile-settings advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show mobile-settings advanced-settings
```

monitor-mode-network

add monitor-mode-network

Description

Configuring "Monitor mode" over interfaces requires a mechanism to determine which are the local networks within the real topology. One of the options is a manual configuration of this topology using this command.

Syntax

```
add monitor-mode-network ipv4-address <ipv4-address> subnet-mask
<subnet-mask>
```

Parameters

Parameter	Description
ipv4-address	Indicates a network IP address that will be recognized as Internal Type: IP address
subnet-mask	Network subnet mask Type: A subnet mask, or 255.255.255.255

Example

```
add monitor-mode-network ipv4-address 192.168.1.1 subnet-mask
255.255.255.0
```

delete monitor-mode-network

Description

Deletes manually configured IP addresses that determine the local networks in monitor mode when not working in automatic detection mode.

Syntax

```
delete monitor-mode-network ipv4-address <ipv4-address>
```

Parameters

Parameter	Description
ipv4-address	Indicates a network IP address that will be recognized as Internal Type: IP address

Example

```
delete monitor-mode-network ipv4-address 192.168.1.1
```

set monitor-mode-network

Description

Configures IP addresses of networks that are manually recognized as local in the non-automatic mode of monitor mode interface inspection.

Syntax

```
set monitor-mode-network ipv4-address <ipv4-address> [ ipv4-address
<ipv4-address> ] [ subnet-mask <subnet-mask> ]
```

Parameters

Parameter	Description
ipv4-address	Indicates a network IP address that will be recognized as Internal Type: IP address
subnet-mask	Network subnet mask Type: A subnet mask, or 255.255.255.255

Example

```
set monitor-mode-network ipv4-address 192.168.1.1 ipv4-address
192.168.1.1 subnet-mask 255.255.255.0
```

show monitor-mode-networks

Description

Shows manually defined local networks for monitor mode configuration.

Syntax

```
show monitor-mode-networks
```

Parameters

Parameter	Description
n/a	

Example

```
show monitor-mode-networks
```

monitor-mode-configuration

set monitor-mode-configuration

Description

Configures mode of work for monitor mode interface inspection. Determines if locally managed networks will be automatically detected or manually configured.

Syntax

```
set monitor-mode-configuration [ use-defined-networks <use-defined-
networks>]
```

Parameters

Parameter	Description
use-defined-networks	Indicates if user-defined internal networks are used for Monitor mode Type: Boolean (true/false)

Example

```
set monitor-mode-configuration use-defined-networks true
```

show monitor-mode-configuration

Description

Shows monitor mode configuration for interfaces.

Syntax

```
show monitor-mode-configuration
```

Parameters

Parameter	Description
n/a	

Example

```
show monitor-mode-configuration
```

message

set message

Description

Configures a banner message for the SSH administrator login

Syntax

```
set message <type> { on | off } [ line ] [ msgvalue <msgvalue> ]
```

Parameters

Parameter	Description
msgvalue	Indicates the banner messages text Type: virtual
status	Indicates if a banner message for SSH login will appear Type: Boolean (true/false)
type	Indicates the type of the message (only banner supported) Options: motd, banner, caption

Example

```
set message motd true line msgvalue "My Banner message"
```

show message

Shows banner message for the ssh login.

show message

Description

Shows banner message for the ssh login.

Syntax

```
show message <type>
```

Parameters

Parameter	Description
type	Indicates the type of the message (only banner supported) Options: motd, banner, caption

Example

```
show message motd
```

show memory usage

Description

Shows the amount of memory that is being used.

Syntax

```
show memory-usage
```

Parameters

Parameter	Description
n/a	

Example

```
show memory-usage
```

Output

Success shows used memory. Failure shows an appropriate error message.

nat

set nat

Configures general NAT policy settings.

set nat

Description

Configures if local networks will be hidden by default behind the external IP addresses of the gateway.

Syntax

```
set nat [ hide-internal-networks <hide-internal-networks> ]
```

Parameters

Parameter	Description
hide-internal-networks	Hide internal networks behind the Gateway's external IP address Type: Boolean (true/false)

Example

```
set nat hide-internal-networks true
```

set nat

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings nat-destination-client-side <nat-destination-
client-side>
```

Parameters

Parameter	Description
n/a	

Example

```
set nat advanced-settings nat-destination-client-side true
```

set nat

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings arp-proxy-merge <arp-proxy-merge>
```

Parameters

Parameter	Description
n/a	

Example

```
set nat advanced-settings arp-proxy-merge true
```

set nat

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings address-trans <address-trans>
```

Parameters

Parameter	Description
n/a	

Example

```
set nat advanced-settings address-trans true
```

set nat

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings nat-automatic-arp <nat-automatic-arp>
```

Parameters

Parameter	Description
n/a	

Example

```
set nat advanced-settings nat-automatic-arp true
```

set nat

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings nat-destination-client-side-manual
```

<nat-destination-client-side-manual>

Parameters

Parameter	Description
n/a	

Example

```
set nat advanced-settings nat-destination-client-side-manual true
```

set nat

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings nat-hash-size <nat-hash-size>
```

Parameters

Parameter	Description
n/a	

Example

```
set nat advanced-settings nat-hash-size 1024
```

set nat

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings nat-cache-num-entries <nat-cache-num-entries>
```

Parameters

Parameter	Description
n/a	

Example

```
set nat advanced-settings nat-cache-num-entries 100
```

set nat

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings nat-limit <nat-limit>
```

Parameters

Parameter	Description
n/a	

Example

```
set nat advanced-settings nat-limit 100
```

set nat

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings increase-hide-capacity <increase-hide-
capacity>
```

Parameters

Parameter	Description
n/a	

Example

```
set nat advanced-settings increase-hide-capacity true
```

set nat

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings nat-cache-expiration <nat-cache-expiration>
```

Parameters

Parameter	Description
n/a	

Example

```
set nat advanced-settings nat-cache-expiration 100
```

set nat

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings perform-cluster-hide-fold <perform-cluster-
hide-fold>
```

Parameters

Parameter	Description
n/a	

Example

```
set nat advanced-settings perform-cluster-hide-fold true
```

set nat

Description

Configures advanced IP-Pool NAT policy settings.

Syntax

```
set nat advanced-settings ip-pool-nat [ ip-pool-securemote <ip-pool-securemote> ] [ ip-pool-log <ip-pool-log> ] [ ip-pool-per-interface <ip-pool-per-interface> ] [ ip-pool-override-hide <ip-pool-override-hide> ] [ ip-pool-gw2Gw <ip-pool-gw2Gw> ] [ ip-pool-unused-return-interval <ip-pool-unused-return-interval> ] [ log-ip-pool-allocation <log-ip-pool-allocation> ] [ ip-pool-mode <ip-pool-mode> ] [ ip-pool-alloc-per-destination <ip-pool-alloc-per-destination> ]
```

Parameters

Parameter	Description
n/a	

Example

```
set nat advanced-settings ip-pool-nat ip-pool-securemote true ip-pool-log none ip-pool-per-interface true ip-pool-override-hide true ip-pool-gw2Gw true ip-pool-unused-return-interval 100 log-ip-pool-allocation none ip-pool-mode do-not-use-IP-pool-NAT ip-pool-alloc-per-destination true
```

show nat

Shows NAT policy.

show nat

Description

Shows NAT policy.

Syntax

```
show nat
```

Parameters

Parameter	Description
n/a	

Example

```
show nat
```

show nat

Description

Shows advanced settings for NAT policy.

Syntax

```
show nat advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show nat advanced-settings
```

nat-rule

add nat-rule

Description

Adds a new manual NAT (translation of source/destination/service) rule to the NAT Rule Base.

Syntax

```
add nat-rule [ original-source <original-source> ] [ original-
destination <original-destination> ] [ original-service <original-
service> ] [ translated-source <translated-source> ] [ translated-
destination <translated-destination> ] [ translated-service
<translated-service> ] [ comment <comment> ] [ hide-sources <hide-
sources> ] [ enable-arp-proxy <enable-arp-proxy> ] [ { position
<position> | position-above <position-above> | position-below
<position-below> } ] [ name <name> ]
```

Parameters

Parameter	Description
comment	Comment for manual NAT rule Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
enable-arp-proxy	The gateway will reply to ARP requests sent to the original destination's IP address (Does not apply to IP ranges/networks) Type: Boolean (true/false)
hide-sources	Hide multiple sources behind the translated source addresses Type: Boolean (true/false)
name	name Type: A string of alphanumeric characters without space between them
original-destination	Original destination of rule
original-service	Original service of rule
original-source	Original source of rule
position	The order of the rule in comparison to other manual rules Type: Decimal number
position-above	The order of the rule in comparison to other manual rules Type: Decimal number

Parameter	Description
position-below	The order of the rule in comparison to other manual rules Type: Decimal number
translated-destination	Translated destination of rule
translated-service	Translated service of rule
translated-source	Translated source of rule

Example

```
add nat-rule original-source TEXT original-destination TEXT original-
service TEXT translated-source TEXT translated-destination TEXT
translated-service TEXT comment "This is a comment." hide-sources true
enable-arp-proxy true position 2 name word
```

delete nat-rule

Description

Deletes a manually configured NAT rule by name.

Syntax

```
delete nat-rule name <name>
```

Parameters

Parameter	Description
name	name Type: A string of alphanumeric characters without space between them

Example

```
delete nat-rule name word
```

set nat-rule

Description

Configures an existing manual NAT rule by name.

Syntax

```
set nat-rule name <name> [ original-source <original-source> ] [
original-destination <original-destination> ] [ original-service
<original-service>] [ translated-source <translated-source> ] [
translated-destination <translated-destination> ] [ translated-service
<translated-service> ] [ comment <comment>] [ hide-sources <hide-
sources> ] [ enable-arp-proxy <enable-arp-proxy> ] [ { position
<position> | position-above <position-above> | position-below
<position-below> } ] [ name <name> ] [ disabled <disabled> ]
```

Parameters

Parameter	Description
comment	Comment for manual NAT rule Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
disabled	Indicates if rule is disabled Type: Boolean (true/false)
enable-arp-proxy	The gateway will reply to ARP requests sent to the original destination's IP address (Does not apply to IP ranges/networks) Type: Boolean (true/false)
hide-sources	Hide multiple sources behind the translated source addresses Type: Boolean (true/false)
name	name Type: A string of alphanumeric characters without space between them
original-destination	Original destination of rule
original-service	Original service of rule
original-source	Original source of rule

Parameter	Description
position	The order of the rule in comparison to other manual rules Type: Decimal number
position-above	The order of the rule in comparison to other manual rules Type: Decimal number
position-below	The order of the rule in comparison to other manual rules Type: Decimal number
translated-destination	Translated destination of rule
translated-service	Translated service of rule
translated-source	Translated source of rule

Example

```
set nat-rule name word original-source TEXT original-destination TEXT
original-service TEXT translated-source TEXT translated-destination
TEXT translated-service TEXT comment "This is a comment." hide-sources
true enable-arp-proxy true position 2 name word disabled true
```

show nat-rule

Description

Shows the name or position of a specific NAT rule. Includes auto-generated rules.

Syntax

```
show nat-rule name <name>
```

```
show nat-rule position <position>
```

Parameters

Parameter	Description
n/a	

Example

```
show nat-rule name word
```

show nat-rules

Description

Shows configuration of all manually and auto-generated NAT rules.

Syntax

```
show nat-rules
```

Parameters

Parameter	Description
n/a	

Example

```
show nat-rules position 2
```

show nat-manual-rules

Description

Shows configuration of manual NAT rules by name or position.

Syntax

```
show nat-manual-rules name <name>
```

```
show nat-manual-rules <position>
```

Parameters

Parameter	Description
<name>	Rule name
<position>	Rule position

Example

```
show nat-rule name word
```

nat-rule position

delete nat-rule position

Description

Deletes a manually configured NAT rule by position.

Syntax

```
delete nat-rule position <position>
```

Parameters

Parameter	Description
position	The order of the rule in comparison to other manual rules Type: Decimal number

Example

```
delete nat-rule position 2
```

set nat-rule position

Description

Configures an existing manual NAT rule by position

Syntax

```
set nat-rule position <position> [ original-source <original-source> ]
[ original-destination <original-destination>] [ original-service
<original-service>] [ translated-source <translated-source> ] [
translated-destination <translated-destination> ] [ translated-service
<translated-service> ] [ comment <comment> ] [ hide-sources <hide-
sources> ] [ enable-arp-proxy <enable-arp-proxy> ] [ { position
<position> | position-above <position-above> | position-below
<position-below> } ] [ name <name> ] [ disabled <disabled> ]
```

Parameters

Parameter	Description
comment	Comment for manual NAT rule Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . -: () @
disabled	Indicates if rule is disabled Type: Boolean (true/false)
enable-arp-proxy	The gateway will reply to ARP requests sent to the original destination's IP address (Does not apply to IP ranges/networks) Type: Boolean (true/false)
hide-sources	Hide multiple sources behind the translated source addresses Type: Boolean (true/false)
name	name Type: A string of alphanumeric characters without space between them
original-destination	Original destination of rule
original-service	Original service of rule
original-source	Original source of rule

Parameter	Description
position	The order of the rule in comparison to other manual rules Type: Decimal number
position-above	The order of the rule in comparison to other manual rules Type: Decimal number
position-below	The order of the rule in comparison to other manual rules Type: Decimal number
translated-destination	Translated destination of rule
translated-service	Translated service of rule
translated-source	Translated source of rule

Example

```
set nat-rule position 2 original-source TEXT original-destination TEXT
original-service TEXT translated-source TEXT translated-destination
TEXT translated-service TEXT comment "This is a comment." hide-sources
true enable-arp-proxy true position 2 name word disabled true
```

netflow collector

add netflow collector

Description

Adds a new Netflow collector object (you can configure up to three). A collector uses a network protocol developed by Cisco for collecting network traffic patterns and volume. The Netflow records will be exported to each defined collector.

Syntax

```
add netflow collector ip <ip> port <port> export-format <export-format>
[ srcaddr <srcaddr>] is-enabled <is-enabled>
```

Parameters

Parameter	Description
export-format	Export format Options: Netflow_V9, Netflow_V5
ip	IP address Type: IP address
is-enabled	Indicates if netflow is enabled Type: Boolean (true/false)
port	UDP port Type: Port number
srcaddr	Source IP address Type: IP address

Example

```
add netflow collector ip 192.168.1.1 port 8080 export-format Netflow_V9
srcaddr 192.168.1.1 is-enabled true
```

delete netflow collector

Description

Deletes an existing Netflow collector object by IP address and port.

Syntax

```
delete netflow collector ip <ip> port <port>
```

Parameters

Parameter	Description
ip	IP address Type: IP address
port	UDP port Type: Port number

Example

```
delete netflow collector ip 192.168.1.1 port 8080
```

set netflow collector

Description

Configures an existing network collector for Netflow protocol.

Syntax

```
set netflow collector for-ip <for-ip> for-port <for-port> [ ip <ip> ] [
port <port> ] [ export-format <export-format> ] [ srcaddr <srcaddr> ] [
is-enabled <is-enabled> ]
```

Parameters

Parameter	Description
export-format	Export format Options: Netflow_V9, Netflow_V5
for-ip	IP address Type: IP address
for-port	UDP port Type: Port number
ip	IP address Type: IP address
is-enabled	Indicates if netflow is enabled Type: Boolean (true/false)
port	UDP port Type: Port number
srcaddr	Source IP address Type:IP address

Example

```
set netflow collector for-ip 192.168.1.1 for-port 8080 ip 192.168.1.1
port 8080 export-format Netflow_V9 srcaddr 192.168.1.1 is-enabled true
```

show netflow collector

Description

Shows configuration of a specific NetFlow collector.

Syntax

```
show netflow collector ip <ip> port <port>
```

Parameters

Parameter	Description
ip	IP address Type: IP address
port	UDP port Type: Port number

Example

```
show netflow collector ip 192.168.1.1 port 8080
```

show netflow collectors

Description

Shows configuration of all NetFlow collectors.

Syntax

```
show netflow collectors
```

Parameters

Parameter	Description
n/a	

Example

```
show netflow collectors
```

network

add network

Description

Adds a new network address range object (a network and a subnet mask).

Syntax

```
add network name <name> network-ipv4-address <network-ipv4-address> {
subnet-mask <subnet-mask> | mask-length <mask-length> }
```

Parameters

Parameter	Description
mask-length	Mask length
name	Network Object name Type: String
network-ipv4-address	Network address
subnet-mask	IP mask used in the related network

Example

```
add network name TEXT network-ipv4-address 172.16.10.0 subnet-mask
255.255.255.0
```

delete network

Description

Deletes an existing network address range object (a network and a subnet mask) by object name.

Syntax

```
delete network <name>
```

Parameters

Parameter	Description
name	Network Object name Type: String

Example

```
delete network TEXT
```

set network

Description

Configures an existing network with subnet.

Syntax

```
set network <name> [ name <name> ] [ network-ipv4-address <network-ipv4-address> ] { [ subnet-mask <subnet-mask> ] | [ mask-length <mask-length> ] }
```

Parameters

Parameter	Description
mask-length	Mask length
name	Network Object name Type: String
network-ipv4-address	Network address
subnet-mask	IP mask used in the related network

Example

```
set network TEXT name TEXT network-ipv4-address 172.16.10.0 subnet-mask 255.255.255.0
```

show network

Description

Shows configuration of a specific IP address network object.

Syntax

```
show network <name>
```

Parameters

Parameter	Description
name	Network Object name Type: String

Example

```
show network TEXT
```

show networks

Description

Shows configuration of all IP address network objects.

Syntax

```
show networks
```

Parameters

Parameter	Description
n/a	

Example

```
show networks
```

show notifications-log

Description

Show the notification logs.

Syntax

```
show notifications-log
```

Parameters

Parameter	Description
n/a	

Example

```
show notifications-log
```

notifications-policy

These commands are relevant for notifications policy.

set notifications-policy

Description

Configure the policy for sending notifications to the user.

Syntax

```
set notifications-policy [ send-push-notifications <send-push-
notifications> ] [ send-detailed-push-notifications <send-detailed-
push-notifications> ]
```

```
set notifications-policy [send-cloud-notifications <send-cloud-
notification>]
```

Parameters

Parameter	Description
send-detailed-push-notifications	Notification previews may contain information about your network. Turning it off means that the security gateway removes this information from the push notification. Type: Boolean (true/false)
send-push-notifications	Indicates whether notifications are sent to mobile application Type: Boolean (true/false)
send-cloud-notifications	Enable sending cloud notifications. Type: Boolean (true/false)

Example

```
set notifications-policy send-push-notifications true send-detailed-
push-notifications true set notifications-policy send-cloud-
notifications true
```

set notifications-policy

Description

Configure the policy for sending notifications to the user.

Syntax

```
set notifications-policy advanced-settings limit-push-notifications
<limit-push-notifications>
```

Parameters

Parameter	Description
n/a	

Example

```
set notifications-policy advanced-settings limit-push-notifications -
1000000
```

set notifications-policy

Description

Configure the policy for sending notifications to the user.

Syntax

```
set notifications-policy advanced-settings send-push-notifications
<send-push-notifications>
```

Parameters

Parameter	Description
n/a	

Example

```
set notifications-policy advanced-settings send-push-notifications true
```

show notifications-policy

Description

Show the policy for sending notifications to the user.

Syntax

```
show notifications-policy
```

Parameters

Parameter	Description
n/a	

Example

```
show notifications-policy
```

show notifications-policy

Description

Show the policy for sending notifications to the user.

Syntax

```
show notifications-policy advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show notifications-policy advanced settings
```

ntp

set ntp

Configures NTP settings.

set ntp

Description

Configures NTP settings.

Syntax

```
set ntp [ local-time-zone <local-time-zone> ] [ auto-adjust-daylight-
saving <auto-adjust-daylight-saving> ]
```

Parameters

Parameter	Description
auto-adjust-daylight- saving	Auto daylight Options: on, off
local-time-zone	Region on earth that has a uniform standard time

Example

```
set ntp local-time-zone GMT-11:00(Midway-Island) auto-adjust-daylight-
saving on
```

set ntp

Description

Enables/Disables NTP functionality.

Syntax

```
set ntp active <active>
```

Parameters

Parameter	Description
active	Region on earth that has a uniform standard time Options: on, off

Example

```
set ntp active on
```

set ntp

Description

Configures NTP settings.

Syntax

```
set ntp interval <interval>
```

Parameters

Parameter	Description
interval	Time interval (minutes) to update date and time settings from the NTP server Type: A number with no fractional part (integer)

Example

```
set ntp interval 15
```

set ntp

Description

Configures NTP settings.

Syntax

```
set ntp auth { on secret-id <secret-id> secret <secret> | off }
```

Parameters

Parameter	Description
auth	Authentication with NTP servers flag Type: Press TAB to see available options
secret	Key string for authentication with the NTP servers Type: A string that contains alphanumeric and special characters
secret-id	Authentication key identifier Type: A number with no fractional part. Values are between 4,503,599,627,370,495 to 4,503,599,627,370,495

Example

```
set ntp auth on secret-id 455397 secret a(&7Ba
```

show ntp

Description

Shows NTP configuration.

Syntax

```
show ntp
```

Parameters

Parameter	Description
n/a	

Example

```
show ntp
```

show ntp active

Description

Shows NTP activation status.

Syntax

```
show ntp active
```

Parameters

Parameter	Description
n/a	

Example

```
show ntp active
```

ntp server

set ntp server

Configures NTP server settings.

set ntp server

Description

Configures primary NTP server's IP address.

Syntax

```
set ntp server primary <primary>
```

Parameters

Parameter	Description
primary	Primary NTP server Type: An IP address or host name

Example

```
set ntp server primary myHost.com
```

set ntp server

Description

Configures secondary NTP server's IP address.

Syntax

```
set ntp server secondary <secondary>
```

Parameters

Parameter	Description
secondary	Secondary NTP server Type: An IP address or host name

Example

```
set ntp server secondary myHost.com
```

show ntp servers

Description

Shows all defined NTP servers.

Syntax

```
show ntp servers
```

Parameters

Parameter	Description
n/a	

Example

```
show ntp servers
```

periodic backup

set periodic-backup

Description

Configures periodic backup to a remote FTP server.

Syntax

```
set periodic-backup [ mode <mode>] [ server-address <server-address> ]
[ server-username <server-username> ] [ server-password <server-
password> ] [ file-encryption { true [ encryption-password <encryption-
password>] | false } ] [ schedule { monthly [ day-of-month <day-of-
month> ] | weekly [ day-of-week <day-of-week> ] | daily } ] [ hour
<hour> ]
```

Parameters

Parameter	Description
day-of-month	Day of the month to backup Type: A number with no fractional part (integer)
day-of-week	Day of the week to backup Options: sunday, monday, tuesday, wednesday, thursday, friday, saturday
encryption-password	Encryption password Type: A string that contains alphanumeric and special characters
file-encryption	Choose whether to encrypt the backup data Type: Boolean (true/false)
hour	Scheduled backup hour. The backup will be performed during this hour Type: A number with no fractional part (integer)
mode	Is periodic backup enabled Type: Boolean (true/false)
schedule	Schedule the frequency of the periodic backup Type: Press TAB to see available options
server-address	Backup server name or IPv4 address (FTP) Type: backupUrl
server-password	Backup server password Type: A string that contains alphanumeric and special characters

Parameter	Description
server-username	Backup server username Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces

Example

```
set periodic-backup mode true server-address backupUrl server-username
admin server-password a(&7Ba file-encryption true encryption-password a
(&7Ba schedule monthly day-of-month 2 hour 2
```

show periodic-backup

Description

Shows periodic backup configuration.

Syntax

```
show periodic-backup
```

Parameters

Parameter	Description
n/a	

Example

```
show periodic-backup
```

set property

Description

Disables or enables first time configuration (from the USB autoplay configuration or the WebUI).

Syntax

```
set property {USB_auto_configuration {always|once|off} | first-time-
wizard {always|once}}
```

Parameters

Parameter	Description
n/a	

Example

- `set property USB_auto_configuration off`
- `set property first-time-wizard off`

privacy settings

set privacy-settings

Description

In Advanced Settings, select if the customer consents to sending diagnostic data to Check Point.

Syntax

```
set privacy-settings advanced-settings customer-consent <customer-
consent>
```

Parameters

Parameter	Description
customer-consent	Type: Boolean (true/false)

Example

```
set privacy-settings advanced-settings customer-consent true
```

show privacy-settings

Description

In Advanced Settings, show if the customer consents to sending diagnostic data.

Syntax

```
show privacy-settings advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show privacy-settings advanced-settings
```

Sample Output

```
customer-consent: true
```

proxy

delete proxy

Description

Deletes configured proxy settings for the appliance.

Syntax

```
delete proxy
```

Parameters

Parameter	Description
n/a	

Example

```
delete proxy
```

set proxy

Configures proxy settings for connecting with Check Point update and license servers.

set proxy

Description

Configures proxy settings for connecting with Check Point update and license servers, when the device is located behind a proxy server.

Syntax

```
set proxy server <server> port <port>
```

Parameters

Parameter	Description
port	The proxy port Type: Port number
server	The proxy Host name or IP address Type: An IP address or host name

Example

```
set proxy server myHost.com port 8080
```

set proxy

Description

Enable/Disable proxy configuration for the device.

Syntax

```
set proxy { enable | disable }
```

Parameters

Parameter	Description
use-proxy	A proxy server between the appliance and the Internet. This proxy server will be used when the appliance?s internal processes must reach a Check Point server. Type: Boolean (true/false)

Example

```
set proxy true
```

show proxy

Description

Shows proxy configuration.

Syntax

```
show proxy
```

Parameters

Parameter	Description
n/a	

Example

```
show proxy
```

qos

set qos

Configures QoS policy.

set qos

Description

Enables/Disables the QoS

Syntax

```
set qos mode <mode>
```

Parameters

Parameter	Description
mode	Indicates if QoS blade is enabled Type: Boolean (true/false)

Example

```
set qos mode true
```

set qos

Description

Configures the default QoS policy.

Syntax

```
set qos default-policy [ limit-bandwidth-consuming-applications { true
[ limit-upload-traffic <limit-upload-traffic>] [ upload-limit <upload-
limit> ] [ limit-download-traffic <limit-download-traffic> ] [
download-limit <download-limit> ] | false } ] [ guarantee-bandwidth-to-
configured-traffic <guarantee-bandwidth-to-configured-traffic> [
guarantee-bandwidth-percentage <guarantee-bandwidth-percentage> ] [
guarantee-bandwidth-traffic <guarantee-bandwidth-traffic> ] [
guarantee-bandwidth-on-services <guarantee-bandwidth-on-services> ] ] [
ensure-low-latency-for-delay-sensitive-services <ensure-low-latency-
for-delay-sensitive-services> ]
```

Parameters

Parameter	Description
n/a	

Example

```
set qos default-policy limit-bandwidth-consuming-applications true
limit-upload-traffic true upload-limit 5 limit-download-traffic true
download-limit 100 guarantee-bandwidth-to-configured-traffic on
guarantee-bandwidth-percentage 80 guarantee-bandwidth-traffic vpn
guarantee-bandwidth-on-services all ensure-low-latency-for-delay-
sensitive-services on
```

set qos

Description

Configures advanced QoS settings.

Syntax

```
set qos low-latency-traffic maximum-percentage-of-bandwidth
```

<maximum-percentage-of-bandwidth>

Parameters

Parameter	Description
n/a	

Example

```
set qos low-latency-traffic maximum-percentage-of-bandwidth 80
```

set qos

Description

Configures advanced QoS settings.

Syntax

```
set qos advanced-settings qos-logging <qos-logging>
```

Parameters

Parameter	Description
n/a	

Example

```
set qos advanced-settings qos-logging true
```

show qos

Shows the policy of the QoS blade.

show qos

Description

Shows the policy of the QoS blade.

Syntax

```
show qos
```

Parameters

Parameter	Description
n/a	

Example

```
show qos
```

show qos

Description

Shows advanced settings of the QoS blade.

Syntax

```
show qos advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show qos advanced-settings
```

qos delay-sensitive-service

set qos delay-sensitive-service

Configures a default used group of services that are delay sensitive.

set qos delay-sensitive-service

Description

Adds an existing service object to the default group of services that are delay sensitive.

Syntax

```
set qos delay-sensitive-service add service <service>
```

Parameters

Parameter	Description
service	Service name

Example

```
set qos delay-sensitive-service add service TEXT
```

set qos delay-sensitive-service

Description

Removes an existing service object from the default group of services that are delay sensitive.

Syntax

```
set qos delay-sensitive-service remove service <service>
```

Parameters

Parameter	Description
service	Service name

Example

```
set qos delay-sensitive-service remove service TEXT
```

show qos delay-sensitive-services

Description

Shows the group of services that are considered delay sensitive.

Syntax

```
show qos delay-sensitive-services
```

Parameters

Parameter	Description
n/a	

Example

```
show qos delay-sensitive-services
```

qos guarantee-bandwidth-selected-services

set qos guarantee-bandwidth-selected-services

Configures a default used group of services that will be guaranteed bandwidth according to QoS default policy.

set qos guarantee-bandwidth-selected-services

Description

Adds an existing service object to the default used group of services that will be guaranteed bandwidth according to QoS default policy.

Syntax

```
set qos guarantee-bandwidth-selected-services add service <service>
```

Parameters

Parameter	Description
service	Service name

Example

```
set qos guarantee-bandwidth-selected-services add service TEXT
```

set qos guarantee-bandwidth-selected-services

Description

Removes an existing service object from the default used group of services that will be guaranteed bandwidth according to QoS default policy.

Syntax

```
set qos guarantee-bandwidth-selected-services remove service <service>
```

Parameters

Parameter	Description
service	Service name

Example

```
set qos guarantee-bandwidth-selected-services remove service TEXT
```

show qos guarantee-bandwidth-selected-services

Description

Shows the group of services that can be guaranteed bandwidth in the QoS default policy.

Syntax

```
show qos guarantee-bandwidth-selected-services
```

Parameters

Parameter	Description
n/a	

Example

```
show qos guarantee-bandwidth-selected-services
```

qos-rule

add qos-rule

Description

Adds a new bandwidth/latency control rule to the QoS Rule Base.

Syntax

```
add qos-rule [ source <source> ] [ destination <destination> ] [
service <service> ] [ { [ low-latency-rule { normal [ limit-bandwidth
<limit-bandwidth> [ limit-percentage <limit-percentage> ] ] [
guarantee-bandwidth <guarantee-bandwidth> [ guarantee-percentage
<guarantee-percentage> ] ] | low } ] | [ limit-bandwidth <limit-
bandwidth> [ limit-percentage <limit-percentage> ] ] [ guarantee-
bandwidth <guarantee-bandwidth> [ guarantee-percentage <guarantee-
percentage> ] ] } ] [ weight <weight> ] [ log <log> ] [ comment
<comment> ] [ vpn <vpn> ] [ hours-range-enabled { true hours-range-from
<hours-range-from> hours-range-to <hours-range-to> | false } ] [
diffserv-mark { true diffserv-mark-val <diffserv-mark-val> | false } ]
[ name <name> ] [ { position <position> | position-above <position-
above> | position-below <position-below> } ]
```

Parameters

Parameter	Description
comment	Description of the rule Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
destination	Network object that is the target of the connection
diffserv-mark	DiffServ Mark is a way to mark connections so a third party will handle it. To use this option, your ISP or private WAN must support DiffServ Type: Boolean (true/false)
diffserv-mark-val	To mark packets that will be given priority on the public network according to their DSCP, select DiffServ Mark (1-63) and select a value. You can get the DSCP value from your ISP or private WAN administrator Type: A number with no fractional part (integer)
guarantee-bandwidth	If true, traffic guarantee is defined Type: Boolean (true/false)
guarantee-percentage	Traffic guarantee percentage Type: A number with no fractional part (integer)

Parameter	Description
hours-range-enabled	If true, time is configured Type: Boolean (true/false)
hours-range-from	Time in the format HH:MM Type: A time format hh:mm
hours-range-to	Time in the format HH:MM Type: A time format hh:mm
limit-bandwidth	If true, traffic limit is defined Type: Boolean (true/false)
limit-percentage	Traffic limit percentage Type: A number with no fractional part (integer)
log	Defines which logging method to use: None - do not log, Log - Create log Options: none, log
low-latency-rule	The latency of the rule (low or normal) Type: Press TAB to see available options
name	name Type: A string of alphanumeric characters without space between them
position	The order of the rule in comparison to other manual rules Type: Decimal number
position-above	The order of the rule in comparison to other manual rules Type: Decimal number
position-below	The order of the rule in comparison to other manual rules Type: Decimal number
service	The network service object that the rule should match to
source	Network object or user group that initiates the connection
vpn	Indicates if traffic is matched on encrypted traffic only or all traffic Type: Boolean (true/false)
weight	Traffic weight, relative to the weights defined for other rules Type: A number with no fractional part (integer)

Example

```
add qos-rule source TEXT destination TEXT service TEXT low-latency-rule
normal limit-bandwidth true limit-percentage 15 guarantee-bandwidth
true guarantee-percentage 30 weight 30 log none comment "This is a
comment." vpn true hours-range-enabled true hours-range-from 23:20
hours-range-to 23:20 diffserv-mark true diffserv-mark-val 5 name word
position 2
```

delete qos-rule

Deletes an existing bandwidth/latency control rule in the QoS Rule Base.

delete qos-rule

Description

Deletes an existing bandwidth/latency control rule in the QoS Rule Base by idx.

