QUANTUM

29 May 2024

QUANTUM SPARK 1500, 1600, 1800, 1900, 2000 APPLIANCES

R81.10.X

CLI Reference Guide

CHECK POINT™

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 R81.10.X Quantum Spark 1500, 1600, 1800, 1900, 2000 Appliances CLI Reference Guide

Latest Version of this Document in English

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
29 May 2024	Updated all pages in *"Configuring the "Reach My Device" Service" on page 1308*
26 May 2024	Added: ■ *"Important Links" on page 55* ■ *"Special Characters in Gaia Clish" on page 59* Updated: ■ *"backup settings (TFTP, SFTP, USB)" on page 1643*
15 April 2024	Added: ■ *"set internet-connection probe-servers" on page 357* Updated: ■ *"show internet-connection icmp-servers" on page 635* ■ *"set internet-connection probe-next-hop" on page 356* ■ *"set internet-connection probe-icmp-servers" on page 359* ■ *"set internet-connection probe-icmp6-servers" on page 629*
28 March 2024	Updated: (removed the "`is-unnumbered-pppoe`" parameter in the PPTP and L2TP connection types) ■ *"add internet-connection interface DMZ" on page 268* ■ *"add internet-connection interface WAN" on page 253* ■ *"add internet-connection interface DMZ - RJ45/SFP-Fiber" on page 276* ■ *"add internet-connection-ipv6 interface-ipv6" on page 374* ■ *"set internet-connection type dhcp / static" on page 328* ■ *"set internet-connection type pptp" on page 331* ■ *"set internet-connection type l2tp" on page 330* ■ *"set internet-connection dmz-connection rj45/sfp-fiber / sfp-dsl" on page 346*
18 March 2024	Added: ■ *"Working with Dr. Spark" on page 1732* Updated: ■ *"show iot-device-type" on page 1328*

Date	Description
26 February 2024	Added the commands and options for the R81.10.10 version
14 November 2023	Added: ■ *"kernel-parameter" on page 1706*
10 October 2023	Added: ■ *"set administrators radius-auth" on page 78* ■ *"Configuring TACACS+ Authentication for Administrators" on page 81* Updated: ■ *"set administrators tacacs-auth" on page 81*
28 September 2023	Updated: ■ *"add internet-connection interface WAN" on page 253*
31 August 2023	Added the commands and options for the R81.10.08 version
18 May 2023	Added the commands and options for the R81.10.07 version
12 March 2023	Added: ■ *"set vpn site add remote-site-enc-dom-route-excluded-network-obj" on page 1378*
19 February 2023	Updated: ■ *"Working with OpenSSH Encryption Algorithms" on page 1499* ■ *"Configuring Smart Accel Settings" on page 536*
06 February 2023	Updated *"Debugging VPN" on page 1441*
25 January 2023	Added the commands and options for the R81.10.05 version
20 July 2022	Updated: ■ *"set administrator session-settings" on page 85*
28 June 2022	First release of this document

Table of Contents

Important Links

Important - Review these materials before configuring your Quantum Spark appliance.

Video

Small Business Cyber Security video channel

SK Articles

- *sk179615 - Quantum Spark Appliances - Releases R81.10.X*
- *sk178604 - Quantum Spark R81.10.X Known Limitations*
- *sk181134 - Quantum Spark R81.10.X Resolved Issues*
- *sk182234 - Quantum Spark - FAQ*
- *sk181924 - Quantum Spark Appliances 1900 and 2000 Models*
- *sk168880 - Quantum Spark Appliances 1600 and 1800 Models*
- *sk157412 - Quantum Spark Appliances 1500 Models*

Documents (in English)

Note - Some topics in an Administration Guide only apply to specific appliances or models.

- *R81.10.X Quantum Spark Release Notes for 1500, 1600, 1800, 1900, 2000 Appliances*
- *R81.10.X Quantum Spark Locally Managed Administration Guide for 1500, 1600, 1800, 1900, 2000 Appliances*
- *R81.10.X Quantum Spark Centrally Managed Administration Guide for 1500, 1600, 1800, 1900, 2000 Appliances*
- *R81.10.X Quantum Spark Dynamic Routing CLI Guide for 1500, 1600, 1800, 1900, 2000 Appliances*

Introduction

This guide contains all relevant CLI commands for these Quantum Spark / Small and Medium Business (SMB) appliance models:

Series	Home Page SK
2000	sk181924
1900	sk181924
1800	sk168880
1600	sk168880
1595R	sk181492
1595	sk157412
1590	sk157412
1575	sk157412
1570R	sk166654
1570	sk157412
1555	sk157412
1550	sk157412
1535	sk157412
1530	sk157412

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 (Gaia 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:

  1. Login to the Expert mode using the Expert mode password.
  2. Run this command: `bashUser on`

  From now, you always log in directly to the Expert mode.

  To turn this mode off, run this command: `bashUser off`
- SCP to the appliance is supported but you need to enable direct login to the Expert mode.

  Note that SFTP that is commonly used by WinSCP is not supported.

  For more information, see sk52763.

Gaia Clish auto-completion

All Gaia Clish commands support auto-completion.

Standard Check Point and native Linux commands can be used from the Gaia Clish shell but do not support auto-completion.

These are examples of the different commands:

- Gaia Clish - `set`, `show`
- Standard Check Point - `fw`, `vpn`, `cphaprob`
- Native Linux - `ping`, `tcpdump`

CLI Syntax

The CLI commands are formatted according to these syntax rules.

Notation	Description	Example
Text without brackets	Items you must enter as appears in the syntax	`set interface`
<*Text inside angle brackets*>	Placeholder for which you must supply a value	`set interface <name>`
[Text inside square brackets]	Optional items	`[ dns-primary <IPv4 Address> ]`
Vertical pipe (|)	Separator for mutually exclusive items; choose one	
{Text inside curly brackets with the vertical pipe}	Set of items; choose one	`{ on | off }`
Ellipsis (...)	You can enter the previous set of options more than one time	`-r <fromIP> <toIP> ...` means you can enter `-r <fromIP1> <toIP1> <fromIP2> <toIP2> <fromIP3> <toIP3>` and so on

Special Characters in Gaia Clish

To enter the "**?**" character, press the **CTRL V** keys and then press the **SHIFT ?** keys.

To enter the "****" character, enter ****.

Running Gaia Clish Commands from Expert Mode

You can run Gaia Clish commands from Expert mode.

Syntax

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

Parameters

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

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 Quantum Spark Appliance CLI:

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

show commands

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows all available Gaia Clish commands.

Syntax

```
show commands
```

cpshell

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Switches from the current shell (Expert mode of Gaia Clish) to the Check Point Shell mode.

The Check Point Shell mode allows to run specific Expert mode commands.

Note - Enter the "`exit`" command to return to the previous shell. See *"exit" on page 65*.

Syntax

```
cpshell
```

expert

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Switches from the current shell to the Expert mode, which is an unrestricted shell.

Note - Enter the "`exit`" command to return to the previous shell. See *"exit" on page 65*.

Syntax

```
expert
```

set expert password

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the initial password or password hash for the Expert mode.

Syntax

```
set expert password <password>
set expert password-hash <password_hash>
```

Parameters

Parameter	Description
password	Configures the password using alphanumeric and special characters
password_hash	Configures the password using an encrypted representation of the password. The password is not visible as text on the terminal command line, or in the command history. Use this option if you want to change passwords using a script. You can generate the hash version of the password using standard Linux hash generating utilities.

Example Command

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

Comments

To generate a password-hash, you can use this command on any Check Point Quantum Spark Appliance (in the Expert mode):

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

exit

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Exits from the current shell.

Syntax

```
exit
```

Configuring Administrator Accounts

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure administrator accounts.

Configuring Administrator Users

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure administrator users.

add administrator

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures a new administrator user, who can access the appliance through WebUI and SSH.

See:

- *"set administrator username password" on page 68*
- *"set administrator username permission" on page 69*
- *"show administrator username" on page 71*
- *"show administrators" on page 72*
- *"show administrators advanced-settings" on page 73*
- *"delete administrator username" on page 74*

Syntax

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

Parameters

Parameter	Description
username	Configures the administrator user name. A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '_' (underscore)
password-hash	Configures the MD5 of the password string. The password is not visible as text on the command line, or in the command history. Use this option if you want to change passwords using a script. To generate a password-hash, you can use this command on any Check PointQuantum Spark Appliance (in the Expert mode): `cryptpw -a md5 <password string>`
permission	Configures the administrator permissions. One of these: ■ `access-policy` ■ `read-write` ■ `readonly` ■ `remote-access` ■ `Super Admin networking`

Example Command

```
add administrator username user1 password-hash TZXPLs20bN0RA
permission read-write
```

set administrator username password

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures a new password for an existing administrator.

Notes:

- The Gaia Embedded operating system prompts you to add a new password.
- You cannot use this command in a script.

See:

- *"add administrator" on page 66*
- *"set administrator username permission" on page 69*
- *"show administrator username" on page 71*
- *"show administrators" on page 72*
- *"show administrators advanced-settings" on page 73*
- *"delete administrator username" on page 74*

Syntax

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

Parameters

Parameter	Description
username	Specifies the administrator user name. Press the TAB key to see the available options.

Example Command

```
set administrator username user1 password
```

set administrator username permission

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

See:

- *"add administrator" on page 66*
- *"set administrator username password" on page 68*
- *"show administrator username" on page 71*
- *"show administrators" on page 72*
- *"show administrators advanced-settings" on page 73*
- *"delete administrator username" on page 74*

Syntax

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

Parameters

Parameter	Description
username	Configures the administrator user name. A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '_' (underscore)
password-hash	Configures the MD5 of the password string. The password is not visible as text on the command line, or in the command history. Use this option if you want to change passwords using a script. To generate a password-hash, you can use this command on any Check Point Quantum Spark Appliance (in the Expert mode): `cryptpw -a md5 <password string>`
permission	Configures the administrator permissions. One of these: ■ `access-policy` ■ `read-write` ■ `readonly` ■ `remote-access` ■ `Super Admin networking`

Example Command

```
set administrator username user1 permission read-write password-
hash TZXPLs20bN0RA
```

show administrator username

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of an existing administrator user.

See:

- *"add administrator" on page 66*
- *"set administrator username password" on page 68*
- *"set administrator username permission" on page 69*
- *"show administrators" on page 72*
- *"show administrators advanced-settings" on page 73*
- *"delete administrator username" on page 74*

Syntax

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

Parameters

Parameter	Description
username	Specified the administrator user name. Press the TAB key to see the available options.

Example Command

```
show administrator username user1
```

show administrators

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of all administrator users.

See:

- *"add administrator" on page 66*
- *"set administrator username password" on page 68*
- *"set administrator username permission" on page 69*
- *"show administrator username" on page 71*
- *"show administrators advanced-settings" on page 73*
- *"delete administrator username" on page 74*

Syntax

```
show administrators
```

show administrators advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the advanced settings of all administrator users.

See:

- *"add administrator" on page 66*
- *"set administrator username password" on page 68*
- *"set administrator username permission" on page 69*
- *"show administrator username" on page 71*
- *"show administrators" on page 72*
- *"delete administrator username" on page 74*

Syntax

```
show administrators advanced-settings
```

delete administrator username

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing defined administrator.

The system does not allow you to delete the last administrator.

See:

- *"add administrator" on page 66*
- *"set administrator username password" on page 68*
- *"set administrator username permission" on page 69*
- *"show administrator username" on page 71*
- *"show administrators" on page 72*
- *"show administrators advanced-settings" on page 73*

Syntax

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

Parameters

Parameter	Description
username	Specifies the administrator user name. Press the TAB key to see the available options.

Example Command

```
delete administrator username user1
```

Configuring Administrator Roles

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure administrator roles.

set administrators roles-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the settings for administrator roles.

See *"show administrators roles-settings" on the next page*.

Syntax

```
set administrators roles-settings customize-roles true roles-conf
<Base64-string>
```

```
set administrators roles-settings customize-roles false
```

Parameters

Parameter	Description
customize-roles	Enables (`true`) or disables (`false`) the customization of default administrator role permissions. The value "`false`" restores the default permissions in the administrator roles. The default administrator roles are: ■ Access Policy ■ Mobile ■ Networking ■ Read-only ■ Remote Access ■ Super
Base64-string	Configures the content of the `roles.conf` file in Base64 format. To get the required configuration, contact *Check Point Support*.

Example Command

```
set administrators roles-settings customize-roles true roles-conf
ew0KCSJST0xF...(truncated)...Q0KCX0NCn0=
```

show administrators roles-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings for administrator roles.

See *"set administrators roles-settings" on the previous page*.

Syntax

```
show administrators roles-settings
```

Configuring RADIUS Authentication for Administrators

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure RADIUS authentication for administrators.

set administrators radius-auth

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the RADIUS authentication for administrators.