Syntax

```
delete qos-rule idx <idx>
```

Parameters

Parameter	Description
idx	The order of the rule in comparison to other manual rules Type: Decimal number

Example

```
delete qos-rule idx 3.141
```

delete qos-rule

Description

Deletes an existing bandwidth/latency control rule in the QoS Rule Base by name.

Syntax

```
delete qos-rule name <name>
```

Parameters

Parameter	Description
name	name Type: A string of alphanumeric characters without space between them

Example

```
delete qos-rule name word
```

set qos-rule

Configures an existing bandwidth/latency control rule within the QoS blade policy.

set qos-rule

Description

Configures an existing bandwidth/latency control rule within the QoS blade policy by idx.

Syntax

```
set qos-rule idx <idx> [ source <source> ] [ destination <destination>
] [ service <service> ] [ { [ low-latency-rule { normal [ limit-
bandwidth <limit-bandwidth> [ limit-percentage <limit-percentage> ] ] [
guarantee-bandwidth <guarantee-bandwidth> [ guarantee-percentage
<guarantee-percentage> ] ] | low } ] | [ limit-bandwidth <limit-
bandwidth> [ limit-percentage <limit-percentage> ] ] [ guarantee-
bandwidth <guarantee-bandwidth>[ guarantee-percentage <guarantee-
percentage> ] ] } ] [ weight <weight> ] [ log <log> ] [ comment
<comment> ] [ vpn <vpn> ] [ hours-range-enabled { true hours-range-from
<hours-range-from> hours-range-to <hours-range-to> | false } ] [
diffserv-mark { true diffserv-mark-val <diffserv-mark-val> | false } ]
[ name  <name> ] [ { position <position> | position-above <position-
above> | position-below <position-below> } ] [ disabled <disabled> ]
```

Parameters

Parameter	Description
comment	Description of the rule Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
destination	Network object that is the target of the connection
diffserv-mark	DiffServ Mark is a way to mark connections so a third party will handle it. To use this option, your ISP or private WAN must support DiffServ Type: Boolean (true/false)
diffserv-mark-val	To mark packets that will be given priority on the public network according to their DSCP, select DiffServ Mark (1-63) and select a value. You can get the DSCP value from your ISP or private WAN administrator Type: A number with no fractional part (integer)
disabled	Indicates if rule is disabled Type: Boolean (true/false)
guarantee-bandwidth	If true, traffic guarantee is defined Type: Boolean (true/false)

Parameter	Description
guarantee-percentage	Traffic guarantee percentage Type: A number with no fractional part (integer)
hours-range-enabled	If true, time is configured Type: Boolean (true/false)
hours-range-from	Time in the format HH:MM Type: A time format hh:mm
hours-range-to	Time in the format HH:MM Type: A time format hh:mm
idx	The order of the rule in comparison to other manual rules Type: Decimal number
limit-bandwidth	If true, traffic limit is defined Type: Boolean (true/false)
limit-percentage	Traffic limit percentage Type: A number with no fractional part (integer)
log	Defines which logging method to use: None - do not log, Log - Create log Options: none, log
low-latency-rule	The latency of the rule (low or normal) Type: Press TAB to see available options
name	name Type: A string of alphanumeric characters without space between them
position	The order of the rule in comparison to other manual rules Type: Decimal number
position-above	The order of the rule in comparison to other manual rules Type: Decimal number
position-below	The order of the rule in comparison to other manual rules Type: Decimal number
service	The network service object that the rule should match to
source	Network object or user group that initiates the connection

Parameter	Description
vpn	Indicates if traffic is matched on encrypted traffic only or all traffic Type: Boolean (true/false)
weight	Traffic weight, relative to the weights defined for other rules Type: A number with no fractional part (integer)

Example

```
set qos-rule idx 3.141 source TEXT destination TEXT service TEXT low-
latency-rule normal limit-bandwidth true limit-percentage 80 guarantee-
bandwidth true guarantee-percentage 80 weight 15 log none comment "This
is a comment." vpn true hours-range-enabled true hours-range-from 23:20
hours-range-to 23:20 diffserv-mark true diffserv-mark-val 5 name word
position 2 disabled true
```

set qos-rule

Description

Configures an existing bandwidth/latency control rule within the QoS blade policy by name.

Syntax

```
set qos-rule name <name> [ source <source> ] [ destination
<destination> ] [ service <service> ] [ { [ low-latency-rule { normal [
limit-bandwidth <limit-bandwidth> [ limit-percentage <limit-percentage>
] ] [ guarantee-bandwidth <guarantee-bandwidth> [ guarantee-percentage
<guarantee-percentage> ] ] | low } ] | [ limit-bandwidth <limit-
bandwidth> [ limit-percentage <limit-percentage> ] ] [ guarantee-
bandwidth <guarantee-bandwidth> [ guarantee-percentage <guarantee-
percentage> ] ] } ] [ weight <weight> ] [ log <log> ] [ comment
<comment> ] [ vpn <vpn> ] [ hours-range-enabled { true hours-range-from
<hours-range-from> hours-range-to <hours-range-to> | false } ] [
diffserv-mark { true diffserv-mark-val <diffserv-mark-val> | false } ]
[ name <name> ] [ { position <position>| position-above <position-
above> | position-below <position-below>} ] [ disabled <disabled> ]
```

Parameters

Parameter	Description
comment	Description of the rule Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
destination	Network object that is the target of the connection
diffserv-mark	DiffServ Mark is a way to mark connections so a third party will handle it. To use this option, your ISP or private WAN must support DiffServ Type: Boolean (true/false)
diffserv-mark-val	To mark packets that will be given priority on the public network according to their DSCP, select DiffServ Mark (1-63) and select a value. You can get the DSCP value from your ISP or private WAN administrator Type: A number with no fractional part (integer)
disabled	Indicates if rule is disabled Type: Boolean (true/false)
guarantee-bandwidth	If true, traffic guarantee is defined Type: Boolean (true/false)

Parameter	Description
guarantee-percentage	Traffic guarantee percentage Type: A number with no fractional part (integer)
hours-range-enabled	If true, time is configured Type: Boolean (true/false)
hours-range-from	Time in the format HH:MM Type: A time format hh:mm
hours-range-to	Time in the format HH:MM Type: A time format hh:mm
limit-bandwidth	If true, traffic limit is defined Type: Boolean (true/false)
limit-percentage	Traffic limit percentage Type: A number with no fractional part (integer)
log	Defines which logging method to use: None - do not log, Log - Create log Options: none, log
low-latency-rule	The latency of the rule (low or normal) Type: Press TAB to see available options
name	name Type: A string of alphanumeric characters without space between them
position	The order of the rule in comparison to other manual rules Type: Decimal number
position-above	The order of the rule in comparison to other manual rules Type: Decimal number
position-below	The order of the rule in comparison to other manual rules Type: Decimal number
service	The network service object that the rule should match to
source	Network object or user group that initiates the connection
vpn	Indicates if traffic is matched on encrypted traffic only or all traffic Type: Boolean (true/false)

Parameter	Description
weight	Traffic weight, relative to the weights defined for other rules Type: A number with no fractional part (integer)

Example

```
set qos-rule name word source TEXT destination TEXT service TEXT low-latency-rule normal limit-bandwidth true limit-percentage 80 guarantee-bandwidth true guarantee-percentage 80 weight 15 log none comment "This is a comment." vpn true hours-range-enabled true hours-range-from 23:20 hours-range-to 23:20 diffserv-mark true diffserv-mark-val 5 name word position 2 disabled true
```

show qos-rule

Shows configuration of QoS (bandwidth/latency control) rules.

show qos-rule

Description

Shows configuration of a QoS rule by ID.

Syntax

```
show qos-rule idx <idx>
```

Parameters

Parameter	Description
idx	The order of the rule in comparison to other manual rules Type: Decimal number
position	The order of the rule in comparison to other manual rules Type: Decimal number

Example

```
show qos-rule idx 3.141 position 2
```

show qos-rule

Description

Shows configuration of a QoS rule by name.

Syntax

```
show qos-rule name <name>
```

Parameters

Parameter	Description
name	name Type: A string of alphanumeric characters without space between them
position	The order of the rule in comparison to other manual rules Type: Decimal number

Example

```
show qos-rule name word position 2
```

show qos-rules

Description

Shows configuration of a QoS rule by position.

Syntax

```
show qos-rules position <position>
```

Parameters

Parameter	Description
position	The order of the generated rules in the QoS Rule Base Type: A number with no fractional part (integer)

Example

```
show qos-rules position 2
```

radius-server

delete radius-server

Description

Deletes an existing configured RADIUS server.

Syntax

```
delete radius-server priority <priority>
```

Parameters

Parameter	Description
priority	Priority of the choose tab, can be primary or secondary Type: A number with no fractional part (integer)

Example

```
delete radius-server priority 1
```

set radius-server

Description

Configures RADIUS servers.

Syntax

```
set radius-server priority <priority> [ ipv4-address <ipv4-address> ] [
udp-port <udp-port> ] [ shared-secret <shared-secret> ] [ timeout
<timeout>]
```

Parameters

Parameter	Description
ipv4-address	The IP address of the RADIUS server Type: IP address
priority	Priority of the choose tab, can be primary or secondary Type: A number with no fractional part (integer)
shared-secret	Pre-shared secret between the RADIUS server and the Appliance Type: A string that contains alphanumeric and special characters
timeout	A timeout value in seconds for communication with the RADIUS server Type: A number with no fractional part (integer)
udp-port	The port number through which the RADIUS server communicates with clients. The default is 1812 Type: A number with no fractional part (integer)

Example

```
set radius-server priority 2 ipv4-address 192.168.1.1 udp-port 1812
shared-secret a(&7Ba timeout 15
```

show radius-server

Description

Shows the configuration of a RADIUS server.

Syntax

```
show radius-server priority <priority>
```

Parameters

Parameter	Description
priority	Priority of the choose tab, can be primary or secondary Type: A number with no fractional part (integer)

Example

```
show radius-server priority 1
```

show radius-servers

Description

Shows the configuration of all RADIUS servers.

Syntax

```
show radius-servers
```

Parameters

Parameter	Description
n/a	

Example

```
show radius-servers
```

reach-my-device

set reach-my-device

Configures the "Reach my device" service, which enables connecting to the device's management portal even when the device is behind NAT.

set reach-my-device

Description

Configures the "Reach my device" service, which enables connecting to the device's management portal even when the device is behind NAT.

Syntax

```
set reach-my-device [ mode <mode> ] [ host-name <host-name> ] [
existing-host-name { true validation-token <validation-token> | false }
]
```

Parameters

Parameter	Description
existing-host-name	Register with an existing host name Type: Boolean (true/false)
host-name	Gateway Host name (DNS Prefix) Type: A string of alphanumeric characters without space between them
mode	Reach my device mode (on/off) Type: Boolean (true/false)
validation-token	Gateway validation token Type: A string of alphanumeric characters without space between them

Example

```
set reach-my-device mode true host-name word existing-host-name true
validation-token word
```

set reach-my-device

Description

Configures advanced settings of the "Reach my device" service, which enables connecting to the device's management portal even when the device is behind NAT.

Syntax

```
set reach-my-device advanced-settings ignore-ssl-cert <ignore-ssl-cert>
```

Parameters

Parameter	Description
n/a	

Example

```
set reach-my-device advanced-settings ignore-ssl-cert true
```

set reach-my-device

Description

Configures advanced settings of the "Reach my device" service, which enables connecting to the device's management portal even when the device is behind NAT.

Syntax

```
set reach-my-device advanced-settings reach-my-device-server-addr
```

<reach-my-device-server-addr>

Parameters

Parameter	Description
n/a	

Example

```
set reach-my-device advanced-settings reach-my-device-server-addr
http://www.checkpoint.com/
```

show reach-my-device

Shows the configuration of "Reach My Device" cloud service.

show reach-my-device

Description

Shows the configuration of "Reach My Device" cloud service.

Syntax

```
show reach-my-device
```

Parameters

Parameter	Description
n/a	

Example

```
show reach-my-device
```

show reach-my-device

Description

Shows advanced settings of "Reach My Device" cloud service.

Syntax

```
show reach-my-device advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show reach-my-device advanced-settings
```

set remote-access users

Description

Configures VPN remote access privileges to users defined in configured RADIUS servers.

Syntax

```
set remote-access users radius-auth { true [ use-radius-groups { true
radius-groups <radius-groups> | false } ] | false }
```

Parameters

Parameter	Description
radius-auth	Remote users RADIUS authentication Type: Boolean (true/false)
radius-groups	RADIUS groups for authentication. Example: RADIUS-group1, RADIUS-class2 Type: A string that contains [A-Z], [0-9], '-', '@', '.', '_', ',' and space characters
use-radius-groups	Use RADIUS groups for authentication Type: Boolean (true/false)

Example

```
set remote-access users radius-auth true use-radius-groups true radius-
groups My group
```

show remote-access users radius-auth

Description

Shows RADIUS-based users VPN remote access configuration.

Syntax

```
show remote-access users radius-auth
```

Parameters

Parameter	Description
n/a	

Example

```
show remote-access users radius-auth
```

reboot

Description

Reboots the system.

Syntax

```
reboot
```

Parameters

Parameter	Description
n/a	

Example

```
reboot
```

restore settings

Description

Restores the appliance settings from a backup file. The backup file can be located on a USB device or on a TFTP server.

Syntax

```
restore settings from {usb|tftp server <serverIP>} filename <file_name>
```

Parameters

Parameter	Description
file_name	Name of the backup file.
serverIP	IPv4 address of the TFTP server.

Example

```
restore settings from tftp server 1.1.1.1 filename sg80
```

Comments

The appliance automatically reboots after the settings are restored.

show restore settings log

Description

Shows the log file of previous restore settings to default operations. You can display these restore settings log files:

- `restore-settings-log`- Log file for restoring saved settings.
- `restore-default-settings-log` - Log file for restoring the default settings.

Syntax

```
show {restore-settings-log|restore-default-settings-log}
```

Parameters

Parameter	Description
`n/a`	

Example

```
show restore-settings-log
```

Output

Success shows the `restore settings` log file. Failure shows an appropriate error message.

show revert log

Description

Shows the log file of previous revert operations.

Syntax

```
show revert-log
```

Parameters

Parameter	Description
`n/a`	

Example

```
show revert-log
```

Output

Success shows the revert log file. Failure shows an appropriate error message.

revert to factory defaults

Description

Revert the appliance to the original factory defaults. This command deletes all data and software images from the appliance.

Syntax

```
revert to factory-defaults
```

Parameters

Parameter	Description
n/a	

Example

```
revert to factory-defaults
```

Output

Success shows a warning message. Enter `yes`to continue.

Failure shows an appropriate error message.

revert to saved image

Description

Reverts the appliance to the previous software image.

Syntax

```
revert to previous-image
```

Parameters

Parameter	Description
n/a	

Example

```
revert to previous-image
```

Output

Success shows `OK`. Failure shows an appropriate error message.

report-settings

set report-settings

Configure local reports settings.

set report-settings

Description

Configure advanced local reports settings.

Syntax

```
set report-settings advanced-settings centrally-max-period
```

<centrally-max-period>

Parameters

Parameter	Description
n/a	

Example

```
set report-settings advanced-settings centrally-max-period report-
period-hour
```

set report-settings

Description

Configure advanced local reports settings.

Syntax

```
set report-settings advanced-settings locally-max-period
```

<locally-max-period>

Parameters

Parameter	Description
n/a	

Example

```
set report-settings advanced-settings locally-max-period report-period-
hour
```

show report-settings

Description

Shows report scheduling and creation configuration.

Syntax

```
show report-settings advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show report-settings advanced-settings
```

show rule hits

Description

Shows the top firewall policy rule hits.

Syntax

```
show rule-hits [top <rule>]
```

Parameters

Parameter	Description
`rule`	Number of rules in the security policy that are displayed. Minimum value i 1 .

Return Value

0
on success,

1
on failure

Example

```
show rule-hits top 3
```

Output

Success shows number of hits per rule. Failure shows an appropriate error message.

show saved image

Description

Shows information about the saved backup image.

Syntax

```
show saved-image
```

Parameters

Parameter	Description
`n/a`	

Example

```
show saved-image
```

Output

Success shows information about the image. Failure shows an appropriate error message.

update security-blades

Description

Manually update Software Blades.

Syntax

```
update security-blades [ all ]
```

Parameters

Parameter	Description
n/a	

Example

```
update security-blades all
```

security-management

connect security-management

Description

Configure first connection to the Security Management Server.

Syntax

```
connect security-management mgmt-addr <mgmt-addr> use-one-time-password
<use-one-time-password> local-override-mgmt-addr { true send-logs-to {
local-override-log-server-addr addr <addr> | local-override-mgmt-addr }
| false }
```

Parameters

Parameter	Description
addr	The logs are sent to this address Type: An IP address or host name
local-override-mgmt-addr	Indicates if the management address used in the next manual fetch command will be saved and continuously used instead of the address downloaded in the policy Type: Boolean (true/false)
mgmt-addr	The IP address or hostname of the Security Management Server Type: An IP address or host name
send-logs-to	Indicates from where the address of the log server is taken Type: Press TAB to see available options
use-one-time-password	Indicates whether to connect to the Security Management Server using a one time password Type: Boolean (true/false)

Example

```
connect security-management mgmt-addr myHost.com use-one-time-password
true local-override-mgmt-addr true send-logs-to local-override-log-
server-addr addr myHost.com
```

set security-management

Configures settings to connect to a remote Security Management Server and log server.

set security-management

Description

Configures a local override to the IP addresses of the Security Management Server and log server. This is relevant when centrally managed.

Syntax

```
set security-management local-override-mgmt-addr { true mgmt-address
<mgmt-address> send-logs-to { local-override-log-server-addr addr
<addr> | local-override-mgmt-addr } | false }
```

Parameters

Parameter	Description
addr	The logs are sent to this address Type: An IP address or host name
local-override-mgmt- addr	Indicates if the management address used in the next manual fetch command will be saved and continuously used instead of the address downloaded in the policy Type: Boolean (true/false)
mgmt-address	IP address or hostname of the Security Management Server Type: An IP address or host name
send-logs-to	Indicates from where the address of the log server is taken Type: Press TAB to see available options

Example

```
set security-management local-override-mgmt-addr true mgmt-address
myHost.com send-logs-to local-override-log-server-addr addr myHost.com
```

set security-management

Description

Configures if the device is managed centrally or locally. In centrally managed appliances only the networking configurations are available and the security policy comes from the remote Security Management Server.

Syntax

```
set security-management mode <mode>
```

Parameters

Parameter	Description
mode	Indicates whether the appliance is managed locally or centrally using a Check Point Security Management Server. Options: locally-managed, centrally-managed

Example

```
set security-management mode locally-managed
```

show security-management

Description

Shows settings of the Security Management Server.

Syntax

```
show security-management
```

Parameters

Parameter	Description
n/a	

Example

```
show security-management
```

serial-port

set serial-port

Configures the physical serial port settings.

set serial-port

Description

Configures the physical serial port data flow settings.

Syntax

```
set serial-port [ port-speed <port-speed> ] [ flow-control <flow-
control> ] [ disabled <disabled> ] [ mode <mode> ]
```

Parameters

Parameter	Description
disabled	Indicates if the serial port is disabled
flow-control	Indicates the method of data flow control to and from the serial port
mode	Indicates if the serial port is used to connect to the appliance's console, a remote telnet server or allow a remote telnet connection to the device connected to the serial port.
port-speed	Indicates the port speed (Baud Rate) of the serial connection

Example

```
set serial-port port-speed 9600 flow-control rts-cts disabled on mode
console
```

set serial-port

Description

Configures the physical serial port as a relay to which incoming TELNET traffic on a configured port will be redirected.

Syntax

```
set serial-port passive-mode [ tcp-port <tcp-port> ] [ allow-implicitly
<allow-implicitly>]
```

Parameters

Parameter	Description
n/a	

Example

```
set serial-port passive-mode tcp-port 8080 allow-implicitly true
```

set serial-port

Description

Configures the physical serial port as a relay to outgoing connection to a remote TELNET server.

Syntax

```
set serial-port active-mode [ tcp-port <tcp-port> ] [ primary-server-
address
```

<primary-server-address>] [secondary-server-address *<secondary-server-address>*

```
]
```

Parameters

Parameter	Description
n/a	

Example

```
set serial-port active-mode tcp-port 8080 primary-server-address
myHost.com secondary-server-address myHost.com
```

show serial-port

Description

Shows configuration for the serial port.

Syntax

```
show serial-port
```

Parameters

Parameter	Description
n/a	

Example

```
show serial-port
```

server

add server

Description

Adds a new server object. Server object are a way to define a network host object with its access and NAT configuration, instead of creating manual rules for it.

Syntax

```
add server name <name> ipv4-address <ipv4-address> [ dhcp-exclude-ip-
addr { on [ dhcp-reserve-ip-addr-to-mac { on mac-addr <mac-addr> | off
} ] | off } ] [ comments <comments> ] [ dns-resolving <dns-resolving> ]
type { web-server | ftp-server | citrix-server | pptp-server | mail-
server | dns-server | custom-server [ tcpProtocol <tcpProtocol> [ tcp-
ports <tcp-ports> ] udpProtocol <udpProtocol> [ udp-ports <udp-ports> ]
] }
```

Parameters

Parameter	Description
comments	Comments Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
dhcp-exclude-ip-addr	Indicates if the internal DHCP service will not distribute the configured IP address of this server/network object to anyone Type: Press TAB to see available options
dhcp-reserve-ip-addr-to-mac	Indicates if the internal DHCP service will distribute the configured IP address only to this server/network object according to its MAC address Type: Press TAB to see available options
dns-resolving	Indicates if the name of the server/network object will be used as a hostname for internal DNS service Type: Boolean (true/false)
ipv4-address	The beginning of the IP range
mac-addr	MAC address of the server Type: MAC address
name	Server object name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Parameter	Description
tcp-ports	TCP ports for server of type 'other' Type: Port range
tcpProtocol	tcpProtocol Type: Boolean (true/false)
udp-ports	UDP ports for server of type 'other' Type: Port range
udpProtocol	udpProtocol Type: Boolean (true/false)

Example

```
add server name myObject_17 ipv4-address 192.168.1.1 dhcp-exclude-ip-
addr on dhcp-reserve-ip-addr-to-mac on mac-addr 00:1C:7F:21:05:BE
comments "This is a comment." dns-resolving true type web-server
```

delete server

Description

Deletes an existing server object.

Syntax

```
delete server <name>
```

Parameters

Parameter	Description
name	Server object name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
delete server myObject_17
```

show server

Description

Shows configuration of an existing server object.

Syntax

```
show server <name>
```

Parameters

Parameter	Description
name	Server object name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
show server myObject_17
```

show servers

Description

Shows the configuration of all server objects.

Syntax

```
show servers
```

Parameters

Parameter	Description
n/a	

Example

```
show servers
```

service-details

set device-details

~~

Description

Configures the device's details.

Syntax

```
set device-details [ hostname <hostname> ] [ country <country> ]
```

Parameters

Parameter	Description
country	The country where you are located. The country configured for the WLAN Options: country
hostname	The appliance name used to identify the gateway. Type: A string that contains [A-Z], [0-9] and '-' characters

Example

```
set device-details hostname My-appliance country albania
```

show device-details

Description

Shows configuration of basic device details.

Syntax

```
show device-details
```

Parameters

Parameter	Description
n/a	

Example

```
show device-details
```

service-group

add service-group

Description

Adds a new group for service objects.

Syntax

```
add service-group name <name> [ comments <comments> ] [ member <member>
]
```

Parameters

Parameter	Description
comments	Comments and explanation about the Service Group Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
member	An association field for the contained services
name	Service Group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
add service-group name myObject_17 comments "This is a comment." member
TEXT
```

delete service-group

Description

Deletes an existing group object for service objects by object name.

Syntax

```
delete service-group <name>
```

Parameters

Parameter	Description
name	Service Group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
delete service-group myObject_17
```

set service-group

Configures an existing service objects group.

set service-group

Description

Configures an existing service objects group.

Syntax

```
set service-group <name> [ new-name <new-name> ] [ comments <comments>
]
```

Parameters

Parameter	Description
comments	Comments and explanation about the Service Group Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
name	Service Group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces
new-name	Service Group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
set service-group myObject_17 new-name myObject_17 comments "This is a
comment."
```

set service-group

Description

Removes all service objects from an existing service objects group.

Syntax

```
set service-group <name> remove-all members
```

Parameters

Parameter	Description
name	Service Group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
set service-group myObject_17 remove-all members
```

set service-group

Description

Adds an existing service object to an existing service objects group.

Syntax

```
set service-group <name> add member <member>
```

Parameters

Parameter	Description
member	Service name
name	Service Group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
set service-group myObject_17 add member TEXT
```

set service-group

Description

Removes an existing service object from an existing service objects group.

Syntax

```
set service-group <name> remove member <member>
```

Parameters

Parameter	Description
member	Service name
name	Service Group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
set service-group myObject_17 remove member TEXT
```

show service-group

Description

Shows the content of a service object group.

Syntax

```
show service-group <name>
```

Parameters

Parameter	Description
name	Service Group name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
show service-group myObject_17
```

show service-groups

Description

Shows the content of all service object groups.

Syntax

```
show service-groups
```

Parameters

Parameter	Description
n/a	

Example

```
show service-groups
```

service-icmp

add service-icmp

Description

Adds a new ICMP-type service object.

Syntax

```
add service-icmp name <name> icmp-code <icmp-code> icmp-type <icmp-type> [ comments <comments>]
```

Parameters

Parameter	Description
comments	Comments and explanation about the service Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
icmp-code	ICMP code Type: A number with no fractional part (integer)
icmp-type	ICMP message type Type: A number with no fractional part (integer)
name	Service name Type: String

Example

```
add service-icmp name TEXT icmp-code 2 icmp-type 5 comments "This is a comment."
```

delete service-icmp

Description

Deletes an existing ICMP-type service object by name.

Syntax

```
delete service-icmp <name>
```

Parameters

Parameter	Description
name	Service name Type: String

Example

```
delete service-icmp TEXT
```

set service-icmp

Description

Configures an existing ICMP-type service object.

Syntax

```
set service-icmp <name>[ name <name> ] [ icmp-code <icmp-code> ] [
icmp-type <icmp-type> ] [ comments <comments> ]
```

Parameters

Parameter	Description
comments	Comments and explanation about the service Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
icmp-code	ICMP code Type: A number with no fractional part (integer)
icmp-type	ICMP message type Type: A number with no fractional part (integer)
name	Service name Type: String

Example

```
set service-icmp TEXT name TEXT icmp-code 2 icmp-type 5 comments "This
is a comment."
```

show service-icmp

Description

Shows the configuration of a specific ICMP-type service object.

Syntax

```
show service-icmp <name>
```

Parameters

Parameter	Description
name	Service name Type: String

Example

```
show service-icmp TEXT
```

add service-protocol

Description

Adds a new non-TCP/UDP service object (a different IP protocol than 6 or 17).

Syntax

```
add service-protocol name <name> ip-protocol <ip-protocol> [ comments
<comments>]
```

Parameters

Parameter	Description
comments	Comments and explanation about the service Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
ip-protocol	IP Protocol number Type: A number with no fractional part (integer)
name	Service name Type: String

Example

```
add service-protocol name TEXT ip-protocol 50 comments "This is a
comment."
```

service-protocol

delete service-protocol

Description

Deletes a non-TCP/UDP service object by name.

Syntax

```
delete service-protocol <name>
```

Parameters

Parameter	Description
name	Service name Type: String

Example

```
delete service-protocol TEXT
```

set service-protocol

Description

Configures an existing non-TCP/UDP service object.

Syntax

```
set service-protocol <name> [ name <name>] [ ip-protocol <ip-protocol>
] [ comments <comments> ] [ session-timeout <session-timeout> ] [
accept-replies
```

<accept-replies>] [sync-connections-on-cluster *<sync-connections-on-cluster>*

```
] [ match <match> ] [ aggressive-aging-enable <aggressive-aging-enable> ]
[ aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
accept-replies	Specifies if service replies are to be accepted
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
comments	Comments and explanation about the service Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
ip-protocol	IP Protocol number Type: A number with no fractional part (integer)
match	INSPECT expression that searches for a pattern in a packet, only relevant for services of type 'other'
name	Service name Type: String
session-timeout	Time (in seconds) before the session times out
sync-connections-on- cluster	Enables state-synchronized High Availability or Load Sharingon a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster

Example

```
set service-protocol TEXT name TEXT ip-protocol 50 comments "This is a
comment." session-timeout 15 accept-replies true sync-connections-on-
cluster true match TEXT aggressive-aging-enable true aggressive-aging-
timeout 15
```

show service-protocol

Description

Shows the configuration of a specific non-TCP/UDP service object.

Syntax

```
show service-protocol <name>
```

Parameters

Parameter	Description
name	Service name Type: String

Example

```
show service-protocol TEXT
```

show services-protocol

Description

Shows the configuration of all non-TCP/UDP service objects.

Syntax

```
show services-protocol
```

Parameters

Parameter	Description
n/a	

Example

```
show services-protocol
```

set server server-access

Description

Configures an existing server object. A server object is a network object with predefined access and NAT configurations.

Syntax

```
set server server-access <name> [ access-zones { blocked [ trusted-
zone-lan <trusted-zone-lan> ] [ trusted-zone-vpn-users <trusted-zone-
vpn-users> ] [ trusted-zone-trusted-wireless-networks <trusted-zone-
trusted-wireless-networks> ] [ trusted-zone-dmz <trusted-zone-dmz> ] [
trusted-zone-vpn-sites <trusted-zone-vpn-sites> ] | allowed } ] [
allow-ping-to-server <allow-ping-to-server> ] [ log-blocked-connections
<log-blocked-connections> ] [ log-accepted-connections <log-accepted-
connections> ]
```

Parameters

Parameter	Description
access-zones	Zones the server is accessible from by default (accept all by default, accept only from configured zones, or define no server-specific default access policy). Manual policy rules will override this policy. Type: Press TAB to see available options
allow-ping-to-server	Indicates if default access policy will work on ICMP traffic as well as defined ports. This option will not work on multiple ports hidden behind the gateway. Type: Boolean (true/false)
log-accepted-connections	Indicates if connections that are accepted by the default access policy to the server are logged Options: none, log
log-blocked-connections	Indicates if connections that are blocked by the default access policy to the server are logged Options: none, log
name	Server object name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces
trusted-zone-dmz	Indicates if traffic from the DMZ network to the server is allowed or blocked by default Options: blocked, allowed

Parameter	Description
trusted-zone-lan	Indicates if traffic from Physical internal networks (LAN ports) to the server is allowed or blocked by default Options: blocked, allowed
trusted-zone-trusted-wireless-networks	Indicates if traffic from trusted wireless networks to the server is allowed or blocked by default Options: blocked, allowed
trusted-zone-vpn-sites	Indicates if encrypted traffic from remote VPN sites to the server is allowed or blocked by default Options: blocked, allowed
trusted-zone-vpn- users	Indicates if encrypted traffic from VPN remote access users to the server is allowed or blocked by default Options: blocked, allowed

Example

```
set server server-access myObject_17 access-zones blocked trusted-zone-
lan blocked trusted-zone-vpn-users blocked trusted-zone-trusted-
wireless-networks blocked trusted-zone-dmz blocked trusted-zone-vpn-
sites blocked allow-ping-to-server true log-blocked-connections none
log-accepted-connections none
```

set server server-nat-settings

Description

Configures NAT settings on an existing server object.

Syntax

```
set server server-nat-settings <name> [ nat-settings { static-nat [
static-nat-ipv4-address <static-nat-ipv4-address> ] [ static-nat-for-
outgoing-traffic <static-nat-for-outgoing-traffic> ] | port-forwarding
} ] [ port-address-translation <port-address-translation> ] [ port-
address-translation-external <port-address-translation-external-port> ]
[ force-source-hide-nat <force-source-hide-nat > ]
```

Parameters

Parameter	Description
force-source-hide-nat	Allow access from internal networks to the external IP address of the server via local switch Type: Boolean (true/false)
name	Server object name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces
nat-settings	Indicates the general NAT settings configured (no NAT, hide behind the gateway's external IP address or use a different external IP address) Type: Press TAB to see available options
port-address-translation	For servers with a single port, indicates if the external port is not the same as the internal port. Type: Boolean (true/false)
port-address-translation-external-port	For servers with a single port, indicates the external port that is used to forward traffic to the server Type: Port number
static-nat-for-outgoing-traffic	indicates if outgoing traffic from the server using static NAT will be hidden behind the configured external IP address without a port change Type: Boolean (true/false)
static-nat-ipv4-address	For servers using static NAT, the external IP address used to forward traffic to the server Type: IP address

Example

```
set server server-nat-settings myObject_17 nat-settings static-nat
static-nat-ipv4-address 192.168.1.1 static-nat-for-outgoing-traffic
true port-address-translation true port-address-translation-external-
port 8080 force-source-hide-nat true
```

set server server-network-settings

Description

Configures network settings on an existing server object.