Note - You must configure the applicable RADIUS server. See *"Configuring RADIUS Servers" on page 878*.

See *"show administrators radius-auth" on page 80*.

Syntax

`set administrators radius-auth enable use-radius-roles true`
`set administrators radius-auth enable use-radius-roles false [ permission <Administrator Role> ] [ use-radius-groups true radius-groups <Group1>,<Group2>,...,<GroupN> ]`
`set administrators radius-auth disable`

Parameters

Parameter	Description
radius-auth	Enables (`enable`) or Disables (`disable`) the RADIUS authentication for administrators.
use-radius-roles	Specifies which RADIUS roles to use: ■ `true` - Use roles defined on the RADIUS server (this is the default). ■ `false` - Use default roles for RADIUS users (predefined on the appliance). Use the "`permission`" parameter to specify the predefined role.
permission	Specifies the default Administrator Role (when the value of the parameter "`use-radius-roles`" is "`false`"): ■ `read-write` - Super Administrator (this is the default). ■ `networking` - Networking Administrator. ■ `access-policy` - Access Policy Administrator. ■ `remote-access` - Remote Access Administrator. ■ `readonly` - Read-Only Administrator. ■ `mobile` - Mobile Administrator.
radius-groups	Specifies the RADIUS Groups to use for authentication (when the value of the parameter "`use-radius-roles`" is "`false`"). **Notes:** ■ You must enter the names of RADIUS Groups as configured on the RADIUS server. ■ To enter more than one RADIUS Group, enter their names separated by commas (without spaces).

Example Command

```
set administrators tacacs-auth enable use-tacacs-roles false
permission mobile use-radius-groups true radius-groups
MyGroup1,MyGroup2
```

show administrators radius-auth

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configured RADIUS authentication for administrators.

See *"set administrators radius-auth" on page 78*.

Syntax

```
show administrators radius-auth
```

Example Output

```
HostName> show administrators radius-auth
radius-auth:                    enable
use-radius-groups:              true
radius-groups:                  MyGroup
permission:                     read-write
use-radius-roles:               false
```

Configuring TACACS+ Authentication for Administrators

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure TACACS+ authentication for administrators.

set administrators tacacs-auth

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Configures the TACACS+ authentication for administrators.

Note - You must configure the applicable TACACS+ server. See *"Configuring TACACS+ Servers" on page 884*.

See *"show administrators tacacs-auth" on page 83*.

Syntax

`set administrators tacacs-auth enable use-tacacs-roles true`
`set administrators tacacs-auth enable use-tacacs-roles false [ permission <Administrator Role> ]`
`set administrators tacacs-auth disable`

Parameters

Parameter	Description
tacacs-auth	Enables (`enable`) or Disables (`disable`) the TACACS+ authentication for administrators.
use-tacacs-roles	Specifies which TACACS+ roles to use: ■ `true` - Use roles defined on the TACACS+ server (this is the default). ■ `false` - Use default roles for TACACS+ users (predefined on the appliance). Use the "`permission`" parameter to specify the predefined role.
permission	Specifies the default Administrator Role (when the value of the parameter "`use-tacacs-roles`" is "`false`"): ■ `read-write` - Super Administrator (this is the default). ■ `networking` - Networking Administrator. ■ `access-policy` - Access Policy Administrator. ■ `readonly` - Read-Only Administrator. ■ `mobile` - Mobile Administrator.

Example Command

```
set administrators radius-auth enable use-radius-roles false
permission mobile
```

show administrators tacacs-auth

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Show the authorized administrators on the TACACS+ server and associated permission and role.

See *"set administrators tacacs-auth" on page 81*.

Syntax

```
show administrators tacacs-auth
```

Example Command

```
HostName> show administrators tacacs-auth
tacacs-auth:       enable
permission:        mobile
use-tacacs-roles:  false
```

Configuring Administrator Session Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure session settings for administrators.

set administrator session-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the session settings for administrators.

These settings are global for all administrators.

Note - We strongly recommend the use of complex passwords. Password must be at least 12 characters in length and contain uppercase, lowercase, numeric and non-alphanumeric characters. Allowed alphanumeric characters: `! @ # % ^ & * ( ) - _ + : ;`

See *"show administrator session-settings" on page 87*.

Syntax

```
set administrator session-settings
      [ inactivity-timeout 1-999 ]
      [ lock-period 5-59940 ]
      [ lockout-enable {on | off} ]
      [ max-lockout-attempts 1-999 ]
      [ password-complexity-level {low | high} ]
      [ password-expiration-timeout 1-360 ]
      [ password-history-mechanism {true | false } ]
```

Parameters

Parameter	Description
inactivity-timeout	Configures the administrator is automatically logged out from the WebUI after the session is idle for this integer number of minutes
lock-period	Configures the lock period - once locked out, the administrator is be unable to login for this integer number of seconds
lockout-enable	Enables (`true`) or disables (`false`) the limit for the number of the failed administrator login attempts
max-lockout-attempts	Configures the maximum number of consecutive login failure attempts before the administrator is locked out
password-complexity-level	Configures additional restrictions on administrator passwords, according to the selected complexity level
password-expiration-timeout	Requires the administrator to change their password after this integer number of days (from the last time the password was changed) Takes effect only if the password complexity level is set to '`high`'
password-history-mechanism	Enables (`true`) or disables (`false`) the password history to prevent the user from configuring a new password that is similar to the current password

Example Command

```
set administrator session-settings lockout-enable on max-lockout-
attempts 5 lock-period 20 inactivity-timeout 360 password-
complexity-level low password-expiration-timeout 60 password-
history-mechanism true
```

show administrator session-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the session settings for administrator users.

See *"set administrator session-settings" on page 85*.

Syntax

```
show administrator session-settings
```

Example Output

```
HostName> show administrator session-settings
lockout-enable:                on
max-lockout-attempts:          10
lock-period:                   30
inactivity-timeout:            720
mobile-app-session-timeout:    30
password-complexity-level:     low
password-history-mechanism:    true
password-expiration-timeout:   90
```

Configuring IP Addresses for Administrator Access

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure IP addresses on the appliances for administrator access.