Syntax

```
set server server-network-settings <name> [ name <name> ] [ dhcp-
exclude-ip-addr { on [ dhcp-reserve-ip-addr-to-mac { on mac-addr <mac-
addr> | off } ] | off } ] [ comments <comments> ] [ dns-resolving <dns-
resolving> ] [ ipv4-address <ipv4-address> ]
```

Parameters

Parameter	Description
comments	Comments Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
dhcp-exclude-ip-addr	Indicates if the internal DHCP service will not distribute the configured IP address of this server/network object to anyone Type: Press TAB to see available options
dhcp-reserve-ip-addr- to-mac	Indicates if the internal DHCP service will distribute the configured IP address only to this server/network object according to its MAC address Type: Press TAB to see available options
dns-resolving	Indicates if the name of the server/network object will be used as a hostname for internal DNS service Type: Boolean (true/false)
ipv4-address	The beginning of the IP range
mac-addr	MAC address of the server Type: MAC address
name	Server object name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces

Example

```
set server server-network-settings myObject_17 name myObject_17 dhcp-
exclude-ip-addr on dhcp-reserve-ip-addr-to-mac on mac-addr
00:1C:7F:21:05:BE comments "This is a comment." dns-resolving true
ipv4-address 192.168.1.1
```

set server server-ports

Description

Configures an existing server object.

Syntax

```
set server server-ports <name> [ web-server { true service-http { true
[ service-http-ports <service-http-ports> ] | false } service-https {
true [ service-https-ports <service-https-ports> ] | false } | false }
] [ mail-server { true service-smtp { true [ service-smtp-ports
<service-smtp-ports> ] | false } service-pop3 { true [ service-pop3-
ports <service-pop3-ports> ] | false } service-imap { true [ service-
imap-ports <service-imap-ports> ] | false } | false } ] [ dns-server {
true service-dns { true [ service-dns-ports <service-dns-ports> ] |
false } | false } ] [ ftp-server { true service-ftp { true [ service-
ftp-ports <service-ftp-ports> ] | false } | false } ] [ citrix-server {
true service-citrix { true [ service-citrix-ports <service-citrix-
ports> ] | false } | false } ] [ pptp-server { true service-pptp-
selected { true [ service-pptp-ports <service-pptp-ports> ] | false } |
false } ] [ custom-server { true [ tcpProtocol <tcpProtocol> [ tcp-
ports <tcp-ports> ] udpProtocol <udpProtocol> [ udp-ports <udp-ports> ]
] | false } ]
```

Parameters

Parameter	Description
citrix-server	Indicates a Citrix server (for each type we provide default but configurable ports)
custom-server	Server type custom
dns-server	Indicates a DNS server (for each type we provide default but configurable ports
ftp-server	Indicates a FTP server (for each type we provide default but configurable ports)
mail-server	Indicates a mail server (for each type we provide default but configurable ports)
name	Server object name Type: A string that begins with a letter and contain up to 32 alphanumeric (0-9, a-z, _ - .) characters without spaces
pptp-server	Indicates a PPTP server (for each type we provide default but configurable ports)
service-citrix	Indicates if ports are defined for Citrix (for a Citrix server)
service-citrix-ports	Configured ports for Citrix (for a Citrix server)

Parameter	Description
service-dns	Indicates if ports are defined for DNS (for a DNS server)
service-dns-ports	Configured ports for DNS (for a DNS server)
service-ftp	Indicates if ports are defined for FTP (for a FTP server)
service-ftp-ports	Configured ports for FTP (for a FTP server)
service-http	Indicates if ports are defined for HTTP (for a web server)
service-http-ports	Configured ports for HTTP (for a web server)
service-https	Indicates if ports are defined for HTTPS (for a web server)
service-https-ports	Configured ports for HTTPS (for a web server)
service-imap	Indicates if ports are defined for IMAP (for a mail server)
service-imap-ports	Configured ports for IMAP (for a web server)
service-pop3	Indicates if ports are defined for POP3 (for a mail server)
service-pop3-ports	Configured ports for POP3 (for a web server)
service-pptp-ports	Configured ports for PPTP (for a PPTP server)
service-pptp-selected	Indicates if ports are defined for PPTP (for a PPTP server)
service-smtp	Indicates if ports are defined for SMTP (for a mail server)
service-smtp-ports	Configured ports for SMTP (for a web server)
tcp-ports	TCP ports for server of type 'other' Type: Port range
tcpProtocol	tcpProtocol Type: Boolean (true/false)
udp-ports	UDP ports for server of type 'other' Type: Port range

Parameter	Description
udpProtocol	udpProtocol Type: Boolean (true/false)
web-server	Indicates a web server (for each type we provide default but configurable ports)

Example

```
set server server-ports myObject_17 web-server true service-http true
service-http-ports 8080-8090 service-https true service-https-ports
8080-8090 mail-server true service-smtp true service-smtp-ports 8080-
8090 service-pop3 true service-pop3-ports 8080-8090 service-imap true
service-imap-ports 8080-8090 dns-server true service-dns true service-
dns-ports 8080-8090 ftp-server true service-ftp true service-ftp-ports
8080-8090 citrix-server true service-citrix true service-citrix-ports
8080-8090 pptp-server true service-pptp-selected true service-pptp-
ports 8080-8090 custom-server true tcpProtocol true tcp-ports 8080-8090
udpProtocol true udp-ports 8080-8090
```

service-system-default

set service-system-default Any_TCP

Description

Configures settings of the built-in Any_TCP service object.

Syntax

```
set service-system-default Any_TCP [ port <port> ] [ session-timeout
<session-timeout> ] [ use-source-port { false | true [ source-port
<source-port> ] } ] [ keep-connections-open-after-policy-installation
<keep-connections-open-after-policy-installation> ] [ sync-connections-
on-cluster <sync-connections-on-cluster> ] [ sync-delay-enable <sync-
delay-enable> ] [ delay-sync-interval <delay-sync-interval> ] [
aggressive-aging-enable <aggressive-aging-enable> ] [ aggressive-aging-
timeout <aggressive-aging-timeout>]
```

Parameters

Parameter	Description
aggressive-aging- enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port
sync-connections-on- cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule BaseRule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster.

Parameter	Description
sync-delay-enable	True to delay connections synchronization.
use-source-port	Use source port

Example

```
set service-system-default Any_TCP port 8080-8090 session-timeout 15
use-source-port false source-port 8080 keep-connections-open-after-
policy-installation true sync-connections-on-cluster true sync-delay-
enable true delay-sync-interval 15 aggressive-aging-enable true
aggressive-aging-timeout 15
```

show service-system-default Any_TCP

Description

Shows the settings of the built-in Any_TCP service object.

Syntax

```
show service-system-default Any_TCP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default Any_TCP
```

set service-system-default Any_UDP

Description

Configures settings of the built-in Any_UDP service object.

Syntax

```
set service-system-default Any_UDP [ port <port> ] [ session-timeout
<session-timeout> ] [ use-source-port { false | true [ source-port
<source-port> ] } ] [ keep-connections-open-after-policy-installation
<keep-connections-open-after-policy-installation> ] [ sync-connections-
on-cluster <sync-connections-on-cluster> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ] [ accept-replies <accept-replies> ]
```

Parameters

Parameter	Description
accept-replies	Specifies if service replies are to be accepted
aggressive-aging- enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port
sync-connections-on- cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster.
use-source-port	Use source port.

Example

```
set service-system-default Any_UDP port 8080-8090 session-timeout 15
use-source-port false source-port 8080 keep-connections-open-after-
policy-installation true sync-connections-on-cluster true aggressive-
aging-enable true aggressive-aging-timeout 15 accept-replies true
```

show service-system-default Any_UDP

Description

Shows the settings of the built-in Any_UDP service object.

Syntax

```
show service-system-default Any_UDP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default Any_UDP
```

set service-system-default CIFS

Description

Configures settings of the built-in CIFS service object.

Syntax

```
set service-system-default CIFS [ port <port> ] [ disable-inspection
<disable-inspection>] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster.
sync-delay-enable	True to delay connections synchronization.
use-source-port	Use source port.

Example

```
set service-system-default CIFS port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default CIFS

Description

Shows the settings of the built-in CIFS service object.

Syntax

```
show service-system-default CIFS
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default CIFS
```

set service-system-default Citrix

Description

Configures settings of the built-in Citrix service object.

Syntax

```
set service-system-default Citrix [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable>] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster.
sync-delay-enable	True to delay connections synchronization.
use-source-port	Use source port.

Example

```
set service-system-default Citrix port 8080-8090 disable-inspection
true session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default Citrix

Description

Shows the settings of the built-in Citrix service object.

Syntax

```
show service-system-default Citrix
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default Citrix
```

set service-system-default Citrix firewall-settings

Description

Configures firewall inspection settings of the built-in Citrix service object.

Syntax

```
set service-system-default Citrix firewall-settings [ protocol-support
<protocol-support> ]
```

Parameters

Parameter	Description
protocol-support	Which protocol to support on the configured ports. The default port 1494 is commonly used by two different protocols - Winframe or Citrix ICA Options: PROTO_TYPE.WIN_FRAME, PROTO_TYPE.CITRIX_ICA

Example

```
set service-system-default Citrix firewall-settings protocol-support
PROTO_TYPE.WIN_FRAME
```

show service-system-default Citrix firewall-settings

Description

Shows the inspection settings of the built-in Citrix service object.

Syntax

```
show service-system-default Citrix firewall-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default Citrix firewall-settings
```

set service-system-default DHCP

Description

Configures settings of the built-in DHCP service object.

Syntax

```
set service-system-default DHCP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ accept-
replies <accept-replies> ]
```

Parameters

Parameter	Description
accept-replies	Specifies if service replies are to be accepted
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port
use-source-port	Use source port

Example

```
set service-system-default DHCP port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 accept-
replies true
```

show service-system-default DHCP

Description

Shows the settings of the built-in DHCP service object.

Syntax

```
show service-system-default DHCP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default DHCP
```

set service-system-default DNS_TCP

Description

Configures settings of the built-in DNS_TCP service object.

Syntax

```
set service-system-default DNS_TCP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster.
sync-delay-enable	True to delay connections synchronization.
use-source-port	Use source port.

Example

```
set service-system-default DNS_TCP port 8080-8090 disable-inspection
true session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default DNS_TCP

Description

Shows the settings of the built-in DNS_TCP service object.

Syntax

```
show service-system-default DNS_TCP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default DNS_TCP
```

set service-system-default DNS_UDP

Description

Configures settings of the built-in DNS_UDP service object.

Syntax

```
set service-system-default DNS_UDP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ accept-
replies <accept-replies> ]
```

Parameters

Parameter	Description
accept-replies	Specifies if service replies are to be accepted.
disable-inspection	Disable deep inspection of traffic matching this service. Type: Boolean (true/false)
port	Destination ports (a comma separated list of ports/ranges). Type: Port range
session-timeout	Time (in seconds) before the session times out.
source-port	Source port.
use-source-port	Use source port.

Example

```
set service-system-default DNS_UDP port 8080-8090 disable-inspection
true session-timeout 15 use-source-port false source-port 8080 accept-
replies true
```

show service-system-default DNS_UDP

Description

Shows the settings of the built-in DNS_UDP service object.

Syntax

```
show service-system-default DNS_UDP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default DNS_UDP
```

set service-system-default FTP

Description

Configures settings of the built-in FTP service object.

Syntax

```
set service-system-default FTP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable>] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability.
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out.
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections.
disable-inspection	Disable deep inspection of traffic matching this service. Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy.
port	Destination ports (a comma separated list of ports/ranges). Type: Port range
session-timeout	Time (in seconds) before the session times out.
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster.
sync-delay-enable	True to delay connections synchronization.
use-source-port	Use source port.

Example

```
set service-system-default FTP port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default FTP

Description

Shows the settings of the built-in FTP service object.

Syntax

```
show service-system-default FTP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default FTP
```

set service-system-default FTP firewall-settings

Description

Configures firewall inspection settings of the built-in FTP service object.

Syntax

```
set service-system-default FTP firewall-settings [ mode <mode> ]
```

Parameters

Parameter	Description
mode	FTP connection mode (allowed values are 'Any', 'Active' or 'Passive'). Options: any, active, passive

Example

```
set service-system-default FTP firewall-settings mode any
```

show service-system-default FTP firewall-settings

Description

Shows the inspection settings of the built-in FTP service object.

Syntax

```
show service-system-default FTP firewall-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default FTP firewall-settings
```

set service-system-default GRE

Description

Configures settings of the built-in GRE service object.

Syntax

```
set service-system-default GRE [ ip-protocol <ip-protocol> ] [ disable-
inspection <disable-inspection> ] [ session-timeout <session-timeout>]
[ accept-replies <accept-replies> ] [ match <match> ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ aggressive-aging-enable <aggressive-aging-
enable> ] [ aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
accept-replies	Specifies if service replies are to be accepted.
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability.
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out.
disable-inspection	Disable deep inspection of traffic matching this service. Type: Boolean (true/false)
ip-protocol	IP Protocol number. Type: A number with no fractional part (integer)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy.
match	INSPECT expression that searches for a pattern in a packet, only relevant for services of type 'other'.
session-timeout	Time (in seconds) before the session times out
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster.

Example

```
set service-system-default GRE ip-protocol 15 disable-inspection true
session-timeout 15 accept-replies true match TEXT keep-connections-
open-after-policy-installation true sync-connections-on-cluster true
aggressive-aging-enable true aggressive-aging-timeout 15
```

show service-system-default GRE

Description

Shows the settings of the built-in GRE service object.

Syntax

```
show service-system-default GRE
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default GRE
```

set service-system-default H323

Description

Configures settings of the built-in H323 service object.

Syntax

```
set service-system-default H323 [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ]
```

Parameters

Parameter	Description
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections.
disable-inspection	Disable deep inspection of traffic matching this service. Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy.
port	Destination ports (a comma separated list of ports/ranges). Type: Port range
session-timeout	Time (in seconds) before the session times out.
source-port	Source port.
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster.
sync-delay-enable	True to delay connections synchronization.
use-source-port	Use source port.

Example

```
set service-system-default H323 port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15
```

show service-system-default H323

Description

Shows the settings of the built-in H323 service object.

Syntax

```
show service-system-default H323
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default H323
```

set service-system-default H323_RAS

Description

Configures settings of the built-in H323_RAS service object.

Syntax

```
set service-system-default H323_RAS [ port <port> ] [ disable-
inspection <disable-inspection> ] [ session-timeout <session-timeout> ]
[ use-source-port { false | true [ source-port <source-port> ] } ] [
accept-replies <accept-replies> ]
```

Parameters

Parameter	Description
accept-replies	Specifies if service replies are to be accepted.
disable-inspection	Disable deep inspection of traffic matching this service. Type: Boolean (true/false)
port	Destination ports (a comma separated list of ports/ranges). Type: Port range
session-timeout	Time (in seconds) before the session times out.
source-port	Source port.
use-source-port	Use source port.

Example

```
set service-system-default H323_RAS port 8080-8090 disable-inspection
true session-timeout 15 use-source-port false source-port 8080 accept-
replies true
```

show service-system-default H323_RAS

Description

Shows the settings of the built-in H323_RAS service object.

Syntax

```
show service-system-default H323_RAS
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default H323_RAS
```

set service-system-default HTTP

Description

Configures settings of the built-in HTTP service object.

Syntax

```
set service-system-default HTTP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable>] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability.
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out.
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections.
disable-inspection	Disable deep inspection of traffic matching this service. Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy.
port	Destination ports (a comma separated list of ports/ranges). Type: Port range
session-timeout	Time (in seconds) before the session times out.
source-port	Source port.

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster.
sync-delay-enable	True to delay connections synchronization.
use-source-port	Use source port.

Example

```
set service-system-default HTTP port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default HTTP

Description

Shows the settings of the built-in HTTP service object.

Syntax

```
show service-system-default HTTP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default HTTP
```

set service-system-default HTTPS

Description

Configures settings of the built-in HTTPS service object.

Syntax

```
set service-system-default HTTPS [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability.
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out.
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections.
disable-inspection	Disable deep inspection of traffic matching this service. Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy.
port	Destination ports (a comma separated list of ports/ranges). Type: Port range
session-timeout	Time (in seconds) before the session times out.
source-port	Source port.

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster.
sync-delay-enable	True to delay connections synchronization.
use-source-port	Use source port.

Example

```
set service-system-default HTTPS port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 >keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default HTTPS

Description

Shows the settings of the built-in HTTPS service object.

Syntax

```
show service-system-default HTTPS
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default HTTPS
```

set service-system-default HTTP ips-settings

Description

Configures IPS settings of the built-in HTTP service object.

Syntax

```
set service-system-default HTTP ips-settings [ non-standard-ports-
action <non-standard-ports-action>] [ non-standard-ports-track <non-
standard-ports-track> ] [ parser-failure-action <parser-failure-action>
] [ parser-failure-track <parser-failure-track> ] [ strict-request
<strict-request> ] [ strict-response <strict-response> ] [ split-url
<split-url> ] [ no-colon <no-colon> ] [ tab-as-seperator <tab-as-
seperator>] [ duplicate-content-length <duplicate-content-length> ] [
duplicate-host <duplicate-host> ] [ responses <responses> ] [ invalid-
chunk <invalid-chunk> ] [ empty-value <empty-value> ] [ post <post>] [
recursive-url <recursive-url> ] [ trailing-whitespaces <trailing-
whitespaces> ]
```

Parameters

Parameter	Description
duplicate-content-length	True to block duplicate Content-Length' header with same value. Type: Boolean (true/false)
duplicate-host	True to block duplicate 'Host' header with same value. Type: Boolean (true/false)
empty-value	True to block HTTP header with empty value. Type: Boolean (true/false)
invalid-chunk	True if invalid chunk. Type: Boolean (true/false)
no-colon	True to block HTTP header with no colon. Type: Boolean (true/false)
non-standard-ports-action	Select action for connection over non standard ports (allowed values are 'Accept' and 'Block'). Options: block, accept

Parameter	Description
non-standard-ports-track	Select track option for connection over non standard ports (allowed values are 'log', 'alert' and 'don't log') . Options: none, log, alert
parser-failure-action	Select action for when the parser fails (allowed values are 'Accept' and 'Block'). Options: block, accept
parser-failure-track	Select track option for when the parser fails (allowed values are 'log', 'alert' and 'don't log'). Options: none, log, alert
post	True to block requests with 'POST' method and without 'Content-Type' header. Type: Boolean (true/false)
recursive-url	True to block HTTP requests with recursive URL encoding. Type: Boolean (true/false)
responses	True to block responses with both 'Content-Length' and 'Transfer-Encoding'headers. Type: Boolean (true/false)
split-url	True to split the URL between the query and fragment sections instructs the HTTP protections to inspect the query and fragment sections separately. Type: Boolean (true/false)
strict-request	True to enforce strict HTTP request parsing. Type: Boolean (true/false)
strict-response	True to enforce strict HTTP response parsing. Type: Boolean (true/false)
tab-as-seperator	True to block HTTP traffic with 'tab' character as a separator. Type: Boolean (true/false)
trailing-whitespaces	True to block request header names with trailing whitespaces. Type: Boolean (true/false)

Example

```
set service-system-default HTTP ips-settings non-standard-ports-action
block non-standard-ports-track none parser-failure-action block parser-
failure-track none strict-request true strict-response true split-url
true no-colon true tab-as-seperator true duplicate-content-length true
duplicate-host true responses true invalid-chunk true empty-value true
post true recursive-url true trailing-whitespaces true
```

show service-system-default HTTP ips-settings

Description

Shows the inspection settings of the built-in HTTP service object.

Syntax

```
show service-system-default HTTP ips-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default HTTP ips-settings
```

set service-system-default HTTPS url-filtering-settings

Description

Configures URL filtering over HTTPS. Enables categorization over HTTPS even without full SSL inspection.

Syntax

```
set service-system-default HTTPS url-filtering-settings [ categorize-
https-sites <categorize-https-sites> ]
```

Parameters

Parameter	Description
categorize-https-sites	Categorize HTTPS sites by their certificate CN. Type: Boolean (true/false)

Example

```
set service-system-default HTTPS url-filtering-settings categorize-
https-sites true
```

show service-system-default HTTPS url-filtering-settings

Description

Shows the configuration of URL filtering categorization option over HTTPS.

Syntax

```
show service-system-default HTTPS url-filtering-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default HTTPS url-filtering-settings
```

set service-system-default IIOP

Description

Configures settings of the built-in IIOP service object.

Syntax

```
set service-system-default IIOP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable>] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability.
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out.
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections.
disable-inspection	Disable deep inspection of traffic matching this service. Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy.
port	Destination ports (a comma separated list of ports/ranges). Type: Port range
session-timeout	Time (in seconds) before the session times out.
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster.
sync-delay-enable	True to delay connections synchronization.
use-source-port	Use source port.

Example

```
set service-system-default IIOP port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default IIOP

Description

Shows the settings of the built-in IIOP service object.

Syntax

```
show service-system-default IIOP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default IIOP
```

set service-system-default IMAP

Description

Configures settings of the built-in IMAP service object.

Syntax

```
set service-system-default IMAP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability.
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out.
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections.
disable-inspection	Disable deep inspection of traffic matching this service. Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy.
port	Destination ports (a comma separated list of ports/ranges). Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default IMAP port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default IMAP

Description

Shows the settings of the built-in IMAP service object.

Syntax

```
show service-system-default IMAP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default IMAP
```

set service-system-default LDAP

Description

Configures settings of the built-in LDAP service object.

Syntax

```
set service-system-default LDAP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default LDAP port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default LDAP

Description

Shows the settings of the built-in LDAP service object.

Syntax

```
show service-system-default LDAP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default LDAP
```

set service-system-default MGCP

Description

Configures settings of the built-in MGCP service object.

Syntax

```
set service-system-default MGCP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port>] } ] [ accept-
replies <accept-replies> ]
```

Parameters

Parameter	Description
accept-replies	Specifies if service replies are to be accepted
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port
use-source-port	Use source port

Example

```
set service-system-default MGCP port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 accept-
replies true
```

show service-system-default MGCP

Description

Shows the settings of the built-in MGCP service object.

Syntax

```
show service-system-default MGCP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default MGCP
```

set service-system-default NetBIOSDatagram

Description

Configures settings of the built-in NetBiosDatagram service object.

Syntax

```
set service-system-default NetBIOSDatagram [ port <port> ] [ disable-inspection <disable-inspection> ] [ session-timeout <session-timeout> ] [ use-source-port { false | true [ source-port <source-port> ] } ] [ accept-replies <accept-replies> ]
```

Parameters

Parameter	Description
accept-replies	Specifies if service replies are to be accepted
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port
use-source-port	Use source port

Example

```
set service-system-default NetBIOSDatagram port 8080-8090 disable-inspection true session-timeout 15 use-source-port false source-port 8080 accept-replies true
```

show service-system-default NetBIOSDatagram

Description

Shows the settings of the built-in NetBiosDatagram service object.

Syntax

```
show service-system-default NetBIOSDatagram
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default NetBIOSDatagram
```

set service-system-default NetBIOSName

Description

Configures settings of the built-in NetBiosName service object.

Syntax

```
set service-system-default NetBIOSName [ port <port> ] [ disable-
inspection <disable-inspection>] [ session-timeout <session-timeout> ]
[ use-source-port { false | true [ source-port <source-port> ] } ] [
accept-replies <accept-replies>]
```

Parameters

Parameter	Description
accept-replies	Specifies if service replies are to be accepted
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port
use-source-port	Use source port

Example

```
set service-system-default NetBIOSName port 8080-8090 disable-
inspection true session-timeout 15 use-source-port false source-port
8080 accept-replies true
```

show service-system-default NetBIOSName

Description

Shows the settings of the built-in NetBiosName service object.

Syntax

```
show service-system-default NetBIOSName
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default NetBIOSName
```

set service-system-default NetShow

Description

Configures settings of the built-in NetShow service object.

Syntax

```
set service-system-default NetShow [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default NetShow port 8080-8090 disable-inspection
true session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default NetShow

Description

Shows the settings of the built-in NetShow service object.

Syntax

```
show service-system-default NetShow
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default NetShow
```

set service-system-default NNTP

Description

Configures settings of the built-in NNTP service object.

Syntax

```
set service-system-default NNTP [ port <port> ] [ disable-inspection
<disable-inspection>] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default NNTP port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default NNTP

Description

Shows the settings of the built-in NNTP service object.

Syntax

```
show service-system-default NNTP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default NNTP
```

set service-system-default POP3

Description

Configures settings of the built-in POP3 service object.

Syntax

```
set service-system-default POP3 [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default POP3 port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default POP3

Description

Shows the settings of the built-in POP3 service object.

Syntax

```
show service-system-default POP3
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default POP3
```

set service-system-default PPTP_TCP

Description

Configures settings of the built-in PPTP_TCP service object.

Syntax

```
set service-system-default PPTP_TCP [ port <port> ] [ disable-
inspection <disable-inspection>] [ session-timeout <session-timeout> ]
[ use-source-port { false | true [ source-port <source-port> ] } ] [
keep-connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable>] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default PPTP_TCP port 8080-8090 disable-inspection
true session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default PPTP_TCP

Description

Shows the settings of the built-in PPTP_TCP service object.

Syntax

```
show service-system-default PPTP_TCP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default PPTP_TCP
```

set service-system-default PPTP_TCP ips-settings

Description

Configures additional inspection settings of the built-in PPTP_TCP service object.

Syntax

```
set service-system-default PPTP_TCP ips-settings [ action <action> ] [
track
```

```
<track> ] [ strict <strict> ]
```

Parameters

Parameter	Description
action	Select action for PPTP connections (allowed values are 'Accept' and 'Block') Options: block, accept
strict	True to enforce strict PPTP parsing Type: Boolean (true/false)
track	Select track option for PPTP connections (allowed values are 'log', 'alert' and 'don't log') Options: none, log, alert

Example

```
set service-system-default PPTP_TCP ips-settings action block track
none strict true
```

show service-system-default PPTP_TCP ips-settings

Description

Shows the inspection settings of the built-in Any_TCP service object.

Syntax

```
show service-system-default PPTP_TCP ips-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default PPTP_TCP ips-settings
```

set service-system-default RealAudio

Description

Configures settings of the built-in RealAudio service object.

Syntax

```
set service-system-default RealAudio [ port <port> ] [ disable-
inspection <disable-inspection> ] [ session-timeout <session-timeout> ]
[ use-source-port { false | true [ source-port <source-port> ] } ] [
keep-connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default RealAudio port 8080-8090 disable-inspection
true session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default RealAudio

Description

Shows the settings of the built-in RealAudio service object.

Syntax

```
show service-system-default RealAudio
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default RealAudio
```

set service-system-default RSH

Description

Configures settings of the built-in RSH service object.

Syntax

```
set service-system-default RSH [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default RSH port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default RSH

Description

Shows the settings of the built-in RSH service object.

Syntax

```
show service-system-default RSH
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default RSH
```

set service-system-default RTSP

Description

Configures settings of the built-in RTSP service object.

Syntax

```
set service-system-default RTSP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default RTSP port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default RTSP

Description

Shows the settings of the built-in RTSP service object.

Syntax

```
show service-system-default RTSP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default RTSP
```

set service-system-default SCCP

Description

Configures settings of the built-in SCCP service object.

Syntax

```
set service-system-default SCCP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default SCCP port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default SCCP

Description

Shows the settings of the built-in SCCP service object.

Syntax

```
show service-system-default SCCP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default SCCP
```

set service-system-default SCCPS

Description

Configures settings of the built-in SCCPS service object.

Syntax

```
set service-system-default SCCPS [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default SCCPS port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default SCCPS

Description

Shows the settings of the built-in SCCPS service object.

Syntax

```
show service-system-default SCCPS
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default SCCPS
```

set service-system-default SIP_TCP

Description

Configures settings of the built-in SIP_TCP service object.

Syntax

```
set service-system-default SIP_TCP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default SIP_TCP port 8080-8090 disable-inspection
true session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default SIP_TCP

Description

Shows the settings of the built-in SIP_TCP service object.

Syntax

```
show service-system-default SIP_TCP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default SIP_TCP
```

set service-system-default SIP_UDP

Description

Configures settings of the built-in SIP_UDP service object.

Syntax

```
set service-system-default SIP_UDP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ accept-
replies <accept-replies> ]
```

Parameters

Parameter	Description
accept-replies	Specifies if service replies are to be accepted
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port
use-source-port	Use source port

Example

```
set service-system-default SIP_UDP port 8080-8090 disable-inspection
true session-timeout 15 use-source-port false source-port 8080 accept-
replies true
```

show service-system-default SIP_UDP

Description

Shows the settings of the built-in SIP_UDP service object.

Syntax

```
show service-system-default SIP_UDP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default SIP_UDP
```

set service-system-default SMTP

Description

Configures settings of the built-in SMTP service object.

Syntax

```
set service-system-default SMTP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default SMTP port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default SMTP

Description

Shows the settings of the built-in SMTP service object.

Syntax

```
show service-system-default SMTP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default SMTP
```

set service-system-default SNMP

Description

Configures settings of the built-in SNMP service object.

Syntax

```
set service-system-default SNMP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ accept-
replies <accept-replies> ]
```

Parameters

Parameter	Description
accept-replies	Specifies if service replies are to be accepted
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port
use-source-port	Use source port

Example

```
set service-system-default SNMP port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 accept-
replies true
```

show service-system-default SNMP

Description

Shows the settings of the built-in SNMP service object.

Syntax

```
show service-system-default SNMP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default SNMP
```

set service-system-default SNMP firewall-settings

Description

Additional configuration for SNMP service

Syntax

```
set service-system-default SNMP firewall-settings [ read-only <read-
only> ]
```

Parameters

Parameter	Description
read-only	True to enforce read-only mode Type: Boolean (true/false)

Example

```
set service-system-default SNMP firewall-settings read-only true
```

show service-system-default SNMP firewall-settings

Description

Shows the inspection settings of the built-in SNMP service object.

Syntax

```
show service-system-default SNMP firewall-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default SNMP firewall-settings
```

set service-system-default SQLNet

Description

Configures settings of the built-in SQLNet service object.

Syntax

```
set service-system-default SQLNet [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default SQLNet port 8080-8090 disable-inspection
true session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default SQLNet

Description

Shows the settings of the built-in SQLNet service object.

Syntax

```
show service-system-default SQLNet
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default SQLNet
```

set service-system-default SSH

Description

Configures settings of the built-in SSH service object.

Syntax

```
set service-system-default SSH [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout>] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable> ] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default SSH port 8080-8090 disable-inspection true
session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default SSH

Description

Shows the settings of the built-in SSH service object.

Syntax

```
show service-system-default SSH
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default SSH
```

set service-system-default SSH ips-settings

Description

Configures additional inspection settings of the built-in SSH service object.

Syntax

```
set service-system-default SSH ips-settings [ block-version <block-
version>
```

Parameters

Parameter	Description
block-version	True to enforce blocking of version 1.x Type: Boolean (true/false)

Example

```
set service-system-default SSH ips-settings block-version true
```

show service-system-default SSH ips-settings

Description

Shows the inspection settings of the built-in SSH service object.

Syntax

```
show service-system-default SSH ips-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default SSH ips-settings
```

set service-system-default TELNET

Description

Configures settings of the built-in TELNET service object.

Syntax

```
set service-system-default TELNET [ port <port> ] [ disable-inspection
<disable-inspection> ] [ session-timeout <session-timeout> ] [ use-
source-port { false | true [ source-port <source-port> ] } ] [ keep-
connections-open-after-policy-installation <keep-connections-open-
after-policy-installation> ] [ sync-connections-on-cluster <sync-
connections-on-cluster> ] [ sync-delay-enable <sync-delay-enable>] [
delay-sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
<aggressive-aging-enable> ] [ aggressive-aging-timeout <aggressive-
aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-system-default TELNET port 8080-8090 disable-inspection
true session-timeout 15 use-source-port false source-port 8080 keep-
connections-open-after-policy-installation true sync-connections-on-
cluster true sync-delay-enable true delay-sync-interval 15 aggressive-
aging-enable true aggressive-aging-timeout 15
```

show service-system-default TELNET

Description

Shows the settings of the built-in TELNET service object.

Syntax

```
show service-system-default TELNET
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default TELNET
```

set service-system-default TFTP

Description

Configures settings of the built-in TFTP service object.

Syntax

```
set service-system-default TFTP [ port <port> ] [ disable-inspection
<disable-inspection> ] [ accept-replies <accept-replies> ] [ session-
timeout <session-timeout> ] [ use-source-port { false | true [ source-
port <source-port> ] } ] [ keep-connections-open-after-policy-
installation <keep-connections-open-after-policy-installation> ] [
sync-connections-on-cluster <sync-connections-on-cluster> ]
```

Parameters

Parameter	Description
accept-replies	Specifies if service replies are to be accepted
disable-inspection	Disable deep inspection of traffic matching this service Type: Boolean (true/false)
keep-connections-open-after-policy-installation	True to keep connections open after policy has been installed, even if they are not allowed under the new policy
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
use-source-port	Use source port

Example

```
set service-system-default TFTP port 8080-8090 disable-inspection true
accept-replies true session-timeout 15 use-source-port false source-
port 8080 keep-connections-open-after-policy-installation true sync-
connections-on-cluster true
```

show service-system-default TFTP

Description

Shows the settings of the built-in TFTP service object.

Syntax

```
show service-system-default TFTP
```

Parameters

Parameter	Description
n/a	

Example

```
show service-system-default TFTP
```

service-tcp

add service-tcp

Description

Adds a new TCP service object with configurable ports.

Syntax

```
add service-tcp name <name> port <port> [ comments <comments> ]
```

Parameters

Parameter	Description
comments	Comments and explanation about the service Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
name	Service name Type: String
port	Destination ports (a comma separated list of ports/ranges) Type: Port range

Example

```
add service-tcp name TEXT port 8080-8090 comments "This is a comment."
```

set service-tcp

Description

Configures an existing TCP service object.

Syntax

```
set service-tcp <name> [ name <name> ] [ port <port> ] [ comments
<comments> ] [ session-timeout <session-timeout>] [ sync-connections-
on-cluster <sync-connections-on-cluster>] [ sync-delay-enable <sync-
delay-enable> ] [ delay-sync-interval
```

<delay-sync-interval>] [aggressive-aging-enable *<aggressive-aging-enable>*

```
] [ aggressive-aging-timeout <aggressive-aging-timeout> ] [ use-source-
port { false | true source-port <source-port>} ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
comments	Comments and explanation about the service Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections
name	Service name Type: String
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
source-port	Source port

Parameter	Description
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster
sync-delay-enable	True to delay connections synchronization
use-source-port	Use source port

Example

```
set service-tcp TEXT name TEXT port 8080-8090 comments "This is a
comment." session-timeout 15 sync-connections-on-cluster true sync-
delay-enable true delay-sync-interval 15 aggressive-aging-enable true
aggressive-aging-timeout 15 use-source-port false source-port 8080
```

delete service-tcp

Description

Deletes a TCP service object by name.

Syntax

```
delete service-tcp <name>
```

Parameters

Parameter	Description
name	Service name Type: String

Example

```
delete service-tcp TEXT
```

show service-tcp

Description

Shows the configuration of a specific TCP service object.

Syntax

```
show service-tcp <name>
```

Parameters

Parameter	Description
name	Service name Type: String

Example

```
show service-tcp TEXT
```

show services-tcp

Description

Shows the configuration of all TCP service objects.

Syntax

```
show services-tcp
```

Parameters

Parameter	Description
n/a	

Example

```
show services-tcp
```

service-udp

add service-udp

Description

Adds a new UDP service object with configurable ports.

Syntax

```
add service-udp name <name> port <port> [ comments <comments> ]
```

Parameters

Parameter	Description
comments	Comments and explanation about the service Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
name	Service name Type: String
port	Destination ports (a comma separated list of ports/ranges) Type: Port range

Example

```
add service-udp name TEXT port 8080-8090 comments "This is a comment."
```

delete service-udp

Description

Deletes a UDP service object by name.

Syntax

```
delete service-udp <name>
```

Parameters

Parameter	Description
name	Service name Type: String

Example

```
delete service-udp TEXT
```

set service-udp

Description

Configures an existing UDP service object

Syntax

```
set service-udp <name> [ name <name> ] [ port <port> ] [ comments
<comments> ] [ session-timeout <session-timeout> ] [ accept-replies
<accept-replies> ] [ sync-connections-on-cluster <sync-connections-on-
cluster> ] [ aggressive-aging-enable <aggressive-aging- enable> ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
accept-replies	Specifies if service replies are to be accepted
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability
aggressive-aging-timeout	Time (in seconds) before the aggressive aging times out
comments	Comments and explanation about the service Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
name	Service name Type: String
port	Destination ports (a comma separated list of ports/ranges) Type: Port range
session-timeout	Time (in seconds) before the session times out
sync-connections-on-cluster	Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with synchronize connections on cluster will be synchronized as they pass through the cluster

Example

```
set service-udp TEXT name TEXT port 8080-8090 comments "This is a
comment." session-timeout 15 accept-replies true sync-connections-on-
cluster true aggressive-aging-enable true aggressive-aging-timeout 15
```

show service-udp

Description

Shows the configuration of a specific UDP service object

Syntax

```
show service-udp <name>
```

Parameters

Parameter	Description
name	Service name Type: String

Example

```
show service-udp TEXT
```

show services-udp

Description

Shows the configuration of all UDP service objects.

Syntax

```
show services-udp
```

Parameters

Parameter	Description
n/a	

Example

```
show services-udp
```

show services-icmp

Description

Shows the configuration of all ICMP-type service objects.

Syntax

```
show services-icmp
```

Parameters

Parameter	Description
n/a	

Example

```
show services-icmp
```

shell/expert

The `shell`and `expert`commands switch between the shell and expert modes.

Description

Changes to expert mode.

Syntax

```
shell
```

```
expert
```

Parameters

Parameter	Description
n/a	

Example

```
shell
```

Comments

Use the cpshell command to start cpshell.

set sic_init

Description

Sets the SIC password.

Syntax

```
set sic_init password <pass>
```

Parameters

Parameter	Description
pass	One-time password, as specified by the Security Management Server administrator.

Example

```
set sic_init password verySecurePassword
```

sim

Description

SecureXL Implementation Module commands

Parameters

Parameter	Description
`ver`	get the version
`if`	get the interface list
`tab [-s] [name]`	print the table content (-s for summary)
`ranges`	print the range content
`tab -d templates`	print only templates in drop state
`dbg <options>`	set the sim debug flags
`affinity`	get/set affinity options
`nonaccel [-s|-c] <name(s)>`	set or clear interface(s) as not accelerated
`feature <feature> {on | off}`	enable/disable features
`tmplquota <options>`	configure template quota feature
`hlqos <options>`	configure Heavy-Load CPU QOS feature

snmp

add snmp

Adds SNMP trap receiver and SNMP users to the SNMP configuration.

add snmp

Description

Adds a new SNMP trap receiver IP address to be used by the SNMP agent.

Syntax

```
add snmp traps-receiver <traps-receiver> version { v2 community
<community> | v3 user <user> }
```

Parameters

Parameter	Description
community	Community name of the receivers trap, public is default for version2 users Type: A string of alphanumeric characters without space between them
traps-receiver	Receivers IP address that the trap associated with Type: IP address
user	SNMP version3 Defined user
version	SNMP Version, options are: v2 or v3 Type: Press TAB to see available options

Example

```
add snmp traps-receiver 192.168.1.1 version v2 community word
```

add snmp

Description

Adds a new user to be used by SNMPv3 protocol.

Syntax

```
add snmp user <user> security-level { true auth-pass-type <auth-pass-type> auth-pass-phrase <auth-pass-phrase> privacy-pass-type <privacy-pass-type> privacy-pass-phrase <privacy-pass-phrase> | false auth-pass-type <auth-pass-type> auth-pass-phrase <auth-pass-phrase> }
```

Parameters

Parameter	Description
auth-pass-phrase	Authentication password for the SNMP version3 user Type: A string that contains alphanumeric and special characters
auth-pass-type	Authentication protocol type for the version3 user, options are: MD5 or SHA1 Options: MD5, SHA1
privacy-pass-phrase	Privacy password chosen by the version3 user in case privacy is set Type: A string that contains alphanumeric and special characters
privacy-pass-type	Privacy protocol type for the version3 user, options are: AES or DES Options: AES, DES
security-level	Does Privacy protocol for this version3 user was set in the security level Type: Boolean (true/false)
user	version3 user name Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces

Example

```
add snmp user admin security-level true auth-pass-type MD5 auth-pass-phrase a(&7Ba privacy-pass-type AES privacy-pass-phrase a(&7Ba
```

delete snmp

Deletes SNMP trap receivers and SNMP users.

delete snmp

Description

Deletes an existing SNMP trap receiver by IP address.

Syntax

```
delete snmp traps-receiver <traps-receiver>
```

Parameters

Parameter	Description
traps-receiver	Receivers IP address that the trap associated with Type: IP address

Example

```
delete snmp traps-receiver 192.168.1.1
```

delete snmp

Description

Deletes a configured SNMP contact.

Syntax

```
delete snmp contact
```

Parameters

Parameter	Description
n/a	

Example

```
delete snmp contact
```

delete snmp

Description

Deletes a configured SNMP location.

Syntax

```
delete snmp location
```

Parameters

Parameter	Description
n/a	

Example

```
delete snmp location
```

set snmp

Configures SNMP settings.

set snmp

escription

Configures SNMP agent settings.

Syntax

```
set snmp agent <agent> [ agent-version <agent-version> ] [ community
<community> ] [ contact <contact> ] [ location <location> ]
```

Parameters

Parameter	Description
agent	Is SNMP option enabled or disabled, disabled is the default Type: Boolean (true/false)
agent-version	Is the defined SNMP version is version3 only Type: Boolean (true/false)
community	Community name of the SNMP, public is the default Type: A string of alphanumeric characters without space between them
contact	System contact name, maximum length is 128 Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
location	System location name Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @

Example

```
set snmp agent true agent-version true community word contact myContact
location myLocation
```

set snmp

Description

Configures SNMP agent settings.

Syntax

```
set snmp agent-version <agent-version> [ agent <agent> ] [ community
<community> ] [ contact <contact> ] [ location <location> ]
```

Parameters

Parameter	Description
agent	Is SNMP option enabled or disabled, disabled is the default Type: Boolean (true/false)
agent-version	Is the defined SNMP version is version3 only Type: Boolean (true/false)
community	Community name of the SNMP, public is the default Type: A string of alphanumeric characters without space between them
contact	System contact name, maximum length is 128 Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
location	System location name Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @

Example

```
set snmp agent-version true agent true community word contact myContact
location myLocation
```

set snmp

Description

Configures SNMP community settings.

Syntax

```
set snmp community <community> [ agent <agent> ] [ agent-version
<agent-version> ] [ contact <contact> ] [ location <location> ]
```

Parameters

Parameter	Description
agent	Is SNMP option enabled or disabled, disabled is the default Type: Boolean (true/false)
agent-version	Is the defined SNMP version is version3 only Type: Boolean (true/false)
community	Community name of the SNMP, public is the default Type: A string of alphanumeric characters without space between them
contact	System contact name, maximum length is 128 Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
location	System location name Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @

Example

```
set snmp community word agent true agent-version true contact myContact
location myLocation
```

set snmp

Description

Configures SNMP contact settings.

Syntax

```
set snmp contact <contact> [ agent <agent> ] [ agent-version <agent-
version>
```

```
] [ community <community> ] [ location <location> ]
```

Parameters

Parameter	Description
agent	Is SNMP option enabled or disabled, disabled is the default Type: Boolean (true/false)
agent-version	Is the defined SNMP version is version3 only Type: Boolean (true/false)
community	Community name of the SNMP, public is the default Type: A string of alphanumeric characters without space between them
contact	System contact name, maximum length is 128 Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
location	System location name Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @

Example

```
set snmp contact myContact agent true agent-version true community word
location myLocation
```

set snmp

Description

Configures SNMP location settings.

Syntax

```
set snmp location <location>[ agent <agent> ] [ agent-version <agent-version> ] [ community <community> ] [ contact <contact> ]
```

Parameters

Parameter	Description
agent	Is SNMP option enabled or disabled, disabled is the default Type: Boolean (true/false)
agent-version	Is the defined SNMP version is version3 only Type: Boolean (true/false)
community	Community name of the SNMP, public is the default Type: A string of alphanumeric characters without space between them
contact	System contact name, maximum length is 128 Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
location	System location name Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @

Example

```
set snmp location myLocation agent true agent-version true community word contact myContact
```

show snmp

Shows SNMP configuration.

show snmp

Description

Shows SNMP agent configuration.

Syntax

```
show snmp agent
```

Parameters

Parameter	Description
n/a	

Example

```
show snmp agent
```

show snmp

Description

Shows SNMP agent version configuration.

Syntax

```
show snmp agent-version
```

Parameters

Parameter	Description
n/a	

Example

```
show snmp agent-version
```

show snmp

Description

Shows SNMP community configuration.

Syntax

```
show snmp community
```

Parameters

Parameter	Description
n/a	

Example

```
show snmp community
```

show snmp

Description

Shows SNMP contact configuration.

Syntax

```
show snmp contact
```

Parameters

Parameter	Description
n/a	

Example

```
show snmp contact
```

show snmp

Description

Shows SNMP location configuration.

Syntax

```
show snmp location
```

Parameters

Parameter	Description
n/a	

Example

```
show snmp location
```

show snmp-general-all

Description

Shows SNMP configuration.

Syntax

```
show snmp-general-all
```

Parameters

Parameter	Description
n/a	

Example

```
show snmp-general-all
```

snmp traps

set snmp traps

Configures, enables or disables traps from the list, the enabled traps are sent to the trap receivers.

set snmp traps

Description

Enable/Disable SNMP traps functionality.

Syntax

```
set snmp traps { enable | disable }
```

Parameters

Parameter	Description
snmpTrapsEnable	snmpTrapsEnable Type: Boolean (true/false)

Example

```
set snmp traps true
```

set snmp traps

Description

Configures an existing SNMP trap.

Syntax

```
set snmp traps trap-name <trap-name> [ enable <enable> ] [ severity
<severity> ] [ repetitions <repetitions> ] [ repetitions-delay
<repetitions-delay> ] [ threshold <threshold> ]
```

Parameters

Parameter	Description
enable	Enable or disable whether a trap is sent for the specific event Type: Boolean (true/false)
repetitions	Repetitions on trap sending times between 0 - 10, optional field Type: A number with no fractional part (integer)
repetitions-delay	Wait time (in seconds) between sending each trap, optional field Type: A number with no fractional part (integer)
severity	Trap hazardous level, optional field, severity of the trap between 1 - 4 Type: A number with no fractional part (integer)
threshold	The mathematical value associated with the thresholds Type: A number with no fractional part (integer)
trap-name	Trap event name Options: trap-name

Example

```
set snmp traps trap-name interface-disconnected enable true severity 15
repetitions 15 repetitions-delay 15 threshold 15
```

set snmp traps

Description

Configures an existing SNMP trap receiver.

Syntax

```
set snmp traps receiver <receiver> version { v2 [ community <community>
] | v3 [ user <user> ] }
```

Parameters

Parameter	Description
community	Community name of the receivers trap, public is default for version2 users Type: A string of alphanumeric characters without space between them
receiver	Receivers IP address that the trap associated with Type: IP address
user	SNMP version3 Defined user
version	SNMP Version, options are: v2 or v3 Type: Press TAB to see available options

Example

```
set snmp traps receiver 192.168.1.1 version v2 community word
```

show snmp traps

Description

Shows SNMP traps status.

Syntax

```
show snmp traps status
```

Parameters

Parameter	Description
n/a	

Example

```
show snmp traps status
```

delete snmp traps-receivers

Description

Deletes all configured SNMP trap receivers.

Syntax

```
delete snmp traps-receivers all
```

Parameters

Parameter	Description
n/a	

Example

```
delete snmp traps-receivers all
```

show snmp traps receivers

Description

Shows all SNMP trap receivers.

Syntax

```
show snmp traps receivers
```

Parameters

Parameter	Description
n/a	

Example

```
show snmp traps receivers
```

show snmp traps enabled-traps

Description

Shows all SNMP traps.

Syntax

```
show snmp traps enabled-traps
```

Parameters

Parameter	Description
n/a	

Example

```
show snmp traps enabled-traps
```

snmp user

delete snmp user

Description

Deletes a configured SNMP user by name.

Syntax

```
delete snmp user <user-name>
```

Parameters

Parameter	Description
user-name	version3 user name Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces

Example

```
delete snmp user admin
```

set snmp user

Description

Configures an existing SNMP user.

Syntax

```
set snmp user <user-name> security-level { true [ auth-pass-type <auth-
pass-type> ] [ auth-pass-phrase <auth-pass-phrase> ] [ privacy-pass-
type <privacy-pass-type> ] [ privacy-pass-phrase <privacy-pass-phrase>
] | false [ auth-pass-type <auth-pass-type> ] [ auth-pass-phrase <auth-
pass-phrase> ] }
```

Parameters

Parameter	Description
auth-pass-phrase	Authentication password for the SNMP version3 user Type: A string that contains alphanumeric and special characters
auth-pass-type	Authentication protocol type for the version3 user, options are: MD5 or SHA1 Options: MD5, SHA1
privacy-pass-phrase	Privacy password chosen by the version3 user in case privacy is set Type: A string that contains alphanumeric and special characters
privacy-pass-type	Privacy protocol type for the version3 user, options are: AES or DES Options: AES, DES
security-level	Does Privacy protocol for this version3 user was set in the security level Type: Boolean (true/false)
user-name	version3 user name Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces

Example

```
set snmp user admin security-level true auth-pass-type MD5 auth-pass-
phrase a(&7Ba privacy-pass-type AES privacy-pass-phrase a(&7Ba
```

show snmp user

Description

Shows the configuration of SNMP user.

Syntax

```
show snmp user <user-name>
```

Parameters

Parameter	Description
user-name	version3 user name Type: A string that contains (0-9, a-z, - . @) up to 64 characters without spaces

Example

```
show snmp user admin
```

show snmp users

Description

Shows the configuration of all SNMP users.

Syntax

```
show snmp users
```

Parameters

Parameter	Description
n/a	

Example

```
show snmp users
```

delete snmp users

Description

Deletes all configured SNMP users.

Syntax

```
delete snmp users all
```

Parameters

Parameter	Description
n/a	

Example

```
delete snmp users all
```

show software version

Description

Shows the version of the current software.

Syntax

```
show software-version | ver
```

Parameters

Parameter	Description
n/a	

Example

```
show software-version
```

Output

Success shows the software version of the appliance. Failure shows an appropriate error message.

ssl-inspection advanced-settings

set ssl-inspection advanced-settings

Description

Configure advanced settings for SSL Inspection.

Syntax

```
set ssl-inspection advanced-settings [ bypass-well-known-update-
services <bypass-well-known-update-services> ] [ validate-crl
<validate-crl> ] [ validate-cert-expiration <validate-cert-expiration>
] [ validate-unreachable-crl <validate-unreachable-crl> ] [ track-
validation-errors <track-validation-errors> ] [ retrieve-intermediate-
ca-certificate <retrieve-intermediate-ca-certificate> ] [ log-empty-
ssl-connections <log-empty-ssl-connections> ] [ additional-https-ports
<additional-https-ports> ] [ validate-untrusted-certificates <validate-
untrusted-certificates>]
```

Parameters

Parameter	Description
additional-https-ports	Additional HTTPS ports for ssl inspection (a comma separated list ofports/ranges) Type: Port range
bypass-well-known-update-services	Bypass HTTPS Inspection of traffic to well known software update services Type: Boolean (true/false)
log-empty-ssl-connections	Log connections that were terminated by the client before data was sent - might indicate the client did not install CA certificate Type: Boolean (true/false)
retrieve-intermediate-ca-certificate	Indicates if the SSL inspection mechanism will perform it's validations on all intermidate CA certificates in the certificate chain Type: Boolean (true/false)
track-validation-errors	Choose if the SSL Inspection validations are tracked Options: none, log, alert
validate-cert-expiration	Indicates if the SSL inspection mechanism will drop connections that present an expired certificate Type: Boolean (true/false)

Parameter	Description
validate-crl	Indicates if the SSL inspection mechanism will drop connections that present a revoked certificate Type: Boolean (true/false)
validate-unreachable-crl	Indicates if the SSL inspection mechanism will drop connections that present a certificate with an unreachable CRL Type: Boolean (true/false)
validate-untrusted-certificates	Indicates if the SSL inspection mechanism will drop connections that present an untrusted server certificate Type: Boolean (true/false)

Example

```
set ssl-inspection advanced-settings bypass-well-known-update-services
true validate-crl true validate-cert-expiration true validate-
unreachable-crl true track-validation-errors none retrieve-
intermediate-ca-certificate true log-empty-ssl-connections true
additional-https-ports 8080-8090 validate-untrusted-certificates true
```

show ssl-inspection advanced-settings

Description

Show advanced settings for SSL Inspection.

Syntax

```
show ssl-inspection advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show ssl-inspection advanced-settings
```

ssl-inspection exception

add ssl-inspection exception

Description

Add a new exception to bypass SSL Inspection policy for specific traffic.

Syntax

```
add ssl-inspection exception [ source <source> ] [ source-negate
<source-negate> ] [ destination <destination> ] [ destination-negate
<destination-negate> ] [ service <service> ] [ service-negate <service-
negate> ] [ { [ category-name <category-name> ] | [ category-id
<category-id> ] } ] [ category-negate <category-negate> ] [ comment
<comment> ] [ track <track> ] [ disabled <disabled> ]
```

Parameters

Parameter	Description
category-id	Application or custom application name
category-name	Application or custom application name
category-negate	If true, the category is all traffic except what is defined in the category field Type: Boolean (true/false)
comment	Description of the rule Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
destination	Network object that is the target of the connection
destination-negate	If true, the destination is all traffic except what is defined in the destination field Type: Boolean (true/false)
disabled	Indicates if the exception is disabled Type: Boolean (true/false)
service	The network service object that the exception should match to
service-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)
source	Network object or user group that initiates the connection
source-negate	If true, the source is all traffic except what is defined in the source field Type: Boolean (true/false)

Parameter	Description
track	The action taken when there is a match on the rule Options: none, log, alert

Example

```
add ssl-inspection exception source TEXT source-negate true destination
TEXT destination-negate true service TEXT service-negate true category-
name TEXT category-negate true comment This is a comment. track none
disabled true
```

delete ssl-inspection exception

Delete an existing SSL Inspection policy exception.

delete ssl-inspection exception

Description

Delete an existing SSL Inspection policy exception.

Syntax

```
delete ssl-inspection exception position <position>
```

Parameters

Parameter	Description
position	The index of exception Type: Decimal number

Example

```
delete ssl-inspection exception position 2
```

delete ssl-inspection exception

Description

Delete an existing SSL Inspection policy exception.

Syntax

```
delete ssl-inspection exception all
```

Parameters

Parameter	Description
n/a	

Example

```
delete ssl-inspection exception all
```

set ssl-inspection exception

Description

Configure an existing SSL Inspection policy exception.

Syntax

```
set ssl-inspection exception position  <position> [ source <source>
] [ source-negate <source-negate> ] [ destination <destination> ] [
destination-negate <destination-negate> ] [ service <service> ] [
service-negate <service-negate> ] [ { [ category-name <category-name> ] |
[ category-id <category-id> ] } ] [ category-negate <category-negate> ] [
comment <comment> ] [ track <track> ] [ disabled <disabled> ]
```

Parameters

Parameter	Description
category-id	Application or custom application name
category-name	Application or custom application name
category-negate	If true, the category is all traffic except what is defined in the category field Type: Boolean (true/false)
comment	Description of the rule Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
destination	Network object that is the target of the connection
destination-negate	If true, the destination is all traffic except what is defined in the destination field Type: Boolean (true/false)
disabled	Indicates if the exception is disabled Type: Boolean (true/false)
position	The index of exception Type: Decimal number
service	The network service object that the exception should match to

Parameter	Description
service-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)
source	Network object or user group that initiates the connection
source-negate	If true, the source is all traffic except what is defined in the source field Type: Boolean (true/false)
track	The action taken when there is a match on the rule Options: none, log, alert

Example

```
set ssl-inspection exception position 2 source TEXT source-negate true
destination TEXT destination-negate true service TEXT service-negate
true category-name TEXT category-negate true comment "This is a
comment." track none disabled true
```

show ssl-inspection exception

Description

Show the configuration of a specific SSL Inspection policy exception.

Syntax

```
show ssl-inspection exception position <position> position <position>
```

Parameters

Parameter	Description
position	The index of exception Type: Decimal number

Example

```
show ssl-inspection exception position 2 position 2
```

show ssl-inspection exceptions

Description

Show all configured SSL Inspection policy exceptions.

Syntax

```
show ssl-inspection exceptions position <position>
```

Parameters

Parameter	Description
position	The index of exception Type: Decimal number

Example

```
show ssl-inspection exceptions position 2
```

ssl-inspection policy

set ssl-inspection policy

Description

Configure SSL Inspection policy.

Syntax

```
set ssl-inspection policy [ mode <mode> ] [ log-policy-bypass-traffic
<log-policy-bypass-traffic> ] [ log-inspected-traffic <log-inspected-
traffic> ] [ bypass-health-category-traffic <bypass-health-category-
traffic> ] [ bypass-government-and-military-category-traffic <bypass-
government-and-military-category-] [ bypass-banking-category-traffic
<bypass-banking-category-traffic>] [ bypass-other-categories-traffic
<bypass-other-categories-traffic> ] [ bypass-streaming-category-traffic
<bypass-streaming-category-traffic> ] [ bypass-trusted-wireless-ssl-
inspection <bypass-trusted-wireless-ssl-inspection> ] [ bypass-
untrusted-wireless-ssl-inspection <bypass-untrusted-wireless-ssl-
inspection> ] [ bypass-well-known-update-services <bypass-well-known-
update-services> ]
```

Parameters

Parameter	Description
bypass-banking-category-traffic	Bypass banking category traffic Type: Boolean (true/false)
bypass-government-and-military-category-traffic	Bypass government category traffic Type: Boolean (true/false)
bypass-health-category-traffic	Bypass health category traffic Type: Boolean (true/false)
bypass-other-categories-traffic	Bypass other categories traffic Type: Boolean (true/false)
bypass-streaming-category-traffic	Bypass streaming category traffic Type: Boolean (true/false)
bypass-trusted-wireless-ssl-inspection	Bypass SSL inspection on trusted wireless networks Type: Boolean (true/false)
bypass-untrusted-wireless-ssl-inspection	Bypass SSL inspection on untrusted wireless networks Type: Boolean (true/false)

Parameter	Description
bypass-well-known-update-services	Bypass HTTPS Inspection of traffic to well known software update services Type: Boolean (true/false)
log-inspected-traffic	Generates an SSL inspection log. You can see the logs of the security policy that is enforced on SSL traffic without enabling this feature. Type: Boolean (true/false)
log-policy-bypass-traffic	Generate an SSL bypass log for SSL traffic that was not inspected by SSL inspection Type: Boolean (true/false)
mode	Indicates if SSL inspection feature is active Type: Boolean (true/false)

Example

```
set ssl-inspection policy mode true log-policy-bypass-traffic true log-inspected-traffic true bypass-health-category-traffic true bypass-government-and-military-category-traffic true bypass-banking-category-traffic true bypass-other-categories-traffic true bypass-streaming-category-traffic true bypass-trusted-wireless-ssl-inspection true bypass-untrusted-wireless-ssl-inspection true bypass-well-known-update-services true
```

set ssl-inspection policy https-categorization-only-mode

Description

Allow URL filtering for HTTPS sites and applications based on server's certificate without activating SSL traffic inspection.

Syntax

```
set ssl-inspection policy https-categorization-only-mode { on }
```

Parameters

Parameter	Description
https-categorization-only-mode	HTTPS categorization only cane be enabled via HTTPS service Type: Boolean (true/false)

Example

```
set ssl-inspection policy https-categorization-only-mode true
```

set ssl-inspection policy inspect-https-protocol

Description

Enable SSL Inspection policy to inspect HTTPS protocol. **Note**- SSL Inspection must be enabled first.

Syntax

```
set ssl-inspection policy inspect-https-protocol { true | false }
```

Parameters

Parameter	Description
true/false	true - Enabled false - Disabled

Example

```
set ssl-inspection policy inspect-https-protocol true
```

set ssl-inspection policy inspect-imaps-protocol

Description

Enable SSL Inspection policy to inspect IMAPS protocol. **Note**- SSL Inspection must be enabled first.

Syntax

```
set ssl-inspection policy inspect-imaps-protocol { true | false }
```

Parameters

Parameter	Description
true/false	true - Enabled false - Disabled

Example

```
set ssl-inspection policy inspect-imaps-protocol true
```

show ssl-inspection policy

Description

Show SSL Inspection policy.

Syntax

```
show ssl-inspection policy
```

Parameters

Parameter	Description
n/a	

Example

```
show ssl-inspection policy
```

delete ssl-network-extender

Description

Forces a manual deletion of the SSL network extender, thus forcing the gateway to re-download the latest version of the extender from the cloud.

Syntax

```
delete ssl-network-extender
```

Parameters

Parameter	Description
n/a	

Example

```
delete ssl-network-extender
```

static-route

add static-route

Description

Adds a new manually configured routing rule.

Syntax

```
add static-route [ source <source> ] [ service <service> ] [
destination <destination> ] [ nexthop gateway { logical <logical> |
ipv4-address <ipv4-address> } ] [ metric <metric> ]
```

Parameters

Parameter	Description
destination	IP address and subnet length of the destination of the packet in the format IP/subnet. e.g. 192.168.0.0/16 Type: An IP address with a mask length
metric	Metric Type: A number with no fractional part (integer)
service	Route service name Type: String
source	IP address and subnet length of the source of the packet in the format IP/subnet. e.g. 192.168.1.0/24 Type: An IP address with a mask length

Example

```
add static-route source 172.15.47.0/24 service TEXT destination
172.15.47.0/24 nexthop gateway logical My_Network metric 10
```

set static-route

Description

Configures an existing manually configured route rule.

Syntax

```
set static-route <id> [ source <source> ] [ service <service> ] [
destination <destination> ] [ nexthop gateway { logical <logical> |
```

```
ipv4-address <ipv4-address> } ] [ metric <metric> ] [ disabled <disabled>
]
```

Parameters

Parameter	Description
destination	IP address and subnet length of the destination of the packet in the format IP/subnet. e.g. 192.168.0.0/16 Type: An IP address with a mask length
disabled	Is rule disabled Type: Boolean (true/false)
id	id Type: A number with no fractional part (integer)
metric	Metric Type: A number with no fractional part (integer)
service	Route service name Type: String
source	IP address and subnet length of the source of the packet in the format IP/subnet. e.g. 192.168.1.0/24 Type: An IP address with a mask length

Example

```
set static-route 15 source 172.15.47.0/24 service TEXT destination
172.15.47.0/24 nexthop gateway logical My_Network metric 15 disabled
true
```

delete static-route

Description

Deletes a manually defined routing rule.

Syntax

```
delete static-route <id>
```

Parameters

Parameter	Description
id	The rule order as shown in "show static-routes" Type: A number with no fractional part (integer)

Example

```
delete static-route 3
```

delete static-routes

Description

Deletes all manually defined static routing rules.

Syntax

```
delete static-routes
```

Parameters

Parameter	Description
n/a	

Example

```
delete static-routes
```

show static-routes

Description

Shows all static routes.

Syntax

```
show static-routes
```

Parameters

Parameter	Description
n/a	

Example

```
show static-routes
```

streaming-engine-settings

set streaming-engine-settings

Configures the streaming engine settings.

set streaming-engine-settings

Description

Configures the streaming engine settings.

Syntax

```
set streaming-engine-settings [ tcp-block-out-of-win-mon-only <tcp-block-out-of-win-mon-only> ] [ tcp-block-out-of-win-track <tcp-block-out-of-win-track> ] [ tcp-block-retrans-err-mon-only <tcp-block-retrans-err-mon-only> ] [ tcp-block-retrans-err-track <tcp-block-retrans-err-track> ] [ tcp-block-syn-retrans-mon-only <tcp-block-syn-retrans-mon-only> ] [ tcp-block-syn-retrans-track <tcp-block-syn-retrans-track> ] [ tcp-block-urg-bit-mon-only <tcp-block-urg-bit-mon-only> ] [ tcp-block-urg-bit-track <tcp-block-urg-bit-track> ] [ tcp-hold-timeout-mon-only <tcp-hold-timeout-mon-only> ] [ tcp-hold-timeout-track <tcp-hold-timeout-track> ] [ tcp-invalid-checksum-mon-only <tcp-invalid-checksum-mon-only> ] [ tcp-invalid-checksum-track <tcp-invalid-checksum-track> ] [ tcp-segment-limit-mon-only <tcp-segment-limit-mon-only> ] [ tcp-segment-limit-track <tcp-segment-limit-track>
```

Parameters

Parameter	Description
tcp-block-out-of-win-mon-only	TCP Out of Sequence activation mode Options: prevent, detect
tcp-block-out-of-win-track	TCP Out of Sequence tracking Options: none, log, alert
tcp-block-retrans-err-mon-only	TCP Invalid Retransmission activation mode Options: prevent, detect
tcp-block-retrans-err-track	TCP Invalid Retransmission tracking Options: none, log, alert
tcp-block-syn-retrans-mon- only	TCP SYN Modified Retransmission activation mode Options: prevent, detect
tcp-block-syn-retrans-track	TCP SYN Modified Retransmission tracking Options: none, log, alert
tcp-block-urg-bit-mon-only	TCP Urgent Data Enforcement activation mode Options: prevent, detect

Parameter	Description
tcp-block-urg-bit-track	TCP Urgent Data Enforcement tracking Options: none, log, alert
tcp-hold-timeout-mon-only	Stream Inspection Timeout activation mode Options: prevent, detect
tcp-hold-timeout-track	Stream Inspection Timeout tracking Options: none, log, alert
tcp-invalid-checksum- mon-only	TCP Invalid Checksum activation mode Options: prevent, detect
tcp-invalid-checksum-track	TCP Invalid Checksum tracking Options: none, log, alert
tcp-segment-limit-mon-only	TCP Segment Limit Enforcement activation mode Options: prevent, detect
tcp-segment-limit-track	TCP Segment Limit Enforcement tracking Options: none, log, alert

Example

```
set streaming-engine-settings tcp-block-out-of-win-mon-only prevent
tcp-block-out-of-win-track none tcp-block-retrans-err-mon-only prevent
tcp-block-retrans-err-track none tcp-block-syn-retrans-mon-only prevent
tcp-block-syn-retrans-track none tcp-block-urg-bit-mon-only prevent
tcp-block-urg-bit-track none tcp-hold-timeout-mon-only prevent tcp-
hold-timeout-track none tcp-invalid-checksum-mon-only prevent tcp-
invalid-checksum-track none tcp-segment-limit-mon-only prevent tcp-
segment-limit-track none
```

set streaming-engine-settings

Description

Configures the streaming engine settings.