Configuring IPv4 Addresses for Administrator Access

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure IPv4 addresses for administrator access.

add admin-access-ipv4-address single-ipv4-address

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

See:

- *"add admin-access-ipv4-address network-ipv4-address" on page 91*
- *"show admin-access-ip-addresses" on page 99*
- *"show admin-access-ipv4-addresses" on page 93*
- *"delete admin-access-ipv4-address" on page 94*
- *"delete admin-access-ipv4-address-all" on page 95*
- *"delete admin-access-ip-address-all" on page 102*

Syntax

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

Parameters

Parameter	Description
single-ipv4-address	Configures the IPv4 address of the allowed computer

Example Command

```
add admin-access-ipv4-address single-ipv4-address 192.168.22.33
```

add admin-access-ipv4-address network-ipv4-address

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

See:

- *"add admin-access-ipv4-address single-ipv4-address" on page 90*
- *"show admin-access-ip-addresses" on page 99*
- *"show admin-access-ipv4-addresses" on page 93*
- *"delete admin-access-ipv4-address" on page 94*
- *"delete admin-access-ipv4-address-all" on page 95*
- *"delete admin-access-ip-address-all" on page 102*

Syntax

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

Parameters

Parameter	Description
network-ipv4-address	Configures the IPv4 address of the allowed network
subnet-mask	Configures the IPv4 subnet mask of the allowed network
mask-length	Configures the IPv4 subnet mask length of the allowed network

Example Command

```
add admin-access-ipv4-address network-ipv4-address 192.168.22.0 subnet-mask 255.255.255.0
```

show admin-access-ip-addresses

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows all the configured IPv4 and IPv6 addresses, from which the administrator can remotely access the appliance according to configuration.

See:

- *"add admin-access-ipv4-address single-ipv4-address" on page 90*
- *"add admin-access-ipv6-address single-ipv6-address" on page 97*
- *"add admin-access-ipv4-address network-ipv4-address" on page 91*
- *"add admin-access-ipv6-address network-ipv6-address" on page 98*
- *"show admin-access-ipv4-addresses" on page 93*
- *"delete admin-access-ipv4-address" on page 94*
- *"delete admin-access-ipv4-address-all" on page 95*
- *"delete admin-access-ipv6-address ipv6-address" on page 100*
- *"delete admin-access-ipv6-address ipv6-network" on page 101*
- *"delete admin-access-ip-address-all" on page 102*

Syntax

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

show admin-access-ipv4-addresses

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows allowed IP addresses, from which the administrator can remotely access the appliance according to configuration.

See:

- *"add admin-access-ipv4-address single-ipv4-address" on page 90*
- *"add admin-access-ipv4-address network-ipv4-address" on page 91*
- *"show admin-access-ip-addresses" on page 99*
- *"delete admin-access-ipv4-address" on page 94*
- *"delete admin-access-ipv4-address-all" on page 95*
- *"delete admin-access-ip-address-all" on page 102*

Syntax

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

delete admin-access-ipv4-address

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

See:

- *"add admin-access-ipv4-address single-ipv4-address" on page 90*
- *"add admin-access-ipv4-address network-ipv4-address" on page 91*
- *"show admin-access-ip-addresses" on page 99*
- *"show admin-access-ipv4-addresses" on page 93*
- *"delete admin-access-ipv4-address-all" on page 95*
- *"delete admin-access-ip-address-all" on page 102*

Syntax

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

Parameters

Parameter	Description
ipv4-address	Specifies the IPv4 address

Example Command

```
delete admin-access-ipv4-address 192.168.22.33
```

delete admin-access-ipv4-address-all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

See:

- *"add admin-access-ipv4-address single-ipv4-address" on page 90*
- *"add admin-access-ipv4-address network-ipv4-address" on page 91*
- *"show admin-access-ip-addresses" on page 99*
- *"show admin-access-ipv4-addresses" on page 93*
- *"delete admin-access-ip-address-all" on page 102*

Syntax

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

delete admin-access-ip-address-all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all the configured IPv4 and IPv6 addresses, from which the administrator can remotely access the appliance according to configuration.

See:

- *"add admin-access-ipv4-address single-ipv4-address" on page 90*
- *"add admin-access-ipv6-address single-ipv6-address" on the next page*
- *"add admin-access-ipv4-address network-ipv4-address" on page 91*
- *"add admin-access-ipv6-address network-ipv6-address" on page 98*
- *"show admin-access-ipv4-addresses" on page 93*
- *"delete admin-access-ipv4-address" on page 94*
- *"delete admin-access-ipv4-address-all" on page 95*
- *"delete admin-access-ipv6-address ipv6-address" on page 100*
- *"delete admin-access-ipv6-address ipv6-network" on page 101*

Syntax

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

Configuring IPv6 Addresses for Administrator Access

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure IPv6 addresses for administrator access.

add admin-access-ipv6-address single-ipv6-address

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an IPv6 address, from which the administrator can remotely access the appliance according to configuration.

See:

- *"add admin-access-ipv6-address network-ipv6-address" on the next page*
- *"show admin-access-ip-addresses" on page 99*
- *"delete admin-access-ipv6-address ipv6-address" on page 100*
- *"delete admin-access-ipv6-address ipv6-network" on page 101*
- *"delete admin-access-ip-address-all" on page 102*

Syntax

```
add admin-access-ipv6-address single-ipv6-address <single-ipv6-address>
```

Parameters

Parameter	Description
single-ipv6-address	Configures the IPv6 address of the allowed computer

Example Command

```
add admin-access-ipv6-address single-ipv6-address 0:0:0:0:0:ffff:c0a8:0101
```

add admin-access-ipv6-address network-ipv6-address

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an IPv6 address with a prefix, from which the administrator can remotely access the appliance according to configuration.

See:

- *"add admin-access-ipv6-address single-ipv6-address" on the previous page*
- *"add admin-access-ipv6-address network-ipv6-address" above*
- *"show admin-access-ip-addresses" on page 99*
- *"delete admin-access-ipv6-address ipv6-address" on page 100*
- *"delete admin-access-ipv6-address ipv6-network" on page 101*

Syntax

```
add admin-access-ipv6-address network-ipv6-address <network-ipv6-address> ipv6-prefix <ipv6-prefix>
```

Parameters

Parameter	Description
network-ipv6-address	Configures the IPv6 address of the allowed network
ipv6-prefix	Configures the IPv6 prefix of the allowed network (between 64 and 128)

Example Command

```
add admin-access-ipv6-address network-ipv6-address 0:0:0:0:0:ffff:c0a8:0100 ipv6-prefix 64
```

show admin-access-ip-addresses

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows all the configured IPv4 and IPv6 addresses, from which the administrator can remotely access the appliance according to configuration.

See:

- *"add admin-access-ipv4-address single-ipv4-address" on page 90*
- *"add admin-access-ipv6-address single-ipv6-address" on page 97*
- *"add admin-access-ipv4-address network-ipv4-address" on page 91*
- *"add admin-access-ipv6-address network-ipv6-address" on page 98*
- *"show admin-access-ipv4-addresses" on page 93*
- *"delete admin-access-ipv4-address" on page 94*
- *"delete admin-access-ipv4-address-all" on page 95*
- *"delete admin-access-ipv6-address ipv6-address" on the next page*
- *"delete admin-access-ipv6-address ipv6-network" on page 101*
- *"delete admin-access-ip-address-all" on page 102*

Syntax

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

delete admin-access-ipv6-address ipv6-address

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an IPv6 address, from which the administrator can remotely access the appliance according to configuration.

See:

- *"add admin-access-ipv6-address single-ipv6-address" on page 97*
- *"add admin-access-ipv6-address network-ipv6-address" on page 98*
- *"show admin-access-ip-addresses" on the previous page*
- *"delete admin-access-ipv6-address ipv6-address" above*
- *"delete admin-access-ipv6-address ipv6-network" on the next page*
- *"delete admin-access-ip-address-all" on page 102*

Syntax

```
delete admin-access-ipv6-address ipv6-address <ipv6-address>
```

Parameters

Parameter	Description
ipv6-address	Specifies the IPv6 address

Example Command

```
delete admin-access-ipv6-address ipv6-address
0:0:0:0:0:ffff:c0a8:1600
```

delete admin-access-ipv6-address ipv6-network

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an IPv6 address, from which the administrator can remotely access the appliance according to configuration.

See:

- *"add admin-access-ipv6-address single-ipv6-address" on page 97*
- *"add admin-access-ipv6-address network-ipv6-address" on page 98*
- *"show admin-access-ip-addresses" on page 99*
- *"delete admin-access-ipv6-address ipv6-address" on the previous page*
- *"delete admin-access-ipv6-address ipv6-network" above*
- *"delete admin-access-ip-address-all" on page 102*

Syntax

```
delete admin-access-ipv6-address ipv6-network <ipv6-network>
```

Parameters

Parameter	Description
ipv6-network	Specifies the IPv6 address or name of the network

Example Command

```
delete admin-access-ipv6-address ipv6-network MyIPv6Network
```

delete admin-access-ip-address-all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all the configured IPv4 and IPv6 addresses, from which the administrator can remotely access the appliance according to configuration.

See:

- *"add admin-access-ipv4-address single-ipv4-address" on page 90*
- *"add admin-access-ipv6-address single-ipv6-address" on page 97*
- *"add admin-access-ipv4-address network-ipv4-address" on page 91*
- *"add admin-access-ipv6-address network-ipv6-address" on page 98*
- *"show admin-access-ipv4-addresses" on page 93*
- *"delete admin-access-ipv4-address" on page 94*
- *"delete admin-access-ipv4-address-all" on page 95*
- *"delete admin-access-ipv6-address ipv6-address" on page 100*
- *"delete admin-access-ipv6-address ipv6-network" on page 101*

Syntax

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

Configuring Administrator Access through WebUI and SSH

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure various parameters for administrator access to the appliance through WebUI and SSH.

set admin-access

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures various parameters for administrator access to the appliance through WebUI and SSH.

See *"show admin-access" on page 106*.

Syntax

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

Parameters

Parameter	Description
{true | false}	Enables (`true`) or disables (`false`) administrator access through the specified interface
allowed-ipv4-addresses	Configures the administrator access permissions policy for source IP addresses
interfaces	Specifies the interface, through which the access is allowed
ssh-access-port	Configures the port number for SSH access
support-weak-tls-version	**Best Practice** - For security reasons, it is highly recommended to keep the default value "`false`". Changing the value to "`true`" exposes the administration portal to at- tacks that use vulnerabilities like Heartbleed (CVE-2014-0160). If you configure the value "`true`", support of TLSv1.0 is added back to the administration portal to allow connectivity with old web browsers (usually, those released prior to 2014).
web-access-port	Configures the port number for HTTPS access to WebUI

Example Command

```
set admin-access interfaces LAN access true web-access-port 8080
ssh-access-port 9090 allowed-ipv4-addresses any
```

show admin-access

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configured settings of administrator access to the appliance through WebUI and SSH.

See *"set admin-access" on page 104*.

Syntax

```
show admin-access
```

set admin-2fa

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Enable/disable Two-Factor Authentication for all administrators to access the Security Gateway. All administrators must have both an email address and phone number configured. If any administrators are missing either an email address or a phone number, you cannot enable the feature. Once enabled, Two-Factor Authentication is required for all logins/access to the gateway.

Before Two-Factor Authentication is activated for the gateway, all administrators receive an email explaining how to use the Authenticator app. The email also contains a QR code and emergency keys. Confirm that you received the email or request to resend (yes/resend/quit). All administrators will receive an email containing instructions and their own keys.

See *"show admin-2fa" on the next page*.

Syntax

```
set admin-2fa { on | off }
```

Parameters

Parameter	Description
`on`	Two-Factor Authentication is enabled.
`off`	Two-Factor Authentication is disabled.

Example Command

```
set admin-2fa on
```

show admin-2fa

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows if Two-Factor Authentication is enabled or disabled:

- `enabled: true` - Enabled
- `enabled: false` - Disabled

See *"set admin-2fa" on the previous page*.

Syntax

```
show admin-2fa
```

Example Output

```
>show admin-2fa
enabled:              true
```

Configuring Messages for SSH Login

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure messages for SSH Login.

set message

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures a message to show during the SSH login.

See *"show message" on page 110*.

Syntax

```
set message <type> { on | off } [ line msgvalue "<text>" ]
```

Parameters

Parameter	Description
type	Configures the type of the message. Options: ■ `banner` ■ `caption` - currently not supported ■ `motd` - currently not supported
text	Configures the message text

Example Command

```
set message banner on line msgvalue "My Banner Message"
```

show message

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configured message for the SSH login.

See *"set message" on page 109*.

Syntax

```
show message <type>
```

Parameters

Parameter	Description
type	Specifies the type of the message. Options: ■ `banner` ■ `caption` - currently not supported ■ `motd` - currently not supported

Example Command

```
show message banner
```

Configuring Local Users

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure local users on the appliance.

add local-user

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new locally-defined user object and configure its remote access VPN permissions.