Syntax

```
set streaming-engine-settings advanced-settings tcp-streaming-engine-
setting-form [ tcp-block-urg-bit-track <tcp-block-urg-bit-track> ] [
tcp-block-retrans-err-track <tcp-block-retrans-err-track> ] [ tcp-
block-syn-retrans-track <tcp-block-syn-retrans-track> ] [ tcp-invalid-
checksum-track <tcp-invalid-checksum-track> ] [ tcp-block-out-of-win-
mon-only <tcp-block-out-of-win-mon-only> ] [ tcp-block-out-of-win-track
<tcp-block-out-of-win-track> ] [ tcp-block-retrans-err-mon-only <tcp-
block-retrans-err-mon-only> ] [ tcp-block-syn-retrans-mon-only <tcp-
block-syn-retrans-mon-only>] [ tcp-invalid-checksum-mon-only <tcp-
invalid-checksum-mon-only> ] [ tcp-segment-limit-track <tcp-segment-
limit-track> ] [ tcp-block-urg-bit-mon-only <tcp-block-urg-bit-mon-
only> ] [ tcp-segment-limit-mon-only <tcp-segment-limit-mon-only> ] [
tcp-hold-timeout-mon-only <tcp-hold-timeout-mon-only> ] [ tcp-hold-
timeout-track <tcp-hold-timeout-track>]
```

Parameters

Parameter	Description
n/a	

Example

```
set streaming-engine-settings advanced-settings tcp-streaming-engine-
setting-form tcp-block-urg-bit-track none tcp-block-retrans-err-track
none tcp-block-syn-retrans-track none tcp-invalid-checksum-track none
tcp-block-out-of-win-mon-only prevent tcp-block-out-of-win-track none
tcp-block-retrans-err-mon-only prevent tcp-block-syn-retrans-mon-only
prevent tcp-invalid-checksum-mon-only prevent tcp-segment-limit-track
none tcp-block-urg-bit-mon-only prevent tcp-segment-limit-mon-only
prevent tcp-hold-timeout-mon-only prevent tcp-hold-timeout-track none
```

show streaming-engine-settings

Shows streaming engine settings.

show streaming-engine-settings

Description

Shows streaming engine settings.

Syntax

```
show streaming-engine-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show streaming-engine-settings
```

show streaming-engine-settings

Description

Shows streaming engine advanced settings.

Syntax

```
show streaming-engine-settings advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show streaming-engine-settings advanced-settings
```

switch

add switch

Description

Adds a new Port-based VLAN switch object. The physical LAN ports can take part in a "switch" object which passes traffic between those ports in the hardware level (traffic doesn't undergo inspection as it is not routed between those ports). In essence the "switch" combines physical LAN ports into a single network.

Syntax

```
add switch name <name>
```

Parameters

Parameter	Description
name	Name Type: A switch name should be LAN[1-8]_Switch

Example

```
add switch name LAN2_Switch
```

delete switch

Description

Deletes a defined port-based VLAN switch object by name.

Syntax

```
delete switch <name>
```

Parameters

Parameter	Description
name	Name Type: A switch name should be LAN[1-8]_Switch

Example

```
delete switch LAN2_Switch
```

set switch

Configures an existing port-based VLAN (switch).

set switch

Description

Add a physical port to an existing port-based VLAN (switch).

Syntax

```
set switch <name> add port <port>
```

Parameters

Parameter	Description
name	Name Type: A switch name should be LAN[1-8]_Switch
port	Name

Example

```
set switch LAN2_Switch add port LAN4
```

set switch

Description

Removes a physical port from an existing port-based VLAN (switch).

Syntax

```
set switch <name> remove port <port>
```

Parameters

Parameter	Description
name	Name Type: A switch name should be LAN[1-8]_Switch
port	Name

Example

```
set switch LAN2_Switch remove port LAN4
```

show switch

Shows port-based VLAN (switch) configuration.

show switch

Description

Shows port-based VLAN (switch) configuration.

Syntax

```
show switch <name>
```

Parameters

Parameter	Description
name	Name Type: A switch name should be LAN[1-8]_Switch

Example

```
show switch LAN2_Switch
```

show switch

Description

Shows ports within a configured port-based VLAN (switch) configuration.

Syntax

```
show switch <name> ports
```

Parameters

Parameter	Description
name	Name Type: A switch name should be LAN[1-8]_Switch

Example

```
show switch LAN2_Switch ports
```

show switches

Description

Shows all port-based VLANs (switches).

Syntax

```
show switches
```

Parameters

Parameter	Description
n/a	

Example

```
show switches
```

syslog-server

add syslog-server

Description

Adds a new external syslog server. The appliance can send its syslog information to multiple syslog servers and can also be configured to relay its security logs to external syslog servers.

Syntax

```
add syslog-server ipv4-address <ipv4-address> [ port <port> ] [ enabled
<enabled> ] name <name> [ sent-logs <sent-logs> ]
```

Parameters

Parameter	Description
enabled	Determine if an external System Log Server is active Type: Boolean (true/false)
ipv4-address	The desired external System Log Server IP address Type: IP address
name	System Log Server name Type: A string of alphanumeric characters with space between them
port	Port in the external System Log Server that receives the logs (default is 514) Type: Port number
sent-logs	Determine which logs types will be sent to the System Log Server Options: system-logs, security-logs, system-and-security-logs

Example

```
add syslog-server ipv4-address 192.168.1.1 port 8080 enabled true name
several words sent-logs system-logs
```

delete syslog-server

Deletes a configured external syslog server.

delete syslog-server

Description

Deletes a configured external syslog server by IP address.

Syntax

```
delete syslog-server ipv4-address <ipv4-address>
```

Parameters

Parameter	Description
ipv4-address	The desired external System Log Server IP address Type: IP address

Example

```
delete syslog-server ipv4-address 192.168.1.1
```

delete syslog-server

Description

Deletes a configured external syslog server by name.

Syntax

```
delete syslog-server name <name>
```

Parameters

Parameter	Description
name	System Log Server name Type: A string of alphanumeric characters with space between them

Example

```
delete syslog-server name syslog_server_name
```

set syslog-server

Configure an existing syslog server's settings.

set syslog-server

Description

Configure an existing syslog server's settings by IP address.

Syntax

```
set syslog-server ipv4-address <ipv4-address> [ ipv4-address <ipv4-
address>
```

```
] [ enabled <enabled> ] [ name <name> ] [ port <port> ] [ sent-logs
<sent-logs> ]
```

Parameters

Parameter	Description
enabled	Determine if an external System Log Server is active Type: Boolean (true/false)
ipv4-address	The desired external System Log Server IP address Type: IP address
name	System Log Server name Type: A string of alphanumeric characters with space between them
port	Port in the external System Log Server that receives the logs (default is 514) Type: Port number
sent-logs	Determine which logs types will be sent to the System Log Server Options: system-logs, security-logs, system-and-security-logs

Example

```
set syslog-server ipv4-address 192.168.1.1 ipv4-address 192.168.1.1
enabled true name several words port 8080 sent-logs system-logs
```

set syslog-server

Description

Configure an existing syslog server's settings by name.

Syntax

```
set syslog-server name <name> [ ipv4-address <ipv4-address> ] [ enabled
<enabled> ] [ name <name> ] [ port <port> ] [ sent-logs <sent-logs> ]
```

Parameters

Parameter	Description
enabled	Determine if an external System Log Server is active Type: Boolean (true/false)
ipv4-address	The desired external System Log Server IP address Type: IP address
name	System Log Server name Type: A string of alphanumeric characters with space between them
port	Port in the external System Log Server that receives the logs (default is 514) Type: Port number
sent-logs	Determine which logs types will be sent to the System Log Server Options: system-logs, security-logs, system-and-security-logs

Example

```
set syslog-server name several words ipv4-address 192.168.1.1 enabled
true name several words port 8080 sent-logs system-logs
```

show syslog-server

Shows configuration of external syslog servers.

show syslog-server

Description

Shows configuration of an external syslog server by IP address.

Syntax

```
show syslog-server ipv4-address <ipv4-address>
```

Parameters

Parameter	Description
ipv4-address	The desired external System Log Server IP address Type: IP address

Example

```
show syslog-server ipv4-address 192.168.1.1
```

show syslog-server

Description

Shows configuration of an external syslog server by name.

Syntax

```
show syslog-server name <name>
```

Parameters

Parameter	Description
name	System Log Server name Type: A string of alphanumeric characters with space between them

Example

```
show syslog-server name several words
```

show syslog-server all

Description

Shows configuration of all external syslog servers.

Syntax

```
show syslog-server all
```

Parameters

Parameter	Description
n/a	

Example

```
show syslog-server all
```

system-settings

Relevant commands for system settings.

show system-settings is-custom-branding

Description

Shows whether white labeling has been enabled and the appliance has been customized with a particular brand.

Syntax

```
show system-settings is-custom-branding
```

Parameters

Parameter	Description
n/a	

Example

```
show system-settings is-custom-branding
```

traceroute-max-ttl

Description

The maximal value for TTL field for a packet to be considered as a traceroute

Syntax

```
set stateful_inspection advanced-settings traceroute-max-ttl <value>
```

Parameters

Parameter	Description
value	Integer between 0 and 64. Default: 29

Example

```
set stateful_inspection advanced-settings traceroute-max-ttl 0
```

threat-prevention-advanced

set threat-prevention-advanced

Description

Configures advanced settings for Threat Prevention blades.

Syntax

```
set threat-prevention-advanced advanced-settings file-inspection-size-
kb <file-inspection-size-kb>
```

Parameters

Parameter	Description
n/a	

Example

```
set threat-prevention-advanced advanced-settings file-inspection-size-
kb 15000
```

show threat-prevention-advanced

Description

Shows advanced settings for the Threat Prevention blades.

Syntax

```
show threat-prevention-advanced advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention-advanced advanced-settings
```

threat-prevention anti-bot

set threat-prevention anti-bot engine

Description

Configures the engine settings of the <tp_bot> blade.

Syntax

```
set threat-prevention anti-bot engine [ malicious-activity <malicious-
activity> ] [ reputation-domains <reputation-domains> ] [ reputation-
ips <reputation-ips> ] [ reputation-urls <reputation-urls> ] [ unusual-
activity <unusual-activity>]
```

Parameters

Parameter	Description
malicious-activity	Indicates if the action upon detecting malicious activity will be according to the policy settings or a manually configured specific action Options: ask, prevent, detect, inactive, policy-action
reputation-domains	Indicates if the action upon detecting attempted access to domains with a bad reputation will be according to the policy or a manually configured specific action Options: ask, prevent, detect, inactive, policy-action
reputation-ips	Indicates if the action upon detecting attempted access to IP addresses with a bad reputation will be according to the policy or a manually configured specific action Options: ask, prevent, detect, inactive, policy-action
reputation-urls	Indicates if the action upon detecting attempted access to URLs with a bad reputation will be according to the policy or a manually configured specific action Options: ask, prevent, detect, inactive, policy-action
unusual-activity	Indicates if the action upon detecting unusual activity will be according to the policy or a manually configured specific action Options: ask, prevent, detect, inactive, policy-action

Example

```
set threat-prevention anti-bot engine malicious-activity ask
reputation-domains ask reputation-ips ask reputation-urls ask unusual-
activity ask
```

show threat-prevention anti-bot engine

Description

Shows the engine settings of the Anti-Bot blade.

Syntax

```
show threat-prevention anti-bot engine
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention anti-bot engine
```

set threat-prevention anti-bot policy

Configures the policy of the Anti-Bot blade.

set threat-prevention anti-bot policy

Description

Configures the policy of the Anti-Bot blade.

Syntax

```
set threat-prevention anti-bot policy [ mode <mode> ] [ detect-mode
<detect-mode> ]
```

Parameters

Parameter	Description
detect-mode	Indicates if the Anti-Bot blade is set to 'Detect Only' mode Type: Boolean (true/false)
mode	Indicates if the Anti-Bot blade is active Type: Boolean (true/false)

Example

```
set threat-prevention anti-bot policy mode true detect-mode true
```

set threat-prevention anti-bot policy

Description

Configures advanced settings of the Anti-Bot blade.

Syntax

```
set threat-prevention anti-bot policy advanced-settings res-class-mode
<res-class-mode>
```

Parameters

Parameter	Description
n/a	

Example

```
set threat-prevention anti-bot policy advanced-settings res-class-mode
rs-hold
```

show threat-prevention anti-bot policy

Shows the policy of the Anti-Bot blade.

show threat-prevention anti-bot policy

Description

Shows the policy of the Anti-Bot blade.

Syntax

```
show threat-prevention anti-bot policy
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention anti-bot policy
```

show threat-prevention anti-bot policy

Description

Shows the advanced settings of the Anti-Bot blade.

Syntax

```
show threat-prevention anti-bot policy advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention anti-bot policy advanced-settings
```

set threat-prevention anti-bot user-check ask

Description

Configures a customizable "ask" message shown to users upon match on browser based traffic.

Syntax

```
set threat-prevention anti-bot user-check ask [ body <body> ] [
activity-text <activity-text> ] [ fallback-action <fallback-action> ] [
frequency <frequency> ] [ subject <subject> ] [ title <title> ] [
reason-displayed <reason-displayed> ]
```

Parameters

Parameter	Description
activity-text	This text appears next to the 'ignore warning' checkbox of an Anti-Bot 'Ask' user message Type: A string that contains only printable characters
body	The informative text that appears in the Anti-Bot 'Ask' user message Type: A string that contains only printable characters
fallback-action	Indicates the action to take when an 'Ask' user message cannot be displayed Options: block, accept
frequency	Indicates how often is the Anti-Bot 'Ask' user message is being presented to the same user Options: day, week, month
reason-displayed	Indicates if the user must enter a reason for ignoring this message in a designated text dialog Type: Boolean (true/false)
subject	The subject of an Anti-Bot 'Ask' user message Type: A string that contains only printable characters
title	The title of an Anti-Bot 'Ask' user message Type: A string that contains only printable characters

Example

```
set threat-prevention anti-bot user-check ask body My Network activity-
text My Network fallback-action block frequency day subject My Network
title My Network reason-displayed true
```

show threat-prevention anti-bot user-check ask

Description

Shows the settings of the customizable "ask" message shown to users upon match on browser based traffic.

Syntax

```
show threat-prevention anti-bot user-check ask
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention anti-bot user-check ask
```

set threat-prevention anti-bot user-check block

Description

Configures a customizable "block" message shown to users upon match on browser based traffic.

Syntax

```
set threat-prevention anti-bot user-check block [ body <body> ] [
redirect-url <redirect-url> ] [ subject <subject> ] [ title <title> ] [
redirect-to-url <redirect-to-url> ]
```

Parameters

Parameter	Description
body	The informative text that appears in the Anti-Bot 'Block' user message Type: A string that contains only printable characters
redirect-to-url	Indicates if the user will be redirected to a custom URL in case of a 'Block' action Type: Boolean (true/false)
redirect-url	Indicates the URL to redirect the user in case of a 'Block' action if configured to do so. The URL to redirect the user in case of a 'Block' action. Redirection happens only if this functionality is turned on Type: urlWithHttp
subject	The subject of an Anti-Bot 'Block' user message Type: A string that contains only printable characters
title	The title of an Anti-Bot 'Block' user message Type: A string that contains only printable characters

Example

```
set threat-prevention anti-bot user-check block body My Network
redirect-url urlWithHttp subject My Network title My Network redirect-
to-url true
```

show threat-prevention anti-bot user-check block

Description

Shows the settings of the customizable "block" message shown to users upon Anti-Bot match on browser based traffic.

Syntax

```
show threat-prevention anti-bot user-check block
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention anti-bot user-check block
```

threat-prevention anti-virus

set threat-prevention anti-virus engine

Description

Configures the engine settings of the Anti-Virus blade

Syntax

```
set threat-prevention anti-virus engine [ urls-with-malware <urls-with-
malware> ] [ viruses <viruses> ]
```

Parameters

Parameter	Description
urls-with-malware	Indicates if the action upon detecting access to and from URLs with a bad reputation will be according to the policy or a manually configured specific action Options: ask, prevent, detect, inactive, policy-action
viruses	Indicates if the action upon detecting viruses will be according to the policy or a manually configured specific action Options: ask, prevent, detect, inactive, policy-action

Example

```
set threat-prevention anti-virus engine urls-with-malware ask viruses
ask
```

show threat-prevention anti-virus engine

Description

Shows the engine settings of the Anti-Virus blade.

Syntax

```
show threat-prevention anti-virus engine
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention anti-virus engine
```

add threat-prevention anti-virus file-type

Description

Adds a new custom file type according to extension, to be handled by the Anti-Virus file type handling mechanism. An action for the Anti-Virus blade is also configured for this new custom file type.

Syntax

```
add threat-prevention anti-virus file-type extension <extension> [
action <action> ] [ description <description> ]
```

Parameters

Parameter	Description
action	Indicates the action when the file type is detected Options: block, pass, scan
description	The file description Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
extension	File extension that represents this file type Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @

Example

```
add threat-prevention anti-virus file-type extension "This is a
comment." action block description This is a comment.
```

delete threat-prevention anti-virus file-type

Description

Deletes a manually configured custom file type according to extension.

Syntax

```
delete threat-prevention anti-virus file-type extension <extension>
```

Parameters

Parameter	Description
extension	File extension that represents this file type Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @

Example

```
delete threat-prevention anti-virus file-type extension pdf
```

set threat-prevention anti-virus file-type

Description

Configure a specific action of the Anti-Virus blade for a specific file extension.

Syntax

```
set threat-prevention anti-virus file-type extension <extension> [
action <action> ] [ description <description> ]
```

Parameters

Parameter	Description
action	Indicates the action when the file type is detected Options: block, pass, scan
description	The file description Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
extension	File extension that represents this file type Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @

Example

```
set threat-prevention anti-virus file-type extension pdf action block
description "This is a comment."
```

show threat-prevention anti-virus file-type

Description

Shows the Anti-Virus blade configuration for a specific file type.

Syntax

```
show threat-prevention anti-virus file-type extension <extension>
```

Parameters

Parameter	Description
extension	File extension that represents this file type Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @

Example

```
show threat-prevention anti-virus file-type extension pdf
```

show threat-prevention anti-virus file-types

Description

Shows the Anti-Virus blade configuration for all defined file types.

Syntax

```
show threat-prevention anti-virus file-types
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention anti-virus file-types
```

delete threat-prevention anti-virus file-type custom

Description

Deletes all manually configured custom file types.

Syntax

```
delete threat-prevention anti-virus file-type custom all
```

Parameters

Parameter	Description
n/a	

Example

```
delete threat-prevention anti-virus file-type custom all
```

set threat-prevention anti-virus policy

Configures the policy of the Anti-Virus blade.

set threat-prevention anti-virus policy

Description

Configures the policy of the Anti-Virus blade.

Syntax

```
set threat-prevention anti-virus policy [ mode <mode> ] [ detect-mod
<detect-mode> ] [ scope <scope> [ interfaces <interfaces> ] ] [
protocol-http <protocol-http> ] [ protocol-mail <protocol-mail> ] [
protocol-ftp <protocol-ftp> ] [ file-types-policy <file-types-policy> ]
```

Parameters

Parameter	Description
detect-mode	Indicates if the Anti-Virus blade is set to 'Detect Only' mode Type: Boolean (true/false)
file-types-policy	Indicates the file types that are inspected by the Anti-Virus blade: malware (known to contain malware), all (all file types), specific (configured file families) Options: malware, all-types, specific-families
interfaces	Indicates the source zones for inspected incoming files: External, External and DMZ or all interfaces Options: all, external, external-dmz
mode	Indicates if the Anti-Virus blade is active Type: Boolean (true/false)
protocol-ftp	Indicates if Anti-Virus inspection will be performed on FTP traffic Type: Boolean (true/false)
protocol-http	Indicates if Anti-Virus inspection will be performed on all configured ports of HTTP traffic Type: Boolean (true/false)
protocol-mail	Indicates if Anti-Virus inspection will be performed on mail traffic (SMTP and POP3) Type: Boolean (true/false)
scope	Indicates the source of scanned filed: Scan incoming files, or scan both incoming and outgoing files Options: incoming, incoming-and-outgoing

Example

```
set threat-prevention anti-virus policy mode true detect-mode true
scope incoming interfaces all protocol-http true protocol-mail true
protocol-ftp true file-types-policy malware
```

set threat-prevention anti-virus policy

Description

Configures advanced settings of the Anti-Virus blade.

Syntax

```
set threat-prevention anti-virus policy advanced-settings priority-scanning <priority-scanning>
```

Parameters

Parameter	Description
n/a	

Example

```
set threat-prevention anti-virus policy advanced-settings priority-scanning true
```

set threat-prevention anti-virus policy

Description

Configures advanced settings of the Anti-Virus blade.

Syntax

```
set threat-prevention anti-virus policy advanced-settings file-scan-size-kb <file-scan-size-kb>
```

Parameters

Parameter	Description
n/a	

Example

```
set threat-prevention anti-virus policy advanced-settings file-scan-size-kb 15000
```

set threat-prevention anti-virus policy

Description

Configures advanced settings of the Anti-Virus blade.

Syntax

```
set threat-prevention anti-virus policy advanced-settings max-nesting-
level <max-nesting-level>
```

Parameters

Parameter	Description
n/a	

Example

```
set threat-prevention anti-virus policy advanced-settings max-nesting-
level 2
```

set threat-prevention anti-virus policy

Description

Configures advanced settings of the Anti-Virus blade.

Syntax

```
set threat-prevention anti-virus policy advanced-settings action-when-
nesting-level-exceeded <action-when-nesting-level-exceeded>
```

Parameters

Parameter	Description
n/a	

Example

```
set threat-prevention anti-virus policy advanced-settings action-when-
nesting-level-exceeded allow
```

set threat-prevention anti-virus policy

Description

Configures advanced settings of the Anti-Virus blade.

Syntax

```
set threat-prevention anti-virus policy advanced-settings res-class-
mode <res-class-mode>
```

Parameters

Parameter	Description
n/a	

Example

```
set threat-prevention anti-virus policy advanced-settings res-class-
mode rs-hold
```

show threat-prevention anti-virus policy

Shows the policy for the Anti-Virus blade.

show threat-prevention anti-virus policy

Description

Shows the policy for the Anti-Virus blade.

Syntax

```
show threat-prevention anti-virus policy
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention anti-virus policy
```

show threat-prevention anti-virus policy

Description

Shows advanced settings for the Anti-Virus blade.

Syntax

```
show threat-prevention anti-virus policy advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention anti-virus policy advanced-settings
```

set threat-prevention anti-virus user-check ask

Description

Configures a customizable "ask" message shown to users upon match on browser based traffic.

Syntax

```
set threat-prevention anti-virus user-check ask [ body <body>] [
activity-text <activity-text> ] [ fallback-action <fallback-action> ] [
frequency <frequency> ] [ subject <subject>] [ title <title> ] [
reason-displayed <reason-displayed> ]
```

Parameters

Parameter	Description
activity-text	This text appears next to the 'ignore warning' checkbox of an Anti-Virus 'Ask' user message Type: A string that contains only printable characters
body	The informative text that appears in the Anti-Virus 'Ask' user message Type: A string that contains only printable characters
fallback-action	Indicates the action to take when an 'Ask' user message cannot be displayed Options: block, accept
frequency	Indicates how often is the Anti-Virus 'Ask' user message is being presented to the same user Options: day, week, month
reason-displayed	Indicates if the user must enter a reason for ignoring this message in a designated text dialog Type: Boolean (true/false)
subject	The subject of an Anti-Virus 'Ask' user message Type: A string that contains only printable characters
title	The title of an Anti-Virus 'Ask' user message Type: A string that contains only printable characters

Example

```
set threat-prevention anti-virus user-check ask body My Network
activity-text My Network fallback-action block frequency day subject My
Network title My Network reason-displayed true
```

show threat-prevention anti-virus user-check ask

Description

Shows the settings of the customizable "ask" message shown to users upon Anti-Virus match on browser based traffic.

Syntax

```
show threat-prevention anti-virus user-check ask
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention anti-virus user-check ask
```

set threat-prevention anti-virus user-check block

Description

Configures a customizable "block" message shown to users upon match on browser based traffic.

Syntax

```
set threat-prevention anti-virus user-check block [ body <body> ] [
redirect-url <redirect-url> ] [ subject <subject> ] [ title <title> ] [
redirect-to-url <redirect-to-url> ]
```

Parameters

Parameter	Description
body	The informative text that appears in the Anti-Virus 'Block' user message Type: A string that contains only printable characters
redirect-to-url	Indicates if the user will be redirected to a custom URL in case of a 'Block' action Type: Boolean (true/false)
redirect-url	Indicates the URL to redirect the user in case of a 'Block' action if configured to do so. The URL to redirect the user in case of a 'Block' action. Redirection happens only if this functionality is turned on Type: urlWithHttp
subject	The subject of an Anti-Virus 'Block' user message Type: A string that contains only printable characters
title	The title of an Anti-Virus 'Block' user message Type: A string that contains only printable characters

Example

```
set threat-prevention anti-virus user-check block body My Network
redirect-url urlWithHttp subject My Network title My Network redirect-
to-url true
```

show threat-prevention anti-virus user-check block

Description

Shows the settings of the customizable "block" message shown to users upon Anti-Virus match on browser based traffic.

Syntax

```
show threat-prevention anti-virus user-check block
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention anti-virus user-check block
```

threat-prevention exception

add threat-prevention exception

Description

Adds a new exception rule for Threat Preventionmalware protection.

Syntax

```
add threat-prevention exception [ destination <destination> ] [ destination-
negate <destination-negate> ] [ service <service> ] [ service-negate <service-
negate> ] [ source <source> ] [ source-negate

<source-negate> ] [ { protection-name <protection-name> | [ protection-code

<protection-code> ] | [ blade <blade> ] } ] [ action <action> ] [ log <log> ] [
comment <comment> ]
```

Parameters

Parameter	Description
action	The action taken when there is a match on the rule Options: ask, prevent, detect, inactive
blade	The blade to which the exception applies: Anti-Virus, Anti-Bot or both Options: any, any-av, any-ab, any-ips
comment	Additional description for the exception Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
destination	Network object that is the target of the connection
destination-negate	If true, the destination is all traffic except what is defined in the destination field Type: Boolean (true/false)
log	The logging method used when there is a match on the rule: None - do not log, Log - Create log, Alert - log with alert Options: none, log, alert
protection-code	Indicates if the exception rule will be matched a specific IPS protection
protection-name	Indicates if the exception rule will be matched a specific IPS protection
service	Type of network service that is under exception
service-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)

Parameter	Description
source	IP address, network object or user group that the exception applies to
source negate	If true, the source is all traffic except what is defined in the source field Type: Boolean (true/false)

Example

```
add threat-prevention exception destination TEXT destination-negate true service
TEXT service-negate true source TEXT source-negate true protection-name word
action ask log none comment This is a comment.
```

delete threat-prevention exception

Description

Deletes an existing malware exception rule by name.

Syntax

```
delete threat-prevention exception name <name>
```

Parameters

Parameter	Description
name	The name of the exception Type: A string of alphanumeric characters without space between them

Example

```
delete threat-prevention exception name word
```

set threat-prevention exception

Description

Configures an existing exception rule for the Threat Prevention malware exceptions.

Syntax

```
set threat-prevention exception <position> [ destination <destination>

] [ destination-negate <destination-negate> ] [ service <service> ] [ service-
negate <service-negate> ] [ source <source> ] [ source-negate

<source-negate> ] [ { protection-name <protection-name> | [ protection-code

<protection-code> ] | [ blade <blade> ] } ] [ action <action> ] [ log <log> ] [
comment <comment> ]
```

Parameters

Parameter	Description
action	The action taken when there is a match on the rule Options: ask, prevent, detect, inactive
blade	The blade to which the exception applies: Anti-Virus, Anti-Bot or both Options: any, any-av, any-ab, any-ips
comment	Additional description for the exception Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . -: () @
destination	Network object that is the target of the connection
destination-negate	If true, the destination is all traffic except what is defined in the destination field Type: Boolean (true/false)
log	The logging method used when there is a match on the rule: None - do not log, Log - Create log, Alert - log with alert Options: none, log, alert
position	The order of the rule in comparison to other rules Type: Decimal number
protection-code	Indicates if the exception rule will be matched a specific IPS protection
protection-name	Indicates if the exception rule will be matched a specific IPS protection

Parameter	Description
service	Type of network service that is under exception
service-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)
source	IP address, network object or user group that the exception applies to
source-negate	If true, the source is all traffic except what is defined in the source field Type: Boolean (true/false)

Example

```
set threat-prevention exception 2 destination TEXT destination-negate true
service TEXT service-negate true source TEXT source-negate true protection-name
word action ask log none comment This is a comment.
```

show threat-prevention exception

Description

Shows the configuration of a specific malware exception rule by name.

Syntax

```
show threat-prevention exception name <name>
```

```
show threat-prevention exception position <position>
```

Parameters

Parameter	Description
name	The name of the exception Type: A string of alphanumeric characters without space between them
position	The order of the rule in comparison to other rules Type: Decimal number

Example

```
show threat-prevention exception name word
```

delete threat-prevention exceptions

Description

Deletes all existing malware exception rules for Anti-Virus, Anti-Bot and Threat Emulation (where applicable).

Syntax

```
delete threat-prevention exceptions all
```

Parameters

Parameter	Description
n/a	

Example

```
delete threat-prevention exceptions all
```

show threat-prevention infected-hosts

Description

Shows a list of infected hosts detected by Threat Prevention blades.

Syntax

```
show threat-prevention infected-hosts
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention infected-hosts
```

threat-prevention ips

set threat-prevention ips custom-default-policy

Description

Configures the default policy of the IPS blade.

Syntax

```
set threat-prevention ips custom-default-policy [ server-protections
<server-protections> ] [ client-protections <client-protections> ] [
disable-by-confidence-level <disable-by-confidence-level > ] [ disable-
confidence-level-below-or-equal <disable-confidence-level-below-or-
equal> ] [ disable-by-severity <disable-by-severity> ] [ disable-
severity-below-or-equal <disable-severity-below-or-equal> ] [ disable-
by-performance-impact <disable-by-performance-impact> ] [ disable-
performance-impact-above-or-equal <disable-performance-impact-above-or-
equal> ] [ disable-protocol-anomalies <disable-protocol-anomalies>]
```

Parameters

Parameter	Description
client-protections	Indicates if Client protections are active by default Type: Boolean (true/false)
disable-by-confidence-level	Indicates if protections will be deactivated if their confidence level is below or equal configured level Type: Boolean (true/false)
disable-by-performance-impact	Indicates if protections will be deactivated if their performance impact is above or equal configured level Type: Boolean (true/false)
disable-by-severity	Indicates if protections will be deactivated if their severity is below or equal configured level Type: Boolean (true/false)
disable-confidence-level-below -or-equal	If configured, protections will be deactivated according to this confidence level Options: Low, Medium-low, Medium, Medium-high, High
disable-performance-impact -above-or-equal	If configured, protections will be deactivated according to this performance impact level Options: Very-low, Low, Medium, High
disable-protocol-anomalies	Do not activate protocol anomaly detection signatures Type: Boolean (true/false)

Parameter	Description
disable-severity-below-or -equal	If configured, protections will be deactivated according to this severity level Options: Low, Medium, High, Critical
server-protections	Indicates if Server protections are active by default Type: Boolean (true/false)

Example

```
set threat-prevention ips custom-default-policy server-protections true
client-protections true disable-by-confidence-level true disable-
confidence-level-below-or-equal Low disable-by-severity true disable-
severity-below-or-equal Low disable-by-performance-impact true disable-
performance-impact-above-or-equal Very-low disable-protocol-anomalies
true
```

show threat-prevention ips custom-default-policy

Description

Shows the configuration of a custom IPS policy.