See:

- *"add local-user" above*
- *"show local-user" on page 119*
- *"show local-users" on page 121*
- *"delete local-user" on page 123*
- *"delete local-user all" on page 124*
- *"delete local-users expired" on page 125*

Syntax

```
add local-user name <name> { password <password> | password-hash
<password-hash> }
      [ comments "<comments>" ]
      [ email <email> ]
      [ is-temp-user { false | true expiration-date <expiration-
date> [ expiration-time <expiration-time> ] } ]
      [ phone-number <phone-number> ]
      [ remote-access-always-on {true | false} ]
```

Parameters

Parameter	Description
comments	Configures the comment text A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '`(`' (opening round bracket) ■ '`)`' (closing round bracket) ■ ':' (colon) ■ '`@`' (at)
email	Configures the user's email **Note** - This parameter is supported starting from the R81.10.05 version.
expiration-date	Configures the expiration date for a temporary user in format YYYY-MM-DD
expiration-time	Configures the expiration time for a temporary user in format HH:MM
is-temp-user	Configures the user entry as temporary (`true`) or not (`false`)
name	Configures the user's name in the local database A string that contains up to 64 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '`@`' (at)
password	Configures the user's password in the local database A string that contains alphanumeric and special characters.

Parameter	Description
password-hash	Configures the DES hash of the password string (used for importing a database). The password is not visible as text on the command line, or in the command history. Use this option if you want to change passwords using a script. To generate a password-hash, you can use this command on any Check Point Quantum Spark Appliance (in the Expert mode): `cryptpw -a des <password string> <salt>`
phone-number	Configures the user's phone number **Note** - This parameter is supported starting from the R81.10.05 version.
remote-access-always-on	Configures the remote access VPN permission as always enabled (`true`) or not (`false`)

Example Command

```
add local-user name user1 password-hash TZXPLs20bN0RA comments
"This is User 1" is-temp-user true expiration-date 2021-01-30
expiration-time 23:59 remote-access-always-on true
```

set local-user

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing locally-defined user object.

See:

- *"add local-user" on page 112*
- *"show local-user" on page 119*
- *"show local-users" on page 121*
- *"delete local-user" on page 123*
- *"delete local-user all" on page 124*
- *"delete local-users expired" on page 125*

Syntax

```
set local-user name <name> email <email> phone-number <phone-
number>
      [ comments "comments" ]
      [ is-temp-user { false | true expiration-date <expiration-
date> [ expiration-time <expiration-time>] } ]
      [ new-name <new-name> ]
      [ { password-hash <password-hash> | password <password> } ]
      [ remote-access-always-on <remote-access-always-on> ]
```

Parameters

Parameter	Description
comments	Configures the comment text A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
expiration-date	Configures the expiration date for a temporary user in format YYYY-MM-DD
expiration-time	Configures the expiration time for a temporary user in format HH:MM
is-temp-user	Configures the user entry as temporary (`true`) or not (`false`)
name	Specifies the user's name in the local database Press the TAB key to see the available options.
new-name	Configures the new user's name in the local database A string that contains up to 64 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '@' (at)
email	The email of the user **Note** - This parameter is supported starting from the R81.10.05 version.
phone-number	The phone number of the user **Note** - This parameter is supported starting from the R81.10.05 version.

Parameter	Description
password	Configures the user's password in the local database A string that contains alphanumeric and special characters.
password-hash	Configures the MD5 of the password string (used for importing a database). The password is not visible as text on the command line, or in the command history. Use this option if you want to change passwords using a script. To generate a password-hash, you can use this command on any Check Point Quantum Spark Appliance (in the Expert mode): `cryptpw -a md5 <password string>`
remote-access-always-on	Configures the remote access VPN permission as always enabled (`true`) or not (`false`)

Example Command

```
set local-user name user1 new-name user2 password-hash
TZXPLs20bN0RA comments "This is User 2" is-temp-user true
expiration-date 2021-01-30 expiration-time 23:59 remote-access-
always-on true
```

set user-management advanced-settings auto-delete-expired-local-users

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures whether to delete the expired locally-defined users automatically.

Syntax

```
set user-management advanced-settings auto-delete-expired-local-
users {true | false}
```

To see the configuration, run:

```
show user-management advanced-settings
```

Example Command

```
set user-management advanced-settings auto-delete-expired-local-
users true
```

show local-user

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of a locally-defined user.

See:

- *"add local-user" on page 112*
- *"show local-user" above*
- *"show local-users" on page 121*
- *"delete local-user" on page 123*
- *"delete local-user all" on page 124*
- *"delete local-users expired" on page 125*

Syntax

```
show local-user name <name>
```

Parameters

Parameter	Description
name	Specifies the user's name in the local database Press the TAB key to see the available options.

Example Output

```
HostName> show local-user name user1
name:                          user1
remote-access-always-on:       true
email:
phone-number:
is-temp-user:                  true
expiration-date:               Fri Sep 03 2021
expiration-time:               23:00
remote-access-on:
created-on:
comments:                      test user
ra-groups-counter:             0
password-hash:                 $5$...(truncated)...2cC
bookmarks:
```

show local-users

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of all locally-defined users.

See:

- *"add local-user" on page 112*
- *"show local-users" above*
- *"show local-user" on page 119*
- *"delete local-user" on page 123*
- *"delete local-user all" on page 124*
- *"delete local-users expired" on page 125*

Syntax

```
show local-users
```

Example Command

```
HostName> show local-users
name      remote-access-always-on   email               phone-number   is-temp-user
expiration-date   expiration-time   remote-access-on   created-on   comments
user1     true                      user1@example.com   1234567890     true           Fri Sep 03
2021   23:00            true                            test user
```

show local-users expired

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows all expired locally-defined users.

See:

- *"add local-user" on page 112*
- *"show local-users expired" above*
- *"show local-user" on page 119*
- *"show local-users" on page 121*
- *"delete local-user" on page 123*
- *"delete local-user all" on page 124*
- *"delete local-users expired" on page 125*

Syntax

```
show local-users expired
```

delete local-user

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing locally-defined user object by user name.

See:

- *"add local-user" on page 112*
- *"delete local-user" above*
- *"show local-user" on page 119*
- *"show local-users" on page 121*
- *"show local-users expired" on page 122*
- *"delete local-user all" on page 124*
- *"delete local-users expired" on page 125*

Syntax

```
delete local-user name <name>
```

Parameters

Parameter	Description
name	Specifies the user's name in the local database

Example Command

```
delete local-user name user1
```

delete local-user all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all existing locally-defined user objects by user name.