Syntax

```
show threat-prevention ips custom-default-policy
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention ips custom-default-policy
```

add threat-prevention ips network-exception

Adds a new exception rule for the IPS blade.

add threat-prevention ips network-exception

Description

Adds a new exception rule for the IPS blade. To create exceptions for specific protections use protection name.

Syntax

```
add threat-prevention ips network-exception protection-name
<protection-name> [ destination <destination> ] [ destination-negate
<destination-negate> ] [ service <service> ] [ service-negate <service-
negate> ] [ source <source> ] [ source-negate <source-negate> ] [
comment <comment> ]
```

Parameters

Parameter	Description
comment	Comment on the IPS Network exception Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
destination	Network object that is the target of the connection
destination-negate	If true, the destination is all traffic except what is defined in the destination field Type: Boolean (true/false)
protection-name	Indicates if the exception rule will be matched on all IPS protections or a specific one
service	Type of network service that is under exception
service-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)
source	Network object or user group that initiates the connection
source-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)

Example

```
add threat-prevention ips network-exception protection-name word
destination TEXT destination-negate true service TEXT service-negate
true source TEXT source-negate true comment "This is a comment."
```

add threat-prevention ips network-exception

Description

Adds a new exception rule for the IPS blade. To create exceptions for specific protections use protection code.

Syntax

```
add threat-prevention ips network-exception [ protection-code
<protection-code> ] [ destination <destination> ] [ destination-negate
<destination-negate> ] [ service <service> ] [ service-negate <service-
negate> ] [ source <source> ] [ source-negate <source-negate> ] [
comment <comment> ]
```

Parameters

Parameter	Description
comment	Comment on the IPS Network exception Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
destination	Network object that is the target of the connection
destination-negate	If true, the destination is all traffic except what is defined in the destination field Type: Boolean (true/false)
protection-code	Indicates if the exception rule will be matched on all IPS protections or a specific one
service	Type of network service that is under exception
service-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)
source	Network object or user group that initiates the connection
source-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)

Example

```
add threat-prevention ips network-exception protection-code 123435
destination TEXT destination-negate true service TEXT service-negate
true source TEXT source-negate true comment "This is a comment."
```

delete threat-prevention ips network-exception

Deletes exception rules to bypass IPS protections for specific traffic.

delete threat-prevention ips network-exception

Description

Deletes an existing exception rule for the IPS blade by position.

Syntax

```
delete threat-prevention ips network-exception position <position>
```

Parameters

Parameter	Description
position	The order of the rule in the Rule Base Type: Decimal number

Example

```
delete threat-prevention ips network-exception position 2
```

delete threat-prevention ips network-exception

Description

Deletes all existing exception rules for the IPS blade.

Syntax

```
delete threat-prevention ips network-exception all
```

Parameters

Parameter	Description
n/a	

Example

```
delete threat-prevention ips network-exception all
```

set threat-prevention ips network-exception

Configure exception rules to bypass IPS protections for specific traffic.

set threat-prevention ips network-exception

Description

Configure an existing exception rule to the IPS blade by position for a specific protection by protection ID (Code).

Syntax

```
set threat-prevention ips network-exception position <position> [
protection-code <protection-code> ] [ destination <destination> ] [
destination-negate <destination-negate> ] [ service <service> ] [
```

```
service-negate <service-negate> ] [ source <source> ] [ source-negate
<source-negate> ] [ comment <comment> ]
```

Parameters

Parameter	Description
comment	Comment on the IPS Network exception Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . -: () @
destination	Network object that is the target of the connection
destination-negate	If true, the destination is all traffic except what is defined in the destination field Type: Boolean (true/false)
position	The order of the rule in the Rule Base Type: Decimal number
protection-code	Indicates if the exception rule will be matched on all IPS protections or a specific one
service	Type of network service that is under exception
service-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)
source	Network object or user group that initiates the connection
source-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)

Example

```
set threat-prevention ips network-exception position 2 protection-code
12345678 destination TEXT destination-negate true service TEXT service-
negate true source TEXT source-negate true comment "This is a comment."
```

set threat-prevention ips network-exception

Description

Configure an existing exception rule to the IPS blade by position for a specific protection by protection name.

Syntax

```
set threat-prevention ips network-exception position <position>
protection-name <protection-name> [ destination <destination> ] [
destination-negate <destination-negate> ] [ service <service>] [
service-negate <service-negate> ] [ source <source> ] [ source-negate
<source-negate> ] [ comment <comment> ]
```

Parameters

Parameter	Description
comment	Comment on the IPS Network exception Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
destination	Network object that is the target of the connection
destination-negate	If true, the destination is all traffic except what is defined in the destination field Type: Boolean (true/false)
position	The order of the rule in the Rule Base Type: Decimal number
protection-name	Indicates if the exception rule will be matched on all IPS protections or a specific one
service	Type of network service that is under exception
service-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)
source	Network object or user group that initiates the connection
source-negate	If true, the service is everything except what is defined in the service field Type: Boolean (true/false)

Example

```
set threat-prevention ips network-exception position 2 protection-name
word destination TEXT destination-negate true service TEXT service-
negate true source TEXT source-negate true comment "This is a comment."
```

show threat-prevention ips network-exception

Description

Shows the configuration of an IPS exception rule by position

Syntax

```
show threat-prevention ips network-exception position <position>
```

Parameters

Parameter	Description
position	The order of the rule in the Rule Base Type: Decimal number

Example

```
show threat-prevention ips network-exception position 2
```

set threat-prevention ips policy

Description

Configures general settings in the policy of the IPS blade.

Syntax

```
set threat-prevention ips policy [ mode <mode> ] [ log <log> ] [
default-policy <default-policy> ] [ detect-mode <detect-mode> ]
```

Parameters

Parameter	Description
default-policy	The type of policy used for IPS - strict, typical or custom
detect-mode	Indicates if the default policy of IPS is to only logs events and not block them Type: Boolean (true/false)
log	Indicates the tracking level for IPS - none, block or alert Options: none, log, alert
mode	Indicates if IPS blade is active Type: Boolean (true/false)

Example

```
set threat-prevention ips policy mode true log none default-policy word
detect-mode true
```

show threat-prevention ips policy

Description

Shows the policy of the IPS blade.

Syntax

```
show threat-prevention ips policy
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention ips policy
```

find threat-prevention ips protection

Description

Find an IPS protection by name (or partial string) to view further details regarding it.

Syntax

```
find threat-prevention ips protection <name>
```

Parameters

Parameter	Description
name	The name of the IPS topic Type: A string of alphanumeric characters without space between them

Example

```
find threat-prevention ips protection word
```

set threat-prevention ips protection-action-override

Configures actions to override the IPS policy for a specific IPS protection.

set threat-prevention ips protection-action-override

Description

Enable/Disable an action override for a specific IPS protection by protection ID (code).

Syntax

```
set threat-prevention ips protection-action-override protection-code
<protection-code> [ action <action> ] [ track <track> ]
```

Parameters

Parameter	Description
action	Indicates the manually configured action for this protection
protection-code	The IPS topic the override belongs to. Every override belongs to a single topic Type: A number with no fractional part. Values are between 4,503,599,627,370,495 to 4,503,599,627,370,495
track	Indicates the manually configured tracking option for this protection

Example

```
set threat-prevention ips protection-action-override protection-code
12345678 action prevent track none
```

set threat-prevention ips protection-action-override

Description

Configures an action override for a specific IPS protection by name.

Syntax

```
set threat-prevention ips protection-action-override protection-name
<protection-name> [ action <action> ] [ track <track> ]
```

Parameters

Parameter	Description
action	Indicates the manually configured action for this protection
protection-name	The name of the IPS topic Type: A string of alphanumeric characters without space between them
track	Indicates the manually configured tracking option for this protection

Example

```
set threat-prevention ips protection-action-override protection-name
word action prevent track none
```

set threat-prevention ips protection-action-override

Description

Configures an action override for a specific IPS protection by protection ID (code).

Syntax

```
set threat-prevention ips protection-action-override protection-code
<protection-code> override-policy-action <override-policy-action>
```

Parameters

Parameter	Description
override-policy-action	Indicates if the action upon detection will be according to the general IPS policy or manually configured for this protection Type: Boolean (true/false)
protection-code	The IPS topic the override belongs to. Every override belongs to a single topic Type: A number with no fractional part. Values are between 4,503,599,627,370,495 to 4,503,599,627,370,495

Example

```
set threat-prevention ips protection-action-override protection-code
12345678 override-policy-action true
```

set threat-prevention ips protection-action-override

Description

Enable/Disable an action override for a specific IPS protection by name.

Syntax

```
set threat-prevention ips protection-action-override protection-name
<protection-name> override-policy-action <override-policy-action>
```

Parameters

Parameter	Description
override-policy-action	Indicates if the action upon detection will be according to the general IPS policy or manually configured for this protection Type: Boolean (true/false)
protection-name	The name of the IPS topic Type: A string of alphanumeric characters without space between them

Example

```
set threat-prevention ips protection-action-override protection-name
word override-policy-action true
```

show threat-prevention ips protection-action-override

Shows action overrides for specific IPS protections.

show threat-prevention ips protection-action-override

Description

Shows action overrides for a specific IPS protection by protection ID (code).

Syntax

```
show threat-prevention ips protection-action-override protection-code
<protection-code>
```

Parameters

Parameter	Description
protection-code	The IPS topic the override belongs to. Every override belongs to a single topic Type: A number with no fractional part. Values are between 4,503,599,627,370,495 to 4,503,599,627,370,495

Example

```
show threat-prevention ips protection-action-override protection-code
12345678
```

show threat-prevention ips protection-action-override

Description

Shows action overrides for a specific IPS protection by protection name.

Syntax

```
show threat-prevention ips protection-action-override protection-name
<protection-name>
```

Parameters

Parameter	Description
protection-name	The name of the IPS topic Type: A string of alphanumeric characters without space between them

Example

```
show threat-prevention ips protection-action-override protection-name
word
```

threat-prevention-profile

Commands relevant for the Unified Threat Prevention profile.

set threat-prevention policy

Description

Configures the policy for the Threat Prevention blades Anti-Virus, Anti-Bot and Threat Emulation (where applicable).

Syntax

```
set threat-prevention policy [ track <track> ] [ profile <profile> ]
```

```
set threat-prevention policy advanced-settings fail-mode <fail-mode>
```

```
set threat-prevention policy advanced-settings block-requests-when-the-
web-service-is-<block-requests-when-the-web-service-is-unavailable>
```

Parameters

Parameter	Description
profile	Unified policy profile
track	Tracking options for Threat Prevention protections: None - do not log, Log -Create log, Alert - log with alert Options: none, log, alert

Example

```
set threat-prevention policy high-confidence ask medium-confidence ask
low-confidence ask performance-impact low track none
```

```
set threat-prevention policy advanced-settings fail-mode allow-all-
requests
```

```
set threat-prevention policy advanced-settings block-requests-when-the-
web-service-is true
```

threat-prevention policy

Shows commands relevant to Threat Prevention policy.

set threat-prevention policy

Description

Configures the policy for the Threat Prevention blades Anti-Virus, Anti-Bot and Threat Emulation (where applicable).

Syntax

```
set threat-prevention policy [ track <track> ] [ profile <profile> ]
```

```
set threat-prevention policy advanced-settings fail-mode <fail-mode>
```

```
set threat-prevention policy advanced-settings block-requests-when-the-
web-service-is-<block-requests-when-the-web-service-is-unavailable>
```

Parameters

Parameter	Description
profile	Unified policy profile
track	Tracking options for Threat Prevention protections: None - do not log, Log -Create log, Alert - log with alert Options: none, log, alert

Example

```
set threat-prevention policy high-confidence ask medium-confidence ask
low-confidence ask performance-impact low track none
```

```
set threat-prevention policy advanced-settings fail-mode allow-all-
requests
```

```
set threat-prevention policy advanced-settings block-requests-when-the-
web-service-is true
```

show threat-prevention policy

Description

Shows the configuration for the Threat Prevention policy shared by the Anti-Bot, Anti-Virus and Threat Emulation (where applicable) blades.

Syntax

```
show threat-prevention policy
```

```
show threat-prevention policy advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention policy
```

```
show threat-prevention policy advanced-settings
```

threat-prevention threat-emulation additional-remote-emulator

add threat-prevention threat-emulation additional-remote-emulator

Description

Add a gateway to the threat emulation list of additional (private) emulation gateways.

Syntax

```
add threat-prevention threat-emulation additional-remote-emulator ip-
address <ip-address> name <name>
```

Parameters

Parameter	Description
ip-address	Remote emulation gateway IP address Type: IP address
name	Remote emulation gateway name Type: A string of alphanumeric characters with space between them

Example

```
add threat-prevention threat-emulation additional-remote-emulator ip-
address 192.168.1.1 name several words
```

delete threat-prevention threat-emulation additional-remote-emulator

Delete a gateway from the threat emulation list of additional (private) emulation gateways.

delete threat-prevention threat-emulation additional-remote-emulator

Description

Delete a gateway from the threat emulation list of additional (private) emulation gateways.

Syntax

```
delete threat-prevention threat-emulation additional-remote-emulator
ip-address <ip-address>
```

Parameters

Parameter	Description
ip-address	Remote emulation gateway IP address Type: IP address

Example

```
delete threat-prevention threat-emulation additional-remote-emulator
ip-address 192.168.1.1
```

delete threat-prevention threat-emulation additional-remote-emulator

Description

Delete a gateway from the threat emulation list of additional (private) emulation gateways.

Syntax

```
delete threat-prevention threat-emulation additional-remote-emulator
name <name>
```

Parameters

Parameter	Description
name	Remote emulation gateway name Type: A string of alphanumeric characters with space between them

Example

```
delete threat-prevention threat-emulation additional-remote-emulator
name several words
```

set threat-prevention threat-emulation additional-remote-emulator

Description

Configure a gateway as an additional (private) emulation gateway.

Syntax

```
set threat-prevention threat-emulation additional-remote-emulator name
<name> [ ip-address <ip-address> ] [ name <name> ]
```

Parameters

Parameter	Description
ip-address	Remote emulation gateway IP address Type: IP address
name	Remote emulation gateway name Type: A string of alphanumeric characters with space between them

Example

```
textset threat-prevention threat-emulation additional-remote-emulator
name several words ip-address 192.168.1.1 name several words
```

show threat-prevention threat-emulation additional-remote-emulator

Show all gateways that are configured as additional (private) emulation gateways.

show threat-prevention threat-emulation additional-remote-emulator

Description

Show all gateways that are configured as additional (private) emulation gateways.

Syntax

```
show threat-prevention threat-emulation additional-remote-emulator
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention threat-emulation additional-remote-emulator
```

show threat-prevention threat-emulation additional-remote-emulator

Description

Show all gateways that are configured as additional (private) emulation gateways.

Syntax

```
show threat-prevention threat-emulation additional-remote-emulator name
<name>
```

Parameters

Parameter	Description
name	Remote emulation gateway name Type: A string of alphanumeric characters with space between them

Example

```
show threat-prevention threat-emulation additional-remote-emulator name
several words
```

set threat-prevention threat-emulation file-types-revert-actions-to-default

Description

Reverts all actions on specific file types to their default value in the factory settings.

Syntax

```
set threat-prevention threat-emulation file-types-revert-actions-to-default
```

Parameters

Parameter	Description
n/a	

Example

```
set threat-prevention threat-emulation file-types-revert-actions-to-default
```

threat-prevention threat-emulation

set threat-prevention threat-emulation file-type

Description

Configures an override action for a specific file type by the Threat Emulation blade (where applicable).

Syntax

```
set threat-prevention threat-emulation file-type <extension> [ action
<action> ] [ description <description> ]
```

Parameters

Parameter	Description
action	Indicates the action when the file type is detected Options: bypass, inspect
description	The file description Type: A string that contains less than 257 characters, of this set: 0-9, a-z or , . - : () @
extension	File extension that represents this file type Type: A string of alphanumeric characters without space between them

Example

```
set threat-prevention threat-emulation file-type word action bypass
description "This is a comment."
```

show threat-prevention threat-emulation file-type

Description

Shows the Threat Emulation (where applicable) configuration for a specific file type.

Syntax

```
show threat-prevention threat-emulation file-type <extension>
```

Parameters

Parameter	Description
extension	File extension that represents this file type Type: A string of alphanumeric characters without space between them

Example

```
show threat-prevention threat-emulation file-type word
```

show threat-prevention threat-emulation file-types

Description

Shows the Threat Emulation (where applicable) configuration for all specific file types.

Syntax

```
show threat-prevention threat-emulation file-types
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention threat-emulation file-types
```

set threat-prevention threat-emulation policy

Configures a policy specific to the Threat Emulation blade (where applicable).

set threat-prevention threat-emulation policy

Description

Configures policy settings for the Threat Emulation blade (where applicable).

Syntax

```
set threat-prevention threat-emulation policy [ mode <mode> ] [ detect-
mode <detect-mode> ] [ scope <scope> ] [ interfaces <interfaces>
```

```
] [ protocol-http <protocol-http> ] [ protocol-mail <protocol-mail> ] [
connection-handling-mode-http <connection-handling-mode-http> ] [
connection-handling-mode-smtp <connection-handling-mode-smtp> ]
```

Parameters

Parameter	Description
connection-handling-mode-http	Indicates the strictness mode of the Threat Emulation engine over HTTP: Back-ground - connections are allowed while the file emulation runs (if needed), Hold - connections are blocked until the file emulation is completed Options: background, hold
connection-handling-mode-smtp	Indicates the strictness mode of the Threat Emulation engine over SMTP: Back-ground - connections are allowed while the file emulation runs (if needed), Hold - connections are blocked until the file emulation is completed Options: background, hold
detect-mode	Indicates if the Threat Emulation blade is set to 'Detect Only' mode Type: Boolean (true/false)
interfaces	Indicates the source zones for inspected incoming files: External, External and DMZ or all interfaces Options: all, external, external-dmz
mode	Indicates if the Threat Emulation blade is active Type: Boolean (true/false)
protocol-http	Indicates if file emulation will be performed on all configured ports of HTTP traffic Type: Boolean (true/false)
protocol-mail	Indicates if file emulation will be performed on mail traffic (SMTP) Type: Boolean (true/false)
scope	Indicates the source of scanned file: scan incoming files, or scan both incoming and outgoing files Options: incoming, incoming-and-outgoing

Example

```
set threat-prevention threat-emulation policy mode true detect-mode
true scope incoming interfaces all protocol-http true protocol-mail
true connection-handling-mode-http background connection-handling-mode-
smtp background
```

set threat-prevention threat-emulation policy

Description

Configures advanced settings for the Threat Emulation blade (where applicable).

Syntax

```
set threat-prevention threat-emulation policy advanced-settings
connection-handling-mode-smtp <connection-handling-mode-smtp>
```

Parameters

Parameter	Description
n/a	

Example

```
set threat-prevention threat-emulation policy advanced-settings
connection-handling-mode-smtp background
```

show threat-prevention threat-emulation policy

Shows the policy of the Threat Emulation policy.

show threat-prevention threat-emulation policy

Description

Shows the policy of the Threat Emulation policy.

Syntax

```
show threat-prevention threat-emulation policy
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention threat-emulation policy
```

show threat-prevention threat-emulation policy

Description

Shows advanced settings of the Threat Emulation policy.

Syntax

```
show threat-prevention threat-emulation policy advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention threat-emulation policy advanced-settings
```

threat-prevention whitelist

add threat-prevention whitelist mail

Description

Adds a new excluded mail addresses for the Threat Emulation blade (where applicable).

Syntax

```
add threat-prevention whitelist mail email-address <email-address> [
type <type> ]
```

Parameters

Parameter	Description
email-address	The email address of the recipient or sender Type: Email address
type	The type of the email address - recipient, sender or both Options: recipient, sender, both

Example

```
add threat-prevention whitelist mail email-address MyEmail@mail.com
type recipient
```

show threat-prevention whitelist files

Description

Shows the list of whitelist files (md5sum) for the Threat Prevention blades.

Syntax

```
show threat-prevention whitelist files
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention whitelist files
```

delete threat-prevention whitelist mail

Description

Deletes an excluded mail address for the Threat Emulation blade (where applicable).

Syntax

```
delete threat-prevention whitelist mail <email-address>
```

Parameters

Parameter	Description
email-address	The email address of the recipient or sender Type: Email address

Example

```
delete threat-prevention whitelist mail MyEmail@mail.com
```

set threat-prevention whitelist mail

Description

Configures excluded mail addresses for the Threat Emulation blade (where applicable).

Syntax

```
set threat-prevention whitelist mail <email-address>type <type>
```

Parameters

Parameter	Description
email-address	The email address of the recipient or sender Type: Email address
type	The type of the email address - recipient, sender or both Options: recipient, sender, both

Example

```
set threat-prevention whitelist mail MyEmail@mail.com type recipient
```

show threat-prevention whitelist mail

Description

Shows the setting for a whitelist email address set for the Threat Prevention blades.

Syntax

```
show threat-prevention whitelist mail <email-address>
```

Parameters

Parameter	Description
email-address	The email address of the recipient or sender Type: Email address

Example

```
show threat-prevention whitelist mail MyEmail@mail.com
```

delete threat-prevention whitelist mails

Description

Deletes all excluded mail addresses for the Threat Emulation blade (where applicable).

Syntax

```
delete threat-prevention whitelist mails all
```

Parameters

Parameter	Description
n/a	

Example

```
delete threat-prevention whitelist mails all
```

show threat-prevention whitelist mails

Description

Shows the whitelist email addresses set for the Threat Prevention blades.

Syntax

```
show threat-prevention whitelist mails
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention whitelist mails
```

add threat-prevention whitelist type-file

Description

Adds a new excluded file for Threat Prevention blades according to md5.

Syntax

```
add threat-prevention whitelist type-file md5 <md5>
```

Parameters

Parameter	Description
md5	MD5 encryption for the file in the whitelist Type: MD5 checksum of a file. Contains only [a-f] and [0-9] characters and of exact length of 32

Example

```
add threat-prevention whitelist type-file md5
d41d8cd98f00b204e9800998ecf8427e
```

delete threat-prevention whitelist type-file

Deletes excluded files for Threat Prevention blades.

delete threat-prevention whitelist type-file

Description

Removes an excluded file for Threat Prevention blades by md5.

Syntax

```
delete threat-prevention whitelist type-file md5 <md5>
```

Parameters

Parameter	Description
md5	MD5 encryption for the file in the whitelist Type: MD5 checksum of a file. Contains only [a-f] and [0-9] characters and of exact length of 32

Example

```
delete threat-prevention whitelist type-file md5
d41d8cd98f00b204e9800998ecf8427e
```

delete threat-prevention whitelist type-file

Description

Removes all excluded files for Threat Prevention blades.

Syntax

```
delete threat-prevention whitelist type-file all
```

Parameters

Parameter	Description
n/a	

Example

```
delete threat-prevention whitelist type-file all
```

add threat-prevention whitelist type-url

Description

Adds a new excluded URL for Threat Prevention blades.

Syntax

```
add threat-prevention whitelist type-url url <url>
```

Parameters

Parameter	Description
url	URL Type: URL

Example

```
add threat-prevention whitelist type-url url
http://somehost.example.com
```

delete threat-prevention whitelist type-url

Deletes excluded URLs for Threat Prevention blades.

delete threat-prevention whitelist type-url

Description

Removes an excluded URL for Threat Prevention blades.

Syntax

```
delete threat-prevention whitelist type-url url <url>
```

Parameters

Parameter	Description
url	URL Type: URL

Example

```
delete threat-prevention whitelist type-url url
http://somehost.example.com
```

delete threat-prevention whitelist type-url

Description

Removes all excluded URLs for Threat Prevention blades.

Syntax

```
delete threat-prevention whitelist type-url all
```

Parameters

Parameter	Description
n/a	

Example

```
delete threat-prevention whitelist type-url all
```

show threat-prevention whitelist urls

Description

Shows the whitelist URLs set for the Threat Prevention blades.

Syntax

```
show threat-prevention whitelist urls
```

Parameters

Parameter	Description
n/a	

Example

```
show threat-prevention whitelist urls
```

ui-settings

set ui-settings

Configures customizations that can be done for the administration portal.

set ui-settings

Description

Configure a custom logo that will appear in the administration portal. The logo can be reached through a URL.

Syntax

```
set ui-settings [ use-custom-webui-logo <use-custom-webui-logo> ] [
custom-webui-logo-url <custom-webui-logo-url> ]
```

Parameters

Parameter	Description
custom-webui-logo-url	Clicking the company logo in the web interface opens this URL Type: urlWithHttp
use-custom-webui-logo	The company logo is displayed on the appliance's web interface and on its login page. The customized logo should follow the size restrictions in order to be displayed properly. Type: Boolean (true/false)

Example

```
set ui-settings use-custom-webui-logo true custom-webui-logo-url
urlWithHttp
```

set ui-settings

Description

Configures customizations that can be done for the administration portal.

Syntax

```
set ui-settings advanced-settings AboutConfigCustomLogos [ custom-webui-logo-url <custom-webui-logo-url> ] [ use-custom-webui-logo <use-custom-webui-logo> ]
```

Parameters

Parameter	Description
n/a	

Example

```
set ui-settings advanced-settings AboutConfigCustomLogos custom-webui-logo-url urlWithHttp use-custom-webui-logo true
```

show ui-settings

Shows web interface settings and customizations.

show ui-settings

Description

Shows web interface settings and customizations.

Syntax

```
show ui-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show ui-settings
```

show ui-settings

Description

Shows web Interface advanced settings.

Syntax

```
show ui-settings advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show ui-settings advanced-settings
```

usb-modem-advanced

add usb-modem-advanced

Description

Add a USB modem advanced entry.

Syntax

```
add usb-modem-advanced field-name <field-name> field-value <field-
value>is-any-device <is-any-device> vendor-id <vendor-id> product-id
<product-id>
```

Parameters

Parameter	Description
field-name	Name Type: A string that contains [a-z], [A-Z], [0-9], '_'
field-value	Value Type: A string that contains [a-z], [A-Z], [0-9], '_', '.', ',', '-', '/', '@', '+', ',', ':', '='
is-any-device	Does paramter apply to all devices Type: Boolean (true/false)
product-id	Product ID Type: A hexadecimal string
vendor-id	Vendor ID Type: A hexadecimal string

Example

```
add usb-modem-advanced field-name usb_advanced_config_name field-value
usb_advanced_config_value is-any-device true vendor-id 7AA1 product-id
7AA1
```

delete usb-modem-advanced

Description

Delete an existing USB modem advanced entry.

Syntax

```
delete usb-modem-advanced <id>
```

Parameters

Parameter	Description
id	id Type: A number with no fractional part (integer)

Example

```
delete usb-modem-advanced -1000000
```

delete usb-modem-advanced-all

Description

Delete all existing USB modem advanced entries.

Syntax

```
delete usb-modem-advanced-all
```

Parameters

Parameter	Description
n/a	

Example

```
delete usb-modem-advanced-all
```

set usb-modem-advanced

Description

Configure a USB modem advanced entry.

Syntax

```
set usb-modem-advanced <id> [ field-name <field-name> ] [ field-value
<field-value> ] [ is-any-device <is-any-device> ] [ vendor-id <vendor-
id> ] [ product-id <product-id>
```

Parameters

Parameter	Description
field-name	Name Type: A string that contains [a-z], [A-Z], [0-9], '_'
field-value	Value Type: A string that contains [a-z], [A-Z], [0-9], '_', '.', ',', '-', '/', '@', '+', ',', ':', '='
id	id Type: A number with no fractional part (integer)
is-any-device	Does parameter apply to all devices Type: Boolean (true/false)
product-id	Product ID Type: A hexadecimal string
vendor-id	Vendor ID Type: A hexa decimal string

Example

```
set usb-modem-advanced -1000000 field-name usb_advanced_config_name
field-value usb_advanced_config_value is-any-device true vendor-id 7AA1
product-id 7AA1
```

show usb-modem-advanced

Description

Show existing USB modem advanced entries.

Syntax

```
show usb-modem-advanced
```

Parameters

Parameter	Description
n/a	

Example

```
show usb-modem-advanced
```

show usb-modem-advanced table

Description

Show the existing USB modem advanced entries in a table.

Syntax

```
show usb-modem-advanced table
```

Parameters

Parameter	Description
n/a	

Example

```
show usb-modem-advanced table
```

usb-modem-info

show usb-modem-info

Description

Show existing USB modem information.

Syntax

```
show usb-modem-info
```

Parameters

Parameter	Description
n/a	

Example

```
show usb-modem-info
```

show usb-modem-info-table

Description

Show existing USB modem information in a table.

Syntax

```
show usb-modem-info table
```

Parameters

Parameter	Description
n/a	

Example

```
show usb-modem-info table
```

usb-modem-watchdog

set usb-modem-watchdog

Configures the internet probing (if probing is enabled) to automatically detect and fix 3G/4G internet connectivity problems.

set usb-modem-watchdog

Description

Configures the internet probing (if probing is enabled) to automatically detect and fix 3G/4G internet connectivity problems.

Syntax

```
set usb-modem-watchdog advanced-settings interval <interval>
```

Parameters

Parameter	Description
n/a	

Example

```
set usb-modem-watchdog advanced-settings interval 10
```

set usb-modem-watchdog

Description

Configures the internet probing (if probing is enabled) to automatically detect and fix 3G/4G internet connectivity problems.

Syntax

```
set usb-modem-watchdog advanced-settings mode <mode>
```

Parameters

Parameter	Description
n/a	

Example

```
set usb-modem-watchdog advanced-settings mode off
```

show usb-modem-watchdog

Description

Shows configuration for additional health monitoring functionality to USB modems.

Syntax

```
show usb-modem-watchdog advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show usb-modem-watchdog advanced-settings
```

set used-ad-group

Configures settings of a user group defined in the AD server.

set used-ad-group

Description

Adds a bookmark to be shown in the SNX landing page to user group defined in the AD server. This is relevant only if the user group is defined with VPN remote access privileges.

Syntax

```
set used-ad-group name <name>add bookmark label <bookmark label>
```

Parameters

Parameter	Description
bookmark label	Text for the bookmark in the SSL Network Extender portal
name	Group name Type: Active Directory group name

Example

```
set used-ad-group name my AD group add bookmark label myLabel
```

set used-ad-group

Description

Removes a bookmark from being shown in the SNX landing page to user group defined in the AD server. This is relevant only if the user group is defined with VPN remote access privileges.

Syntax

```
set used-ad-group name <name> remove bookmark label <bookmark label>
```

Parameters

Parameter	Description
bookmark label	Text for the bookmark in the SSL Network Extender portal
name	Group name Type: Active Directory group name

Example

```
set used-ad-group name my AD group remove bookmark label myLabel
```

user-awareness

set user-awareness

Configures settings for the User Awareness blade.

set user-awareness

Description

Configures the activation mode and user identification methods for the User Awareness blade.

Syntax

```
set user-awareness [ mode <mode>] [ ad-queries-mode <ad-queries-mode> ]
[ browser-based-authentication-mode <browser-based-authentication-mode>
]
```

Parameters

Parameter	Description
ad-queries-mode	Indicates if User Awareness seamlessly queries the AD (Active Directory) servers to get user information Type: Boolean (true/false)
browser-based-authentication- mode	Indicates if User Awareness uses a portal to identify locally defined users or as a backup to other identification methods Type: Boolean (true/false)
mode	User Awareness mode - true for on, false for off Type: Boolean (true/false)

Example

```
set user-awareness mode true ad-queries-mode true browser-based-
authentication-mode true
```

set user-awareness

Description

Configures advanced settings for the User Awareness blade.

Syntax

```
set user-awareness advanced-settings association-timeout <association-timeout>
```

Parameters

Parameter	Description
n/a	

Example

```
set user-awareness advanced-settings association-timeout 10
```

set user-awareness

Description

Configures advanced settings for the User Awareness blade.

Syntax

```
set user-awareness advanced-settings assume-single-user <assume-single-user>
```

Parameters

Parameter	Description
n/a	

Example

```
set user-awareness advanced-settings assume-single-user true
```

set user-awareness browser-based-authentication

Configures settings for browser-based authentication (captive portal) by the User Awareness blade.

set user-awareness browser-based-authentication

Description

Configures settings for browser-based authentication (captive portal) by the User Awareness blade.

Syntax

```
set user-awareness browser-based-authentication [ redirect-upon-
destinations { manually-defined [ redirect-upon-destination-internet
<redirect-upon-destination-internet> ] [ redirect-upon-destinations-
net-objs <redirect-upon-destinations-net-objs> ] | all } ] [ block-
unauthenticated-non-web-traffic <block-unauthenticated-non-web-traffic>
] [ require-user-agreement <require-user-agreement> ] [ agreement-text
<agreement-text> ] [ portal-address <portal-address> ] [ session-
timeout <session-timeout> ] [ log-out-on-portal-close <log-out-on-
portal-close> ]
```

Parameters

Parameter	Description
agreement-text	The conditions shown to the users to agree to Type: A string that contains only printable characters
block-unauthenticated- non-web-traffic	When true, users using non-HTTP traffic are forced to login first through Browser-Based Authentication Type: Boolean (true/false)
log-out-on-portal-close	When true, the user is forced to keep the portal window open to remain logged in Type: Boolean (true/false)
portal-address	Use the auto option unless you want to redirect to a manually configured URL Type: String Enter "<auto>" for default
redirect-upon-destination-internet	When choosing redirect to manually defined destinations - indicates if the destinations include the internet (external interfaces) Type: Boolean (true/false)
redirect-upon-destinations	Browser based authentication will only be shown to unidentified users on traffic to these configured destinations Type: Press TAB to see available options

Parameter	Description
redirect-upon-destinations-net-objs	When choosing redirect to manually defined destinations - indicates if the destinations include a manual list of network objects Type: Boolean (true/false)
require-user-agreement	Indicates if users must agree to the legal conditions Type: Boolean (true/false)
session-timeout	Session timeout duration, in minutes, for browser-based authentication Type: A number with no fractional part (integer) Units should be entered in minutes

Example

```
set user-awareness browser-based-authentication redirect-upon-
destinations manually-defined redirect-upon-destination-internet true
redirect-upon-destinations-net-o true block-unauthenticated-non-web-
traffic true require-user-agreement true agreement-text My Network
portal-address TEXT session-timeout 10 log-out-on-portal-close true
```

set user-awareness browser-based-authentication

Description

Configures network objects to be used in the User Awareness blade.

Syntax

```
set user-awareness browser-based-authentication add net-obj <net-obj>
```

Parameters

Parameter	Description
net-obj	Network object name

Example

```
set user-awareness browser-based-authentication add net-obj TEXT
```

set user-awareness browser-based-authentication

Description

Configures network objects to be used in the User Awareness blade.

Syntax

```
set user-awareness browser-based-authentication remove net-obj <net-
obj>
```

Parameters

Parameter	Description
net-obj	Network object name

Example

```
set user-awareness browser-based-authentication remove net-obj TEXT
```

set user-awareness browser-based-authentication

Description

Configures network objects to be used in the User Awareness blade.

Syntax

```
set user-awareness browser-based-authentication remove-all net-objs
```

Parameters

Parameter	Description
n/a	

Example

```
set user-awareness browser-based-authentication remove-all net-objs
```

show user-awareness

Shows the configuration of the User Awareness blade.

show user-awareness

Description

Shows the configuration of the User Awareness blade.

Syntax

```
show user-awareness
```

Parameters

Parameter	Description
n/a	

Example

```
show user-awareness
```

show user-awareness

Description

Shows advanced settings of the User Awareness blade.

Syntax

```
show user-awareness advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show user-awareness advanced-settings
```

show user-awareness browser-based-authentication

Description

Shows the browser-based authentication configuration of the User Awareness blade.

Syntax

```
show user-awareness browser-based-authentication
```

Parameters

Parameter	Description
n/a	

Example

```
show user-awareness browser-based-authentication
```

set user-management

Description

Configures advanced settings for the User Awareness blade.

Syntax

```
set user-management advanced-settings auto-delete-expired-local-users
<auto-delete-expired-local-users>
```

Parameters

Parameter	Description
n/a	

Example

```
set user-management advanced-settings auto-delete-expired-local-users
true
```

show upgrade log

Description

Shows upgrade log files.

Syntax

```
show upgrade-log
```

Parameters

Parameter	Description
n/a	

Example

```
show upgrade-log
```

show used-ad-group bookmarks

Description

Show bookmarks configured to a user group defined in AD.

Syntax

```
show used-ad-group bookmarks name <name>
```

Parameters

Parameter	Description
name	Group name Type: Active Directory group name

Example

```
show used-ad-group bookmarks name my AD group
```

upgrade from usb or tftp server

Description

Upgrades the software image from a file on a USB drive or TFTP server.

Syntax

```
upgrade from {usb [file <usb_file>]|tftp server <server> filename
<tftp_file>}
```

Parameters

Parameter	Description
`usb_file`	Name of software image file on USB drive.
`server`	Host name or IP address of TFTP server.
`tftp_file`	Name of software image file on TFTP server.

Example

```
upgrade from tftp server my-tftp-server filename my-new-software
```

vpn

vpn

The vpncommand manages the VPN driver and helps to debug the VPN.

Managing the VPN Driver

Description

Installs the VPN kernel (vpnk) and connects to the firewall kernel (fwk), attaching the VPN driver to the Firewall driver.

Syntax

```
vpn drv <on|off>
```

Parameters

Parameter	Description
`on|off`	Starts or stops the VPN kernel

Return Value

0 on success, 1 on failure

Example

```
vpn drv on
```

Output

Success shows OK. Failure shows an appropriate error message.

Launching TunnelUtil Tool

Description

Launches the VPN TunnelUtil tool to:

- List IKE and IPSec SAs
- Delete IKE and IPSec SAs

Syntax

```
vpn tunnelutil
```

Parameters

Parameter	Description
n/a	

Return Value

0 on success, 1 on failure

Example

```
vpn tunnelutil
```

Output

Success launches VPN TunnelUtil tool. Failure shows an appropriate error message.

Debugging VPN

Description

Contains multiple utilities for troubleshooting VPN issues.

Syntax

```
vpn debug {on [TOPIC=level]|off} [ikeon|ikeoff] [trunc [TOPIC=level]]
[mon|moff]
```

Parameters

Parameter	Description
`on|off`	Writes debugging information t $FWDIR/log/sfwd.elg
`[TOPIC=level]`	Sets level of debugging for a particular topic. This argument can only be used afte on o trunc .
`ikeon|ikeoff`	Writes IKE packet information int $FWDIR/log/ike.elg
`trunc`	Writes bot sfwd.elg an ike.elg , but first clears the files
`mon|moff`	Writes raw IKE packets t $FWDIR/log/ikemonitor.snoop

Return Value

0
on success,

1
on failure

Example

```
vpn debug on
```

delete vpn

Description

Delete a configured Virtual Tunnel Interface (VTI) by tunnel ID.

Syntax

```
delete vpn tunnel <tunnel>
```

Parameters

Parameter	Description
tunnel	A number identifying the Virtual Tunnel Interface (VTI) Type: A number with no fractional part (integer)

Example

```
delete vpn tunnel 12
```

set vpn

Configures existing remote VPN sites.

set vpn

Description

Configures existing remote VPN sites.

Syntax

```
set vpn site <site> [ enabled <enabled> ] [ remote-site-enc-dom-type
<remote-site-enc-dom-type> ] [ enc-profile <enc-profile> ] [ phase1-
reneg-interval <phase1-reneg-interval> ] [ phase2-reneg-interval
<phase2-reneg-interval> ] [ enable-perfect-forward-secrecy { true [
phase2-dh <phase2-dh> ] | false } ] [ is-check-point-site { true [
enable-permanent-vpn-tunnel <enable-permanent-vpn-tunnel> ] | false } ]
[ disable-nat <disable-nat> ] [ aggressive-mode-enabled { true
aggressive-mode-DH-group <aggressive-mode-DH-group> | false } ] [ {
aggressive-mode-enable-peer-id { true aggressive-mode-peer-id-type
<aggressive-mode-peer-id-type> aggressive-mode-peer-id <aggressive-
mode-peer-id> | false } | aggressive-mode-enable-gateway-id { true
aggressive-mode-gateway-id-type <aggressive-mode-gateway-id-type>
aggressive-mode-gateway-id <aggressive-mode-gateway-id> | false } } ] [
enc-method <enc-method> ] [ use-trusted-ca <use-trusted-ca> ] [ match-
cert-ip <match-cert-ip> ] [ match-cert-dn { true match-cert-dn-string
<match-cert-dn-string> | false } ] [ match-cert-e-mail { true match-
cert-e-mail-string <match-cert-e-mail-string> | false } ] [ link-
selection-probing-method <link-selection-probing-method> ] [ name
<name>] [ remote-site-link-selection <remote-site-link-selection> ] [
remote-site-host-name <remote-site-host-name> ] [ remote-site-ip-
address <remote-site-ip-address> ] [ is-site-behind-static-nat <is-
site-behind-static-nat> ] [ static-nat-ip <static-nat-ip> ] [ auth-
method { preshared-secret password <password> | certificate } ] [ link-
selection-primary-addr <link-selection-primary-addr>]
```

Parameters

Parameter	Description
aggressive-mode-DH-group	Determine the strength of the key when aggressive mode is enabled
aggressive-mode- enable-gateway-id	Indicates if gateway ID matching will be used. This adds a layer of security to aggressive mode Type: Boolean (true/false)
aggressive-mode- enable-peer-id	Indicates if peer ID matching will be used. This adds a layer of security to aggressive mode Type: Boolean (true/false)

Parameter	Description
aggressive-mode-enabled	Indicates if Aggressive mode, a less secure negotiation protocol compared to main mode, is used. It is less recommended if the remote site supports IPSec main mode Type: Boolean (true/false)
aggressive-mode-gateway-id	The gateway ID that will be used for matching when configured to Type: vpnAggressiveModePeerId
aggressive-mode- gateway-id-type	Indicates the type of gateway ID that will be used for matching when configured Options: domain-name, user-name
aggressive-mode-peer-id	The peer ID that will be used for matching when configured to Type: vpnAggressiveModePeerId
aggressive-mode-peer-id-type	Indicates the type of peer ID that will be used for matching when configured Options: domain-name, user-name
auth-method	Indicates the type of authentication used when connecting to the remote site Type: Press TAB to see available options
disable-nat	Disable NAT for traffic to/from the remote site. Useful when one of the internal networks contains a server Type: Boolean (true/false)
enable-perfect-forward-secrecy	Ensures that a session key will not be compromised if one of the (long-term) private keys is compromised in the future. Type: Boolean (true/false)
enable-permanent-vpn-tunnel	VPN Tunnels are constantly kept active and as a result, make it easier to recognize malfunctions and connectivity problems Type: Boolean (true/false)
enabled	Indicates whether or not the remote site is enabled Type: Boolean (true/false)
enc-method	Indicates which encryption method is used Options: ike-v1, ike-v2, prefer-ike-v2
enc-profile	Encryption profile (one of predefined profiles or custom) Type: virtual
is-check-point-site	Enable if the remote site is connected through a Check Point Security Gateway Type: Boolean (true/false)

Parameter	Description
is-site-behind-static-nat	When connection type is IP address, this indicates if it is behind static NAT
link-selection-primary-addr	Specifies The primary IP address for the link selection Type: A string of alphanumeric characters without space between them
link-selection-probing-method	The type of probing used for link selection when multiple IP addresses are configured for the remote site Options: ongoing, one-time
match-cert-dn	Indicates if certificate matching should match the DN string in the certificate to the configured DN string Type: Boolean (true/false)
match-cert-dn-string	Indicates the configured DN string for certificate matching Type: String
match-cert-e-mail	Indicates if certificate matching should match the E-mail string in the certificate to the configured E-mail string Type: Boolean (true/false)
match-cert-e-mail-string	Indicates the configured E-mail string for certificate matching Type: Email address
match-cert-ip	Indicates if certificate matching should match IP address in the certificate to the site's IP address Type: Boolean (true/false)
name	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces
password	Preshared secret (minimum 6 characters) to be used when authentication method is configured as such Type: vpnPassword
phase1-reneg-interval	The period, in minutes, between each IKE SA renegotiation Type: A number with no fractional part (integer)
phase2-dh	Determine the strength of the key used for the IPsec (Phase 2) key exchange process. The higher the group number, the stronger and more secure the key is.
phase2-reneg-interval	The period, in seconds, between each IPSec SA renegotiation Type: A number with no fractional part (integer)

Parameter	Description
remote-site-enc-dom-type	The method of defining the remote site's encryption domain Options: manually-defined-enc-dom, route-all-traffic-to-site, route-based-vpn, enc-dom-hidden-behind-remote-site
remote-site-host-name	Indicates the remote site's host name when the link selection method is configured as such
remote-site-ip-address	Indicates the remote site's single IP address when the link selection method is configured as such
remote-site-link-selection	Indicates the method of determining the destination IP address/s of the remote site Options: ip-address, host-name, high-availability, load-sharing, connection-initiated-only-from-remote-site
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces
static-nat-ip	Indicates an external routable IP address via static NAT used by the remote site, when configured as such
use-trusted-ca	Indicates if a specific trusted CA is used for matching the remote site's certificate or all configured trusted CAs

Example

```
set vpn site site17 enabled true remote-site-enc-dom-type manually-
defined-enc-dom enc-profile custom phase1-reneg-interval 15 phase2-
reneg-interval 15 enable-perfect-forward-secrecy true phase2-dh word
is-check-point-site true enable-permanent-vpn-tunnel true disable-nat
true aggressive-mode-enabled true aggressive-mode-DH-group word
aggressive-mode-enable-peer-id true aggressive-mode-peer-id-type
domain-name aggressive-mode-peer-id vpnAggressiveModePeerId enc-method
ike-v1 use-trusted-ca TEXT match-cert-ip true match-cert-dn true match-
cert-dn-string TEXT match-cert-e-mail true match-cert-e-mail-string
MyEmail@mail.com link-selection-probing-method ongoing name site17
remote-site-link-selection ip-address remote-site-host-name myHost.com
remote-site-ip-address 192.168.1.1 is-site-behind-static-nat true
static-nat-ip 192.168.1.1 auth-method preshared-secret password
vpnPassword link-selection-primary-addr word
```

set vpn

Description

Adds network objects to the encryption domain of existing remote VPN sites.

Syntax

```
set vpn site <site> add remote-site-enc-dom-network-obj <remote-site-
enc-dom-network-obj>
```

Parameters

Parameter	Description
remote-site-enc-dom-network-obj	Network Object name
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 add remote-site-enc-dom-network-obj TEXT
```

set vpn

Description

Removes all network objects from the encyryption domain of existing remote VPN sites.

Syntax

```
set vpn site <site> remove-all remote-site-enc-dom-network-obj
```

<remote-site-enc-dom-network-obj>

Parameters

Parameter	Description
remote-site-enc-dom-network-obj	Network Object name
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 remove-all remote-site-enc-dom-network-obj TEXT
```

set vpn

Description

Removes network objects from the encryption domain of existing remote VPN sites.

Syntax

```
set vpn site <site> remove remote-site-enc-dom-network-obj <remote-site-enc-dom-network-obj>
```

Parameters

Parameter	Description
remote-site-enc-dom- network-obj	Network Object name
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 remove remote-site-enc-dom-network-obj TEXT
```

set vpn

Description

Adds IP addresses to an existing remote VPN site. This allows High Availability or Load Sharing between the remote links using the link selection functionality.

Syntax

```
set vpn site <site> add link-selection-multiple-addrs addr <link-
selection-multiple-addrs addr>
```

Parameters

Parameter	Description
link-selection-multiple- addrs addr	IP address
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 add link-selection-multiple-addrs addr 192.168.1.1
```

set vpn

Description

Removes all IP addresses from an existing remote VPN site configured with multiple links.

Syntax

```
set vpn site <site>remove-all link-selection-multiple-addrs addr <link-selection-multiple-addrs addr>
```

Parameters

Parameter	Description
link-selection-multiple- addrs addr	IP address
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 remove-all link-selection-multiple-addrs addr 192.168.1.1
```

set vpn

Description

Removes IP addresses from an existing remote VPN site. This allows High Availability or Load Sharing between the remote links using the link selection functionality.

Syntax

```
set vpn site <site> remove link-selection-multiple-addrs addr <link-
selection-multiple-addrs addr>
```

Parameters

Parameter	Description
link-selection-multiple- addrs addr	IP address
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 remove link-selection-multiple-addrs addr
192.168.1.1
```

set vpn

Description

Adds a phase 1 encryption algorithm to an existing remote VPN site configured with a custom encryption suite.

Syntax

```
set vpn site <site> add custom-enc-phase1-enc <custom-enc-phase1-enc>
```

Parameters

Parameter	Description
custom-enc-phase1-enc	Encryption algorithm preferences for phase1 in the VPN encryption algorithm, which sets the base for phase2
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 add custom-enc-phase1-enc word
```

set vpn

Description

Removes all phase 1 encryption algorithm from an existing remote VPN site configured with a custom encryption suite.

Syntax

```
set vpn site <site> remove-all custom-enc-phase1-enc <custom-enc-
phase1-enc>
```

Parameters

Parameter	Description
custom-enc-phase1-enc	Encryption algorithm preferences for phase1 in the VPN encryption algorithm, which sets the base for phase2
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 remove-all custom-enc-phase1-enc word
```

set vpn

Description

Removes a phase 1 encryption algorithm from an existing remote VPN site configured with a custom encryption suite

Syntax

```
set vpn site <site> remove custom-enc-phase1-enc <custom-enc-phase1-
enc>
```

Parameters

Parameter	Description
custom-enc-phase1-enc	Encryption algorithm preferences for phase1 in the VPN encryption algorithm, which sets the base for phase2
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 remove custom-enc-phase1-enc word
```

set vpn

Description

Adds a phase 1 authentication algorithm to an existing remote VPN site configured with a custom encryption suite.

Syntax

```
set vpn site <site> add custom-enc-phase1-auth <custom-enc-phase1-auth>
```

Parameters

Parameter	Description
custom-enc-phase1-auth	Authentication algorithm used for encryption validation
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 add custom-enc-phase1-auth word
```

set vpn

Description

Removes all phase 1 authentication algorithms from an existing remote VPN site configured with a custom encryption suite.

Syntax

```
set vpn site <site> remove-all custom-enc-phase1-auth <custom-enc-phase1-auth>
```

Parameters

Parameter	Description
custom-enc-phase1-auth	Authentication algorithm used for encryption validation
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 remove-all custom-enc-phase1-auth word
```

set vpn

Description

Removes a phase 1 authentication algorithm from an existing remote VPN site configured with a custom encryption suite.

Syntax

```
set vpn site <site> remove custom-enc-phase1-auth <custom-enc-phase1-
auth>
```

Parameters

Parameter	Description
custom-enc-phase1-auth	Authentication algorithm used for encryption validation
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 remove custom-enc-phase1-auth word
```

set vpn

Description

Adds a Diffie-Hellman group to an existing remote VPN site configured with a custom encryption suite.

Syntax

```
set vpn site <site> add custom-enc-phase1-dh-group <custom-enc-phase1-
dh-group>
```

Parameters

Parameter	Description
custom-enc-phase1-dh-group	VPN Diffie-Hellman key exchange encryption level
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 add custom-enc-phase1-dh-group word
```

set vpn

Description

Removes all Diffie-Hellman groups from an existing remote VPN site configured with a custom encryption suite.

Syntax

```
set vpn site <site> remove-all custom-enc-phase1-dh-group <custom-enc-
phase1-dh-group>
```

Parameters

Parameter	Description
custom-enc-phase1-dh-group	VPN Diffie-Hellman key exchange encryption level
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 remove-all custom-enc-phase1-dh-group word
```

set vpn

Description

Removes an Diffie-Hellman group from an existing remote VPN site configured with a custom encryption suite.

Syntax

```
set vpn site <site> remove custom-enc-phase1-dh-group <custom-enc-
phase1-dh-group>
```

Parameters

Parameter	Description
custom-enc-phase1-dh-group	VPN Diffie-Hellman key exchange encryption level
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 remove custom-enc-phase1-dh-group word
```

set vpn

Description

Adds a phase 2 encryption algorithm to an existing remote VPN site configured with a custom encryption suite.

Syntax

```
set vpn site <site> add custom-enc-phase2-enc <custom-enc-phase2-enc>
```

Parameters

Parameter	Description
custom-enc-phase2-enc	Encryption algorithm preferences for phase2 in the VPN encryption algorithm
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 add custom-enc-phase2-enc word
```

set vpn

Description

Removes all phase 2 encryption algorithms from an existing remote VPN site configured with a custom encryption suite.

Syntax

```
set vpn site <site> remove-all custom-enc-phase2-enc <custom-enc-
phase2-enc>
```

Parameters

Parameter	Description
custom-enc-phase2-enc	Encryption algorithm preferences for phase2 in the VPN encryption algorithm
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 remove-all custom-enc-phase2-enc word
```

set vpn

Description

Removes a phase 2 encryption algorithm from an existing remote VPN site configured with a custom encryption suite.

Syntax

```
set vpn site <site> remove custom-enc-phase2-enc <custom-enc-phase2-enc>
```

Parameters

Parameter	Description
custom-enc-phase2-enc	Encryption algorithm preferences for phase2 in the VPN encryption algorithm
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 remove custom-enc-phase2-enc word
```

set vpn

Description

Adds a phase 2 authentication algorithm to an existing remote VPN site configured with a custom encryption suite.

Syntax

```
set vpn site <site> add custom-enc-phase2-auth <custom-enc-phase2-auth>
```

Parameters

Parameter	Description
custom-enc-phase2-auth	Authentication algorithm used for encryption validation
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 add custom-enc-phase2-auth word
```

set vpn

Description

Removes all phase 2 authentication algorithms from an existing remote VPN site configured with a custom encryption suite.

Syntax

```
set vpn site <site> remove-all custom-enc-phase2-auth <custom-enc-
phase2-auth>
```

Parameters

Parameter	Description
custom-enc-phase2-auth	Authentication algorithm used for encryption validation
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 remove-all custom-enc-phase2-auth word
```

set vpn

Description

Removes a phase 2 authentication algorithm from an existing remote VPN site configured with a custom encryption suite.

Syntax

```
set vpn site <site> remove custom-enc-phase2-auth <custom-enc-phase2-auth>
```

Parameters

Parameter	Description
custom-enc-phase2-auth	Authentication algorithm used for encryption validation
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
set vpn site site17 remove custom-enc-phase2-auth word
```

set vpn

Description

Configures an existing Virtual Tunnel Interface (VTI) for route based VPN.

Syntax

```
set vpn tunnel <tunnel> type { unnumbered [ peer <peer> ] [ internet-
connection <internet-connection> ] | numbered [ local <local> ] [
remote <remote> ] [ peer <peer> ] }
```

Parameters

Parameter	Description
internet-connection	The local interface for unnumbered VTI
local	Enter the IP address of the interface Type: IP address
peer	Remote peer name as defined in the VPN community. You must define the two peers in the VPN community before you can define the VTI. The Peer ID is an alpha-numeric character string. Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces
remote	Defines the remote peer IPv4 address, used at the peer gateway's point-to-point virtual interface (numbered VTI only) Type: IP address
tunnel	A number identifying the Virtual Tunnel Interface (VTI) Type: A number with no fractional part (integer)
type	The type of VTI: Numbered VTI that uses a specified, static IPv4 addresses for local and remote connections, or unnumbered VTI that uses the interface and the remote peer name to get addresses Type: Press TAB to see available options

Example

```
set vpn tunnel 15 type unnumbered peer site17 internet-connection My
connection
```

show vpn

Shows VPN site to site configuration.

show vpn

Description

Shows the configuration of a remote VPN site.

Syntax

```
show vpn site <site>
```

Parameters

Parameter	Description
site	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
show vpn site site17
```

show vpn

Description

Shows the configuration of a Virtual Tunnel Interface (VTI) used for route-based VPN.

Syntax

```
show vpn tunnel <tunnel>
```

Parameters

Parameter	Description
tunnel	A number identifying the Virtual Tunnel Interface (VTI) Type: A number with no fractional part (integer)

Example

```
show vpn tunnel 12
```

vpn remote-access

set vpn remote-access

Configures settings for VPN remote access (Client to server VPN).

set vpn remote-access

Description

Configures settings for VPN remote access.

Syntax

```
set vpn remote-access [ default-access-to-lan <default-access-to-lan>
```

```
] [ mode <mode> ] [ track <track> ] [ mobile-client <mobile-client> ] [
sslvpn-client <sslvpn-client> ] [ l2tp-vpn-client <l2tp-vpn-client> ] [
l2tp-pre-shared-key <l2tp-pre-shared-key> ]
```

Parameters

Parameter	Description
default-access-to-lan	Allow traffic from Remote Access clients (by default) Options: block, accept
l2tp-pre-shared-key	L2TP Pre-Shared Key Type: A string of alphanumeric characters without space between them
l2tp-vpn-client	Enable VPN remote access clients to connect via native VPN client (L2TP) Type: Boolean (true/false)
mobile-client	Enable VPN remote access mobile clients to connect via Check Point Mobile VPN client Type: Boolean (true/false)
mode	Enable VPN Remote Access Type: Boolean (true/false)
sslvpn-client	Enable VPN remote access clients to connect via SSL VPN Type: Boolean (true/false)
track	Log traffic from Remote Access clients (by default) Options: none, log

Example

```
set vpn remote-access default-access-to-lan block mode true track none
mobile-client true sslvpn-client true l2tp-vpn-client true l2tp-pre-
shared-key word
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings enc-dns-traffic <enc-dns-traffic>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings enc-dns-traffic true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings verify-gateway-cert <verify-gateway-cert>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings verify-gateway-cert true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings update-topo-startup <update-
topo-startup>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings update-topo-startup true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings keep-alive-time <keep-alive-
time>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings keep-alive-time 15
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings endpoint-vpn-user-re-auth-timeout <endpoint-vpn-user-re-auth-timeout>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings endpoint-vpn-user-re-auth-timeout 15
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings ike-over-tcp <ike-over-tcp>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings ike-over-tcp true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings is-udp-enc-active <is-udp-enc-active>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings is-udp-enc-active true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings radius-retransmit-timeout
<radius-retransmit-timeout>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings radius-retransmit-timeout 15
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings om-method-radius <om-method-
radius>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings om-method-radius true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings snx-uninstall-on-disconnect
<snx-uninstall-on-disconnect>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings snx-uninstall-on-disconnect
ask-user
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings snx-keep-alive-timeout <snx-keep-alive-timeout>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings snx-keep-alive-timeout 15
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings snx-min-tls <snx-min-tls>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings snx-min-tls tls-1-0
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings snx-encryption-enable-3des
<snx-encryption-enable-3des>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings snx-encryption-enable-3des true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings update-topo <update-topo>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings update-topo 15
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings use-limited-auth-timeout <use-limited-auth-timeout>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings use-limited-auth-timeout true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings auth-timeout-limit <auth-
timeout-limit>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings auth-timeout-limit 15
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings om-enable-with-multiple-if <om-enable-with-multiple-if>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings om-enable-with-multiple-if true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings disconnect-enc-domain
<disconnect-enc-domain>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings disconnect-enc-domain true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings enable-back-conn <enable-back-conn>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings enable-back-conn true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings allow-update-topo <allow-
update-topo>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings allow-update-topo true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings snx-encryption-enable-rc4 <snx-encryption-enable-rc4>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings snx-encryption-enable-rc4 true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings ike-ip-comp-support <ike-ip-comp-support>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings ike-ip-comp-support true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings enc-method <enc-method>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings enc-method ike-v1
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings snx-upgrade <snx-upgrade>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings snx-upgrade ask-user
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings ike-support-crash-recovery
<ike-support-crash-recovery>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings ike-support-crash-recovery true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings allow-clear-traffic-while-disconnected <allow-clear-traffic-while-disconnected>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings allow-clear-traffic-while-disconnected true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings allow-caching-passwords-on-
client <allow-caching-passwords-on-client>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings allow-caching-passwords-on-
client true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings prevent-ip-pool-nat <prevent-ip-pool-nat>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings prevent-ip-pool-nat true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings disable-office-mode <disable-office-mode>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings disable-office-mode true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings snx-user-re-auth-timeout <snx-
user-re-auth-timeout>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings snx-user-re-auth-timeout 15
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings allow-simultaneous-login
<allow-simultaneous-login>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings allow-simultaneous-login true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings port [ visitor-mode-port
<visitor-mode-port> ] [ reserve-port-443 <reserve-port-443> ]
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings port visitor-mode-port 8080
reserve-port-443 true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings office-mode [ om-perform-antispoofing <om-perform-antispoofing> ] [ single-om-per-site <single-om-per-site> ]
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings office-mode om-perform-antispoofing true single-om-per-site true
```

set vpn remote-access

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings visitor-mode [ enable-visitor-mode-all <enable-visitor-mode-all> ] [ visitor-mode-interface <visitor-mode-interface>]
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn remote-access advanced-settings visitor-mode enable-visitor-mode-all all visitor-mode-interface 192.168.1.1
```

show vpn remote-access

Shows configuration of remote access VPN.

show vpn remote-access

Description

Shows configuration of remote access VPN.

Syntax

```
show vpn remote-access
```

Parameters

Parameter	Description
n/a	

Example

```
show vpn remote-access
```

show vpn remote-access

Description

Shows advanced settings of remote access VPN.

Syntax

```
show vpn remote-access advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show vpn remote-access advanced-settings
```

set vpn remote-access advanced

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced [ om-network-ip <om-network-ip> ] [ om-
subnet-mask <om-subnet-mask> ] [ default-route-through-this-gateway
<default-route-through-this-gateway> ] [ enc-dom <enc-dom> ] [
```

```
use-this-gateway-as-dns-server <use-this-gateway-as-dns-server> ] [ dns-
primary <dns-primary> ] [ dns-secondary <dns-secondary> ] [ dns-tertiary
<dns-tertiary> ] [ dns-domain-mode <dns-domain-mode> ] [ domain-name
<domain-name> ]
```

Parameters

Parameter	Description
default-route-through- this-gateway	Indicates if Internet traffic from connected clients will be routed first through this gateway Type: Boolean (true/false)
dns-domain-mode	Indicates if remote access clients use the domain name configured under DNS network settings of the device, or a manually configured domain name Type: Boolean (true/false)
dns-primary	Configure manually office mode first DNS Type: IP address
dns-secondary	Configure manually office mode second DNS Type: IP address
dns-tertiary	Configure manually office mode third DNS Type: IP address
domain-name	Manual configuration of the domain used by remote access clients Type: A FQDN
enc-dom	Indicates if the encryption domain for remote access clients is calculated automatically or manually configured Options: manual, auto
om-network-ip	Office Mode - Allocate IP addresses from the following network Type: Network address

Parameter	Description
om-subnet-mask	Subnet for allocating IP addresses of incoming remote access connections (Office Mode) Type: Subnet mask
use-this-gateway-as- dns-server	Indicates if the remote access clients will use this gateway as a DNS server. Applicable only when encryption domain is calculated automatically Type: Boolean (true/false)

Example

```
set vpn remote-access advanced om-network-ip 172.16.10.0 om-subnet-mask
255.255.255.0 default-route-through-this-gateway true enc-dom manual
use-this-gateway-as-dns-server true dns-primary 192.168.1.1 dns-
secondary 192.168.1.1 dns-tertiary 192.168.1.1 dns-domain-mode true
domain-name somehost.example.com
```

show vpn remote-access advanced

Description

Shows advanced settings of remote access VPN.

Syntax

```
show vpn remote-access advanced
```

Parameters

Parameter	Description
n/a	

Example

```
show vpn remote-access advanced
```

set vpn remote-access advanced enc-dom-obj manual

Configures manual encryption domain for VPN remote access users.

set vpn remote-access advanced enc-dom-obj manual

Description

Adds a network object to the manual encryption domain of VPN remote access.

Syntax

```
set vpn remote-access advanced enc-dom-obj manual add name <name>
```

Parameters

Parameter	Description
name	Network Object name

Example

```
set vpn remote-access advanced enc-dom-obj manual add name TEXT
```

set vpn remote-access advanced enc-dom-obj manual

Description

Removes a network object from the manual encryption domain of VPN remote access.

Syntax

```
set vpn remote-access advanced enc-dom-obj manual remove name <name>
```

Parameters

Parameter	Description
name	Network Object name

Example

```
set vpn remote-access advanced enc-dom-obj manual remove name TEXT
```

vpn site

add vpn site

Description

Adds a new remote VPN site for VPN site-to-site.