See:

- *"add local-user" on page 112*
- *"delete local-user all" above*
- *"show local-user" on page 119*
- *"show local-users" on page 121*
- *"show local-users expired" on page 122*
- *"delete local-user" on page 123*
- *"delete local-users expired" on page 125*

Syntax

```
delete local-user all
```

delete local-users expired

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all expired locally-defined user objects from the database.

See:

- *"add local-user" on page 112*
- *"delete local-users expired" above*
- *"show local-user" on page 119*
- *"show local-users" on page 121*
- *"show local-users expired" on page 122*
- *"delete local-user" on page 123*
- *"delete local-user all" on page 124*

Syntax

```
delete local-users expired
```

Working with Licenses

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to work with local licenses.

fetch license

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Fetches a license from a file in one of these locations:

- Local appliance
- Check Point User Center
- USB device

See *"show license" on page 129*.

Syntax

```
fetch license local [file <file_name>]
fetch license usercenter [ retry 0-60 ]
fetch license usb [ file <file_name> ]
```

Parameters

Parameter	Description
local	Fetches a license from the local appliance You can specify the file that contains the license
usercenter	Fetches a license from the local appliance If the User Center is not available, the appliance tries to fetch the license in the background in defined intervals (minutes).
usb	Fetches a license from the USB device You can specify the file that contains the license
file_name	Specifies the name of the file that contains the license

Return Value

- 0 - success.
- 1 - failure.

Example 1

```
fetch license usb file LicenseFile.xml
```

Example 2

```
fetch license usercenter retry 15
```

show license

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the installed licenses and contract coverage.

See *"fetch license" on page 127*.

Syntax

```
show license
```

Example Output

```
HostName> show license
Host             Expiration  Features
192.168.10.20    never       CPAP-AP1550 CPWIFI-IL CPSB-FW CPSG-C-4-U CPSB-VPN CPSB-IA CPSB-ADNC CPSB-ADNC-M CPSB-SSLVPN-50 CPSB-SSLVPN-
50 CPSB-IPS-S1 CPSB-URLF CPSB-APCL-S1 CPSB-AV CPSB-ABOT-S CPSB-ASPM CPAP-CLOUD-MGMT CK-00-XX-XX-XX-XX-XX

Contract Coverage:

 #   ID          Expiration   SKU
===+===========+============+====================
1  | XXXXXXX   | 16Feb2022  | CPSB-APCL-S-1Y
   +-----------+------------+--------------------
   |Covers:     CPAP-AP1550 CPWIFI-IL CPSB-FW CPSG-C-4-U CPSB-VPN CPSB-IA CPSB-ADNC CPSB-ADNC-M CPSB-SSLVPN-50 CPSB-SSLVPN-50 CPSB-IPS-S1
CPSB-URLF CPSB-APCL-S1 CPSB-AV CPSB-ABOT-S CPSB-ASPM CPAP-CLOUD-MGMT CK-00-XX-XX-XX-XX-XX
===+===========+============+====================
... ... (truncated for brevity) ... ...
===+===========+============+====================
10 | YYYYYYY   | 16Feb2022  | CPES-SS-PREMIUM-1550W-BUN-ADD
   +-----------+------------+--------------------
   |Covers:     CPAP-AP1550 CPWIFI-IL CPSB-FW CPSG-C-4-U CPSB-VPN CPSB-IA CPSB-ADNC CPSB-ADNC-M CPSB-SSLVPN-50 CPSB-SSLVPN-50 CPSB-IPS-S1
CPSB-URLF CPSB-APCL-S1 CPSB-AV CPSB-ABOT-S CPSB-ASPM CPAP-CLOUD-MGMT CK-00-XX-XX-XX-XX-XX
===+===========+============+====================
HostName>
```

Configuring Proxy

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure proxy settings the appliance must use to connect to Check Point update and license servers.

set proxy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure an IPv4 proxy server to connect to Check Point servers to get updates and licenses.

See:

- *"show proxy" on page 132*
- *"delete proxy" on page 133*

Syntax

```
set proxy
      {enable | disable}
      port <port_number>
      server {<hostname> | <ipv4_address>}
```

Parameters

Parameter	Description
{enable | disable}	Enables or disables the use of a proxy server
port	Configures the proxy port
server	Configures the proxy server - enter a Host name or an IPv4 address

Example Command

```
set proxy server MyProxy.com port 8080
set proxy enable
```

show proxy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the IPv4 proxy server configuration.

See:

- *"set proxy" on page 131*
- *"delete proxy" on page 133*

Syntax

```
show proxy
```

Example Output

```
HostName> show proxy
use-proxy:                      true
server:                         proxy.example.com
port:                           8080

HostName>
```

delete proxy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete the configured IPv4 proxy server settings.

See:

- *"set proxy" on page 131*
- *"show proxy" on page 132*

Syntax

```
delete proxy
```

Customizing the WebUI

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

set ui-settings use-custom-webui-logo

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 {false | true custom-webui-
logo-url <custom-webui-logo-url> }
```

Parameters

Parameter	Description
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.
custom-webui-logo-url	Clicking the company logo in the web interface opens this URL

Example Command

```
set ui-settings use-custom-webui-logo true custom-webui-logo-url
http://example.com/mylogo.png
```

set ui-settings advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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> ]
```

Example Command

```
set ui-settings advanced-settings AboutConfigCustomLogos custom-
webui-logo-url urlWithHttp use-custom-webui-logo true
```

show ui-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows web interface settings and customizations.

Syntax

```
show ui-settings
```

Example Command

```
show ui-settings
```

show ui-settings advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows web Interface advanced settings.

Syntax

```
show ui-settings advanced-settings
```

Example Command

```
show ui-settings advanced-settings
```

show system-settings is-custom-branding

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
```

Example Command

```
show system-settings is-custom-branding
```

Configuring Interfaces

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure different interfaces on the appliance.

set interface ipv4-address

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an IPv4 address and DNSv4 servers on the local interface / connection.

See:

- Other "`set`" commands
- *"show interface" on page 156*
- *"delete interface" on page 166*

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> ] ]
]
```

```
set interface <name> ipv4-address <ipv4-address> 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	Configures the default gateway.
dns-primary	Configures the IPv4 address of the first DNS server.
dns-secondary	Configures the IPv4 address of the second DNS server.
dns-tertiary	Configures the IPv4 address of the third DNS server.
ipv4-address	Configures the IPv4 address.
mask-length	Configures the subnet mask length.
name	Specifies the interface / connection. Press the TAB key to see the available options.
subnet-mask	Configures the IPv4 subnet mask.

Example Command

```
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 ipv6-address

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an IPv6 address on the local interface / connection.