Syntax

```
add vpn site name <name> remote-site-link-selection { host-name remote-
site-host-name <remote-site-host-name> auth-method { preshared-secret
password <password> [ enabled <enabled> ] [ remote-site-enc-dom-type
<remote-site-enc-dom-type> ] [ enc-profile <enc-profile> ] [ phase1-
reneg-interval <phase1-reneg-interval> ] [ phase2-reneg-interval
<phase2-reneg-interval> ] [ enable-perfect-forward-secrecy { true [
phase2-dh <phase2-dh> ] | false } ] [ is-check-point-site { true [
enable-permanent-vpn-tunnel <enable-permanent-vpn-tunnel> ] | false } ]
[ disable-nat <disable-nat> ] [ aggressive-mode-enabled { true
aggressive-mode-DH-group <aggressive-mode-DH-group> [ { aggressive-
mode-enable-peer-id { true aggressive-mode-peer-id-type <aggressive-
mode-peer-id-type> aggressive-mode-peer-id <aggressive-mode-peer-id> |
false } | aggressive-mode-enable-gateway-id { true aggressive-mode-
gateway-id-type <aggressive-mode-gateway-id-type> aggressive-mode-
gateway-id <aggressive-mode-gateway-id> | false } } ] | false } ] [
enc-method <enc-method> ] [ use-trusted-ca <use-trusted-ca> ] [ match-
cert-ip <match-cert-ip> ] [ match-cert-dn { true match-cert-dn-string
<match-cert-dn-string>| false } ] [ match-cert-e-mail { true match-
cert-e-mail-string <match-cert-e-mail-string> | false } ] [ link-
selection-probing-method <link-selection-probing-method> ] |
certificate [ enabled <enabled> ] [ remote-site-enc-dom-type <remote-
site-enc-dom-type> ] [ enc-profile <enc-profile> ] [ phase1-reneg-
interval <phase1-reneg-interval> ] [ phase2-reneg-interval <phase2-
reneg-interval> ] [ enable-perfect-forward-secrecy { true [ phase2-dh
<phase2-dh> ] | false } ] [ is-check-point-site { true [ enable-
permanent-vpn-tunnel <enable-permanent-vpn-tunnel> ] | false } ] [
disable-nat <disable-nat> ] [ aggressive-mode-enabled { true
aggressive-mode-DH-group <aggressive-mode-DH-group> [ { aggressive-
mode-enable-peer-id { true aggressive-mode-peer-id-type <aggressive-
mode-peer-id-type> aggressive-mode-peer-id <aggressive-mode-peer-id> |
false } | aggressive-mode-enable-gateway-id { true aggressive-mode-
gateway-id-type <aggressive-mode-gateway-id-type> aggressive-mode-
gateway-id <aggressive-mode-gateway-id> | false } } ] | false } ] [
enc-method <enc-method> ] [ use-trusted-ca <use-trusted-ca>] [ match-
cert-ip <match-cert-ip> ] [ match-cert-dn { true match-cert-dn-string
<match-cert-dn-string> | false } ] [ match-cert-e-mail { true match-
cert-e-mail-string <match-cert-e-mail-string> | false } ] [ link-
selection-probing-method <link-selection-probing-method> ] } | ip-
address remote-site-ip-address <remote-site-ip-address> is-site-behind-
static-nat { true static-nat-ip <static-nat-ip> auth-method {
preshared-secret password <password> [ enabled <enabled> ] [ remote-
site-enc-dom-type <remote-site-enc-dom-type> ] [ enc-profile <enc-
profile> ] [ phase1-reneg-interval <phase1-reneg-interval> ] [ phase2-
reneg-interval <phase2-reneg-interval> ] [ enable-perfect-forward-
secrecy { true [ phase2-dh <phase2-dh> ] | false } ] [ is-check-point-
site { true [ enable-permanent-vpn-tunnel <enable-permanent-vpn-tunnel>
] | false } ] [ disable-nat <disable-nat> ] [ aggressive-mode-enabled {
true aggressive-mode-DH-group <aggressive-mode-DH-group> [ {
aggressive-mode-enable-peer-id { true aggressive-mode-peer-id-type
<aggressive-mode-peer-id-type> aggressive-mode-peer-id <aggressive-
mode-peer-id> | false } | aggressive-mode-enable-gateway-id { true
aggressive-mode-gateway-id-type <aggressive-mode-gateway-id-type>
aggressive-mode-gateway-id <aggressive-mode-gateway-id> | false } } ] |
false } ] [ enc-method <enc-method> ] [ use-trusted-ca <use-trusted-ca>
] [ match-cert-ip <match-cert-ip> ] [ match-cert-dn { true match-cert-
dn-string <match-cert-dn-string> | false } ] [ match-cert-e-mail { true
match-cert-e-mail-string <match-cert-e-mail-string> | false } ] [ link-
selection-probing-method <link-selection-probing-method> ] |
```

Parameters

Parameter	Description
aggressive-mode-DH-group	determine the strength of the key when aggressive mode is enabled
aggressive-mode-enable-gateway-id	Indicates if gateway ID matching will be used. This adds a layer of security to aggressive mode Type: Boolean (true/false)
aggressive-mode-enable-peer-id	Indicates if peer ID matching will be used. This adds a layer of security to aggressive mode Type: Boolean (true/false)
aggressive-mode-enabled	main mode, is used. It is less recommended if the remote site supports IPSec main mode Type: Boolean (true/false)
aggressive-mode-gateway-id	The gateway ID that will be used for matching when configured to Type: vpnAggressiveModePeerId
aggressive-mode-gateway-id-type	Indicates the type of gateway ID that will be used for matching when configured Options: domain-name, user-name
aggressive-mode-peer-id	The peer ID that will be used for matching when configured to Type: vpnAggressiveModePeerId
aggressive-mode-peer-id-type	Indicates the type of peer ID that will be used for matching when configured Options: domain-name, user-name
auth-method	Indicates the type of authentication used when connecting to the remote site Type: Press TAB to see available options
disable-nat	Disable NAT for traffic to/from the remote site. Useful when one of the internal networks contains a server Type: Boolean (true/false)
enable-perfect-forward-secrecy	Ensures that a session key will not be compromised if one of the (long-term) private keys is compromised in the future. Type: Boolean (true/false)
enable-permanent- vpn-tunnel	VPN Tunnels are constantly kept active and as a result, make it easier to recognize malfunctions and connectivity problems Type: Boolean (true/false)

Parameter	Description
enabled	Indicates whether or not the remote site is enabled Type: Boolean (true/false)
enc-method	Indicates which encryption method is used Options: ike-v1, ike-v2, prefer-ike-v2
enc-profile	Encryption profile (one of predefined profiles or custom) Type: virtual
is-check-point-site	Enable if the remote site is connected through a Check Point Security Gateway Type: Boolean (true/false)
is-site-behind-static- nat	Indicates if the remote site is behind static NAT Type: Boolean (true/false)
link-selection-multiple-addrs addr	IP address
link-selection-probing- method	The type of probing used for link selection when multiple IP addresses are configured for the remote site Options: ongoing, one-time
match-cert-dn	Indicates if certificate matching should match the DN string in the certificate to the configured DN string Type: Boolean (true/false)
match-cert-dn-string	Indicates the configured DN string for certificate matching Type: String
match-cert-e-mail	Indicates if certificate matching should match the E-mail string in the certificate to the configured E-mail string Type: Boolean (true/false)
match-cert-e-mail- string	Indicates the configured E-mail string for certificate matching Type: Email address
match-cert-ip	Indicates if certificate matching should match IP address in the certificate to the site's IP address Type: Boolean (true/false)
name	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Parameter	Description
password	Preshared secret (minimum 6 characters) to be used when authentication method is configured as such Type: vpnPassword
phase1-reneg-interval	The period, in minutes, between each IKE SA renegotiation Type: A number with no fractional part (integer)
phase2-dh	Determine the strength of the key used for the IPsec (Phase 2) key exchange process. The higher the group number, the stronger and more secure the key is.
phase2-reneg-interval	The period, in seconds, between each IPSec SA renegotiation Type: A number with no fractional part (integer)
remote-site-enc-dom- type	The method of defining the remote site's encryption domain Options: manually-defined-enc-dom, route-all-traffic-to-site, route-based-vpn, enc-dom-hidden-behind-remote-site
remote-site-host-name	Indicates the host name of the remote site Type: An IP address or host name
remote-site-ip-address	Indicates the IP address of the remote site Type: IP address
remote-site-link-selection	Indicates the method of determining the destination IP address/s of the remote site Type: Press TAB to see available options
static-nat-ip	Indicates an external routable IP address via static NAT used by the remote site Type: IP address
use-trusted-ca	Indicates if a specific trusted CA is used for matching the remote site's certificate or all configured trusted CAs

Example

```
add vpn site name site17 remote-site-link-selection host-name remote-
site-host-name myHost.com auth-method preshared-secret password
vpnPassword enabled true remote-site-enc-dom-type manually-defined-enc-
dom enc-profile custom phase1-reneg-interval 15 phase2-reneg-interval
15 enable-perfect-forward-secrecy true phase2-dh word is-check-point-
site true enable-permanent-vpn-tunnel true disable-nat true aggressive-
mode-enabled true aggressive-mode-DH-group word aggressive-mode-enable-
peer-id true aggressive-mode-peer-id-type domain-name aggressive-mode-
peer-id vpnAggressiveModePeerId enc-method ike-v1 use-trusted-ca TEXT
match-cert-ip true match-cert-dn true match-cert-dn-string TEXT match-
cert-e-mail true match-cert-e-mail-string MyEmail@mail.com link-
selection-probing-method ongoing enabled true remote-site-enc-dom-type
manually-defined-enc-dom enc-profile custom phase1-reneg-interval 15
phase2-reneg-interval 15 enable-perfect-forward-secrecy true phase2-dh
word is-check-point-site true enable-permanent-vpn-tunnel true disable-
nat true aggressive-mode-enabled true aggressive-mode-DH-group word
aggressive-mode-enable-peer-id true aggressive-mode-peer-id-type
domain-name aggressive-mode-peer-id vpnAggressiveModePeerId enc-method
ike-v1 use-trusted-ca TEXT match-cert-ip true match-cert-dn true match-
cert-dn-string TEXT match-cert-e-mail true match-cert-e-mail-string
MyEmail@mail.com link-selection-probing-method ongoing auth-method
preshared-secret password vpnPassword enabled true remote-site-enc-dom-
type manually-defined-enc-dom enc-profile custom phase1-reneg-interval
15 phase2-reneg-interval 15 enable-perfect-forward-secrecy true phase2-
dh word is-check-point-site true enable-permanent-vpn-tunnel true
disable-nat true aggressive-mode-enabled true aggressive-mode-DH-group
word aggressive-mode-enable-peer-id true aggressive-mode-peer-id-type
domain-name aggressive-mode-peer-id vpnAggressiveModePeerId enc-method
ike-v1 use-trusted-ca TEXT match-cert-ip true match-cert-dn true match-
cert-dn-string TEXT match-cert-e-mail true match-cert-e-mail-string
MyEmail@mail.com link-selection-probing-method ongoing enabled true
remote-site-enc-dom-type manually-defined-enc-dom enc-profile custom
phase1-reneg-interval 15 phase2-reneg-interval 15 enable-perfect-
forward-secrecy true phase2-dh word is-check-point-site true enable-
permanent-vpn-tunnel true disable-nat true aggressive-mode-enabled true
aggressive-mode-DH-group word aggressive-mode-enable-peer-id true
aggressive-mode-peer-id-type domain-name aggressive-mode-peer-id
vpnAggressiveModePeerId enc-method ike-v1 use-trusted-ca TEXT match-
cert-ip true match-cert-dn true match-cert-dn-string TEXT match-cert-e-
mail true match-cert-e-mail-string MyEmail@mail.com link-selection-
probing-method ongoing
```

delete vpn site

Delete VPN sites.

delete vpn site

Description

Delete an existing VPN site by name.

Syntax

```
delete vpn site name <name>
```

Parameters

Parameter	Description
name	Site name Type: A string that begins with a letter and contains up to 32 alphanumeric (0-9, a-z, _ -) characters without spaces

Example

```
delete vpn site name site17
```

delete vpn site

Description

Delete all existing VPN sites.

Syntax

```
delete vpn site all
```

Parameters

Parameter	Description
n/a	

Example

```
delete vpn site all
```

show vpn sites

Description

Show all configured remote VPN sites.

Syntax

```
show vpn sites
```

Parameters

Parameter	Description
n/a	

Example

```
show vpn sites
```

vpn site-to-site

set vpn site-to-site

Configure global settings for VPN site to site.

set vpn site-to-site

Description

Configure global settings for VPN site to site.

Syntax

```
set vpn site-to-site [ mode <mode> ] [ default-access-to-lan <default-
access-to-lan> ] [ track <track> ] [ local-encryption-domain <local-
encryption-domain> ] [ manual-source-ip-address <manual-source-ip-
address> ] [ source-ip-address-selection <source-ip-address-selection>
] [ outgoing-interface-selection <outgoing-interface-selection> ] [
use-dpd-responder-mode <use-dpd-responder-mode> ] [ tunnel-health-
monitor-mode <tunnel-health-monitor-mode>]
```

Parameters

Parameter	Description
default-access-to-lan	Allow traffic from remote sites (by default)?A? ?I Options: block, accept
local-encryption-domain	Indicates if the local encryption domain is configured manually or determined automatically using the local networks Options: auto, manual
manual-source-ip-address	A manually configured source IP address to be used (if configured to) for VPN tunnels Type: IP address
mode	Indicates whether or not VPN site to site is active Type: Boolean (true/false)
outgoing-interface-selection	Indicates the method according to which the outgoing interface selection for VPN traffic is chosen Options: routing-table, route-based-probing
source-ip-address-selection	Select whether the source IP address is chosen automatically according to the outgoing interface or manually configured Options: automatically, manually
track	The default Logging setting for traffic from remote sites Options: none, log

Parameter	Description
tunnel-health-monitor-mode	VPN tunnel monitor mechanism, can work with permanent tunnel or with DPD mode Options: tunnel-test, dpd
use-dpd-responder-mode	Once checked DPD responder mode will be enabled, otherwise permanent tunnel based on DPD mode will be enabled Type: Boolean (true/false)

Example

```
set vpn site-to-site mode true default-access-to-lan block track none
local-encryption-domain auto manual-source-ip-address 192.168.1.1
source-ip-address-selection automatically outgoing-interface-selection
routing-table use-dpd-responder-mode true tunnel-health-monitor-mode
tunnel-test
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings sync-sa-with-other-cluster-members <sync-sa-with-other-cluster-members>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings sync-sa-with-other-cluster-members 15
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings keep-dont-fragment-flag-on-
packet <keep-dont-fragment-flag-on-packet>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings keep-dont-fragment-flag-on-
packet true
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings delete-ipsec-sas-on-ikes-delete
<delete-ipsec-sas-on-ikes-delete>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings delete-ipsec-sas-on-ikes-delete
true
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings period-after-crl-not-valid
<period-after-crl-not-valid>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings period-after-crl-not-valid 2
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings log-notification-for-
administrative-actions <log-notification-for-administrative-actions>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings log-notification-for-
administrative-actions none
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings udp-encapsulation-for-firewalls-
and-proxies <udp-encapsulation-for-firewalls-and-proxies>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings udp-encapsulation-for-firewalls-
and-proxies true
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings copy-diff-serv-from-ipsec-packet
<copy-diff-serv-from-ipsec-packet>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings copy-diff-serv-from-ipsec-packet
true
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings log-vpn-successful-key-exchange
<log-vpn-successful-key-exchange>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings log-vpn-successful-key-exchange
none
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings dpd-triggers-new-ike-negotiation
<dpd-triggers-new-ike-negotiation>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings dpd-triggers-new-ike-negotiation
true
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings log-vpn-packet-handling-errors
<log-vpn-packet-handling-errors>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings log-vpn-packet-handling-errors
none
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings keep-ikesa-keys <keep-ikesa-keys>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings keep-ikesa-keys do-not-keep
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings permanent-tunnel-up-track
<permanent-tunnel-up-track>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings permanent-tunnel-up-track none
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings tunnel-test-from-internal
<tunnel-test-from-internal>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings tunnel-test-from-internal true
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings vpn-tunnel-sharing <vpn-tunnel-
sharing>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings vpn-tunnel-sharing hosts
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings vpn-configuration-and-key-
exchange-errors <vpn-configuration-and-key-exchange-errors>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings vpn-configuration-and-key-
exchange-errors none
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings reply-from-same-ip <reply-from-same-ip>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings reply-from-same-ip true
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings no-local-dns-encrypt <no-local-
dns-encrypt>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings no-local-dns-encrypt true
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings is-admin-access-agnostic <is-
admin-access-agnostic>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings is-admin-access-agnostic true
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings period-before-crl-valid <period-before-crl-valid>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings period-before-crl-valid 5
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings maximum-concurrent-vpn-tunnels
<maximum-concurrent-vpn-tunnels>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings maximum-concurrent-vpn-tunnels 5
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings limit-open-sas <limit-open-sas>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings limit-open-sas 5
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings permanent-tunnel-down-track
<permanent-tunnel-down-track>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings permanent-tunnel-down-track none
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings enable-link-selection <enable-
link-selection>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings enable-link-selection true
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings check-validity-of-ipsec-reply-
packets <check-validity-of-ipsec-reply-packets>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings check-validity-of-ipsec-reply-
packets true
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings ike-dos-protection-unknown-sites
<ike-dos-protection-unknown-sites>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings ike-dos-protection-unknown-sites
none
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings ike-dos-protection-known-sites
<ike-dos-protection-known-sites>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings ike-dos-protection-known-sites
none
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings maximum-concurrent-ike-negotiations <maximum-concurrent-ike-negotiations>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings maximum-concurrent-ike-negotiations 20
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings log-vpn-outgoing-link <log-vpn-outgoing-link>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings log-vpn-outgoing-link none
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings delete-ike-sas-from-a-dead-peer
<delete-ike-sas-from-a-dead-peer>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings delete-ike-sas-from-a-dead-peer
true
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings timeout-for-an-rdp-packet-reply
<timeout-for-an-rdp-packet-reply>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings timeout-for-an-rdp-packet-reply
15
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings perform-ike-using-cluster-ip
<perform-ike-using-cluster-ip>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings perform-ike-using-cluster-ip
true
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings reply-from-incoming-interface
<reply-from-incoming-interface>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings reply-from-incoming-interface
true
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings ike-use-largest-possible-subnets
<ike-use-largest-possible-subnets>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings ike-use-largest-possible-subnets
true
```

set vpn site-to-site

Description

Configure advanced settings for VPN site to site.

Syntax

```
set vpn site-to-site advanced-settings copy-diff-serv-to-ipsec-packet
<copy-diff-serv-to-ipsec-packet>
```

Parameters

Parameter	Description
n/a	

Example

```
set vpn site-to-site advanced-settings copy-diff-serv-to-ipsec-packet
true
```

shows vpn site-to-site

Shows configuration of site-to-site VPN.

show vpn site-to-site

Description

Shows configuration of site-to-site VPN.

Syntax

```
show vpn site-to-site
```

Parameters

Parameter	Description
n/a	

Example

```
show vpn site-to-site
```

shows vpn site-to-site

Description

Shows advanced settings of site-to-site VPN.

Syntax

```
show vpn site-to-site advanced-settings
```

Parameters

Parameter	Description
n/a	

Example

```
show vpn site-to-site advanced-settings
```

set vpn site-to-site enc-dom manual

Configures manually the local encryption domain for site-to-site VPN

set vpn site-to-site enc-dom manual

Description

Adds a network object to the local encryption domain for site-to-site VPN.

Syntax

```
set vpn site-to-site enc-dom manual add name <name>
```

Parameters

Parameter	Description
name	Network Object name

Example

```
set vpn site-to-site enc-dom manual add name TEXT
```

set vpn site-to-site enc-dom manual

Description

Removes all network objects from the local encryption domain for site-to-site VPN.

Syntax

```
set vpn site-to-site enc-dom manual remove-all name <name>
```

Parameters

Parameter	Description
name	Network Object name

Example

```
set vpn site-to-site enc-dom manual remove-all name TEXT
```

set vpn site-to-site enc-dom manual

Description

Removes a network object from the local encryption domain for site-to-site VPN.

Syntax

```
set vpn site-to-site enc-dom manual remove name <name>
```

Parameters

Parameter	Description
name	Network Object name

Example

```
set vpn site-to-site enc-dom manual remove name TEXT
```

vpn tunnel

show vpn tunnel

Description

Shows all IKE (Internet Key Exchange) and IPSec (Internet Protocol Security) SAs (Security Associations) for the VPN tunnel.

Syntax

```
show vpn-tunnel-info
```

Parameters

Parameter	Description
n/a	

Example

```
show vpn-tunnel-info
```

show vpn tunnels

Description

Shows all Virtual Tunnel Interfaces (VTIs).

Syntax

```
show vpn tunnels
```

Parameters

Parameter	Description
n/a	

Example

```
show vpn tunnels
```

wlan

delete wlan

Description

Delete an existing wireless Virtual Access Point (VAP) by SSID.

Syntax

```
delete wlan vap <vap>
```

Parameters

Parameter	Description
vap	The name of the Virtual Access Point Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
delete wlan vap My_Network
```

set wlan

Configures a virtual access point (VAP) wireless network in appliance models that contain wireless options).

set wlan

Description

Turn on/off the first wireless network (VAP) that was created.

Syntax

```
set wlan { on | off }
```

Parameters

Parameter	Description
mode	The mode of the Virtual Access Point Options: on, off

Example

```
set wlan on
```

set wlan

Description

Configures the SSID of the first wireless network that was created.

Syntax

```
set wlan ssid <ssid>
```

Parameters

Parameter	Description
ssid	Wireless network name (SSID) Type: A string that contains [A-Z], [0-9], '_', '.', '-' and space characters

Example

```
set wlan ssid My wireless
```

set wlan

Description

Configures the first wireless network that was created.

Syntax

```
set wlan security-type <security-type>
```

Parameters

Parameter	Description
security-type	Security Type Options: none, WEP, WPA2, WPA/WPA2

Example

```
set wlan security-type none
```

set wlan

Description

Configures the first wireless network that was created.

Syntax

```
set wlan wpa-auth-type password <password> [ hotspot <hotspot > ]
```

Parameters

Parameter	Description
n/a	

Example

```
set wlan wpa-auth-type password gTd&3(gha_ hotspot on
```

set wlan

Description

Configures the first wireless network that was created.

Syntax

```
set wlan wpa-auth-type { radius [ hotspot <hotspot > ] }
```

Parameters

Parameter	Description
hotspot	The Hotspot of the Virtual Access Point Options: on, off
wpa-auth-type	Wireless protected access authentication Type: Press TAB to see available options

Example

```
set wlan wpa-auth-type radius hotspot on
```

set wlan

Description

Configures the first wireless network that was created.

Syntax

```
set wlan wpa-encryption-type <wpa-encryption-type>
```

Parameters

Parameter	Description
wpa-encryption-type	Wireless protected access encryption type Options: Auto, CCMP-AES, TKIP

Example

```
set wlan wpa-encryption-type Auto
```

set wlan

Description

Configures the first wireless network that was created.

Syntax

```
set wlan assignment <assignment>
```

Parameters

Parameter	Description
assignment	The network assigned to the virtual access point Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set wlan assignment My_Network
```

set wlan

Description

Enable/Disable an existing wireless network (VAP).

Syntax

```
set wlan vap <vap>{ enable | disable }
```

Parameters

Parameter	Description
mode	The mode of the Virtual Access Point Options: on, off
vap	The name of the Virtual Access Point Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set wlan vap My_Network on
```

set wlan

Description

Configures the SSID of an existing wireless network (VAP).

Syntax

```
set wlan vap <vap> ssid <ssid>
```

Parameters

Parameter	Description
ssid	Wireless network name (SSID) Type: A string that contains [A-Z], [0-9], '_', '.', '-' and space characters
vap	The name of the Virtual Access Point Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set wlan vap My_Network ssid My wireless
```

set wlan

Description

Configures an existing wireless network (VAP).

Syntax

```
set wlan vap <vap> security-type <security-type>
```

Parameters

Parameter	Description
security-type	Security Type Options: none, WEP, WPA2, WPA/WPA2
vap	The name of the Virtual Access Point Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set wlan vap My_Network security-type none
```

set wlan

Description

Configures an existing wireless network (VAP).

Syntax

```
set wlan vap <vap> wpa-auth-type password <password> [ hotspot <hotspot
> ]
```

Parameters

Parameter	Description
vap	The name of the Virtual Access Point Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set wlan vap My_Network wpa-auth-type password gTd&3(gha_ hotspot on
```

set wlan

Description

Configures an existing wireless network (VAP).

Syntax

```
set wlan vap <vap> wpa-auth-type { radius [ hotspot <hotspot >] }
```

Parameters

Parameter	Description
hotspot	The Hotspot of the Virtual Access Point Options: on, off
vap	The name of the Virtual Access Point Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
wpa-auth-type	Wireless protected access authentication Type: Press TAB to see available options

Example

```
set wlan vap My_Network wpa-auth-type radius hotspot on
```

set wlan

Description

Configures an existing wireless network (VAP).

Syntax

```
set wlan vap <vap> wpa-encryption-type <wpa-encryption-type>
```

Parameters

Parameter	Description
vap	The name of the Virtual Access Point Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
wpa-encryption-type	Wireless protected access encryption type Options: Auto, CCMP-AES, TKIP

Example

```
set wlan vap My_Network wpa-encryption-type Auto
```

set wlan

Description

Configures an existing wireless network (VAP).

Syntax

```
set wlan vap <vap> assignment <assignment>
```

Parameters

Parameter	Description
assignment	The network assigned to the virtual access point Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters
vap	The name of the Virtual Access Point Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set wlan vap My_Network assignment My_Network
```

set wlan

Description

Configures an existing wireless network (VAP).

Syntax

```
set wlan vap <vap> advanced-settings [ hide-ssid <hide-ssid> ] [
station-to-station <station-to-station> ] [ wds <wds> ]
```

Parameters

Parameter	Description
vap	The name of the Virtual Access Point Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
set wlan vap My_Network advanced-settings hide-ssid on station-to-
station allow wds on
```

set wlan wireless advanced-settings protected-mgmt-frames

Description

Enable or disable protection of 802.11 management frames (refers to the main wireless access point).

Syntax

```
set wlan <main-wireless-name>advanced-settings protected-mgmt-frames {
on | off }
```

Parameters

Parameter	Description
main-wireless-name	Name of the main wireless access point
Type	Press TAB to see available options
on/off	on - Enabled off - Disabled

Example

```
set wlan NANCY-wireless advanced-settings protected-mgmt-frames off
```

show wlan

Shows configuration for wireless networks (relevant to hardware models with wireless).

show wlan

Description

Shows configuration for a virtual access point (VAP or wireless network).

Syntax

```
show wlan vap <vap>
```

Parameters

Parameter	Description
vap	The name of the Virtual Access Point Type: A string that contains [A-Z], [0-9], '_', '.', '-' and '/' characters

Example

```
show wlan vap My_Network
```

show wlan

Description

Shows configuration of the wireless radio.

Syntax

```
text
```

```
show wlan
```

Parameters

Parameter	Description
n/a	

Example

```
show wlan
```

wlan radio

set wlan radio

Configures the radio settings of wireless antennas (in appliance models that contain wireless options).

set wlan radio

Description

Configures the radio settings of wireless antennas.

Syntax

```
set wlan radio [ country <country> ] [ operation-mode <operation-mode>
] [ channel <channel> ] [ channel-width <channel-width> ]
```

Parameters

Parameter	Description
channel	Channel Options: channel
channel-width	Channel width Options: auto, 20, 40, 80
country	Country Options: country
operation-mode	Operation mode Options: 11b, 11g, 11bg, 11n, 11ng, 11ac, 11nac

Example

```
set wlan radio country albania operation-mode 11b channel auto channel-
width auto
```

set wlan radio

Description

Configures the radio settings of wireless antennas per band (in wireless models that contain a concurrent dual band option using two radio antennas).

Syntax

```
set wlan radio band <band> [ country <country> ] [ operation-mode
<operation-mode> ] [ channel <channel> ] [ channel-width <channel-
width> ]
```

Parameters

Parameter	Description
band	type Options: 5GHz, 2.4GHz
channel	Channel Options: channel
channel-width	Channel width Options: auto, 20, 40, 80
country	Country Options: country
operation-mode	Operation mode Options: 11b, 11g, 11bg, 11n, 11ng, 11ac, 11nac

Example

```
set wlan radio band 5GHz country albania operation-mode 11b channel
auto channel-width auto
```

set wlan radio

Description

Enable/Disable the wireless radio.

Syntax

```
set wlan radio { off | on }
```

Parameters

Parameter	Description
mode	Wireless radio mode Options: off, on

Example

```
set wlan radio off
```

set wlan radio

Description

Enable/Disable the wireless radio per band (in wireless models that contain a concurrent dual band option using two radio antennas).

Syntax

```
set wlan radio band <band> { off | on }
```

Parameters

Parameter	Description
band	type Options: 5GHz, 2.4GHz
mode	Wireless radio mode Options: off, on

Example

```
set wlan radio band 5GHz off
```

set wlan radio

Description

Configures advanced radio settings for the wireless radio.

Syntax

```
set wlan radio advanced-settings [ transmitter-power <transmitter-
power> ] [ guard-interval <guard-interval> ] [ antenna <antenna> ]
```

Parameters

Parameter	Description
n/a	

Example

```
set wlan radio advanced-settings transmitter-power minimum guard-
interval short antenna auto
```

set wlan radio

Description

Configures advanced radio settings for the wireless radio per band (in wireless models that contain a concurrent dual band option using two radio antennas).

Syntax

```
set wlan radio band <band> advanced-settings [ transmitter-power
<transmitter-power> ] [ guard-interval <guard-interval> ] [ antenna
<antenna>]
```

Parameters

Parameter	Description
band	type Options: 5GHz, 2.4GHz

Example

```
set wlan radio band 5GHz advanced-settings transmitter-power minimum
guard-interval short antenna auto
```

show wlan radio

Description

Shows configuration of the wireless radio.

Syntax

```
show wlan radio
```

Parameters

Parameter	Description
n/a	

Example

```
show wlan radio
```

show wlan statistics

Description

Shows statistics of the wireless radio.

Syntax

```
show wlan statistics
```

Parameters

Parameter	Description
n/a	

Example

```
show wlan statistics
```

wlan vaps

add wlan vap

Description

Adds a new wireless network (Virtual Access Point or VAP) to an available wireless radio. In hardware models were dual antennas are available, during configuration of a wireless network the specific band for the network must be selected (2.4Ghz/5Ghz).

Syntax

```
add wlan vap ssid <ssid> band <band>
```

Parameters

Parameter	Description
band	Wireless radio transmitter Options: 5GHz, 2.4GHz
ssid	Wireless network name (SSID) Type: A string that contains [A-Z], [0-9], '_', '.', '-' and space characters

Example

```
add wlan vap ssid My wireless band 5GHz
```

delete wlan vaps

Description

Delete all existing wireless Virtual Access Points (VAP).

Syntax

```
delete wlan vaps
```

Parameters

Parameter	Description
n/a	

Example

```
delete wlan vaps
```

set wlan vap wireless advanced-settings protected-mgmt-frames

Description

Enable or disable protection of 802.11 management frames

Syntax

```
set wlan vap <wireless-name> advanced-settings protected-mgmt-frames {
on | off }
```

Parameters

Parameter	Description
wireless-name	Name of the wireless network
Type	Press TAB to see available options
on/off	on - Enabled off - Disabled

Example

```
set wlan vap cp7f7e5168 advanced-settings protected-mgmt-frames off
```

set wlan vap

Description

Use MAC address as wireless password.

Syntax

```
set wlan vap <vap> wpa-auth-type password-set-as-mac-with-prefix
<prefix>
```

Parameters

Parameter	Description
vap	Name of the VAP that is being edited.
prefix	The authentication type is password-set-as-mac-with-prefix.

Example

```
set wlan vap Guest1 wpa-auth-type password-set-as-mac-with-prefix aaa
```

show wlan vap wireless

Description

Show wlan vap wireless networks for which 802.11w is enabled

Syntax

```
show wlan vap <wireless-name>
```

Parameters

Parameter	Description
<wireless-name>	Name of the wireless network

Example

```
show wlan vap MyWiFi
```

show wlan vaps

Description

Shows all Virtual Access points (VAPs or wireless network).

Syntax

```
show wlan vaps
```

Parameters

Parameter	Description
n/a	

Example

```
show wlan vaps
```

show wlan vaps statistics

Description

Shows statistics per Virtual Access Point.

Syntax

```
show wlan vaps statistics
```

Parameters

Parameter	Description
n/a	

Example

```
show wlan vaps statistics
```

zero-touch

set zero-touch

Description

Configure parameters for the ZeroTouch service.

Syntax

```
set zero-touch [ cloud-url <cloud-url> ] [ verify-certificate <verify-certificate> ] [ mode <mode> ]
```

Parameters

Parameter	Description
cloud-url	The DNS or IP address of the cloud service. Default: `zerotouch.checkpoint.com` Type: URL or IP address
mode	When the mode is set to on, the appliance will constantly try to fetch configuration from the Zero Touch server if the First Time Configuration Wizard is not started. Options: on, off Default: on
verify-certificate	When verify-certificate is set to on, the appliance will verify the SSL certificate of the Zero Touch server. You are advised NOT to change this value. Options: on, off Default: on

Example

```
set zero-touch cloud-url <url> verify-certificate on mode on
```

show zero-touch

Description

Show the parameters configured for the Zero Touch service.

Syntax

```
show zero-touch
```

Parameters

Parameter	Description
n/a	

Example

```
show zero-touch
```

test zero-touch-request

Description

Test the procedure of receiving configuration from the Zero Touch server. If the command is executed without parameters, the gateway will connect to the Zero Touch server and display the received configuration without enforcing it. There is an option to store the configuration in the `/storage/zt_cfg.clish` file.

Syntax

```
test zero-touch-request [save-config-as file ]
```

Parameters

Optional Parameter	Description
save-configuration-as file	Save received configuration to the `/storage/zt_cfg.clish` file.

Example

```
test zero-touch-request test zero-touch-request save-config-as file
```