See:

- Other "`set`" commands
- *"show interface" on page 156*
- *"delete interface" on page 166*

Syntax

```
set interface <name> ipv6-address <ip6-address> ipv6-prefix-length
<ipv6-prefix-length>
```

Parameters

Parameter	Description
name	Specifies the interface / connection. Press the TAB key to see the available options.
ipv6-address	Configures the IPv6 address of the interface.
ipv6-prefix-length	Configures the IPv6 prefix length.

Example Command

```
set interface My_Network ipv6-address
2001:db8:3333:4444:5555:6666:7777:8888 ipv6-prefix-length 64
```

set interface state

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables or disables an existing local network / interface.

See:

- Other "`set`" commands
- *"show interface" on page 156*
- *"delete interface" on page 166*

Syntax

```
set interface <name> state { on | off }
```

Parameters

Parameter	Description
name	Specifies the interface / connection. Press the TAB key to see the available options.

Example Command

```
set interface My_Network state on
```

set interface description

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures a description for an existing local interface / connection.

See:

- Other "`set`" commands
- *"show interface" on page 156*
- *"delete interface" on page 166*

Syntax

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

Parameters

Parameter	Description
name	Specifies the interface / connection. Press the TAB key to see the available options.
description	Configures the description text. A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '`(`' (opening round bracket) ■ '`)`' (closing round bracket) ■ ':' (colon) ■ '`@`' (at)

Example Command

```
set interface My_Network description "This is a my internal
network"
```

set interface auto-negotiation mtu link-speed

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures networking settings on an existing local interface / IPv4 connection.

See:

- Other "`set`" commands
- *"show interface" on page 156*
- *"delete interface" on page 166*

Syntax

```
set interface <name> [ auto-negotiation {on | off} ] [ link-speed
<link-speed> ] [ mtu 68-1500 ]
```

Parameters

Parameter	Description
auto-negotiation	Controls whether the interface configures the link speed automatically (`on`) or manually (`off`).
link-speed	Configures the link speed of the interface manually: ■ `1/full` - 1 Gbps/Full duplex ■ `1/half` - 1 Gbps/Half duplex ■ `100/full` - 100 Mbps/Full duplex ■ `100/half` - 100 Mbps/Half duplex ■ `100BaseFx` - 100Base-FX ■ `10/full` - 10 Mbps/Full duplex ■ `10/half` - 10 Mbps/Half duplex
mtu	Configures the Maximum Transmission Unit size (in bytes).
name	Specifies the interface / connection. Press the TAB key to see the available options.

Example Command

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

set interface unassigned

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Removes a physical interface from existing networks, in which it is configured.

See:

- Other "`set`" commands
- *"show interface" on page 156*
- *"delete interface" on page 166*

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the local interface / connection. Press the TAB key to see the available options.

Example Command

```
set interface LAN2 unassigned
```

set interface monitor-mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the monitor mode on an existing local interface / connection.

See *"Configuring Monitor Mode" on page 1555*.

See:

- Other "`set`" commands
- *"show interface" on page 156*
- *"delete interface" on page 166*

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.

Example Command

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

set interface mac-address-override exclude-from-dns-proxy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings on an existing local interface / connection:

- Custom MAC address
- Exclusion from DNS Proxy

See:

- Other "`set`" commands
- *"show interface" on page 156*
- *"delete interface" on page 166*

Syntax

```
set interface <name> [ mac-address-override <mac-address-override>
] [ exclude-from-dns-proxy {on | off} ]
```

Parameters

Parameter	Description
name	Specifies the interface / connection. Press the TAB key to see the available options.
mac-address-override	Configures the MAC address (to override the default MAC address).
exclude-from-dns- proxy	Controls whether to exclude (`on`) or not (`off`) the interface / connection from the DNS proxy.

Example Command

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

set interface lan-access lan-access-track

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the automatic access policy for an existing local interface / connection.

Important - This configuration applies only if the appliance is Locally Managed.

See:

- Other "`set`" commands
- *"show interface" on page 156*
- *"delete interface" on page 166*

Syntax

```
set interface <name> [ lan-access {accept | block} ] [ lan-access-
track {log | none}
```

Parameters

Parameter	Description
lan-access	Enables (`accept`) or disables (`block`) the access from the specified interface / connection to local networks.
lan-access-track	Controls whether to generate logs (`log`) or not (`none`) for the traffic from the specified interface / connection to local networks.
name	Specifies the interface / connection. Press the TAB key to see the available options.

Example Command

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

set interface <LAN> enable-port-mirroring

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

All traffic that goes through one or more LAN ports of the appliance can be duplicated into one designated mirror port.

For example, all traffic that passes through LAN1 and LAN2 ports is duplicated into LAN5 port, which is configured as the mirror port. If an external device is connected to the mirror port, it receives all traffic that goes through LAN1/LAN2 of the appliance. This enables you to monitor traffic that goes through the appliance from the external device.

- You can only configure one port to be mirrored at a time.
- You can configure more than one port to be mirrored to the same port.

See:

- Other "`set`" commands
- *"show interface" on page 156*
- *"delete interface" on page 166*

Syntax

```
set interface <LAN> enable-port-mirroring { on | off } port <LAN>
```

Parameters

Parameter	Description
interface <LAN>	The LAN port to be mirrored.
port <LAN>	The LAN port to which the traffic will be mirrored.

Example Command

```
set interface LAN1 enable-port-mirroring on port LAN5
set interface LAN2 enable-port-mirroring on port LAN5
```

To see the mirror configuration

1. Run:

```
show interface LAN5
```

2. Examine these rows:

Parameter	Description
is-mirror-enabled	Indicates if this interface is used as a mirror port. Values: ■ `true` ■ `false`
mirrored-ports	List of LAN ports that are mirrored to this port.
enable-port-mirroring	Indicates if this port is mirrored to another port. Values: ■ `true` - enabled ■ `false` - disabled

Example:

```
show interface LAN5
...(truncated for brevity)...
is-mirror-enabled:            true
mirrored-ports:               LAN1,LAN2
enable-port-mirroring:        false
...(truncated for brevity)...
```

LAN5 is used as the mirror port, but is not mirrored to another port.

set interface hotspot

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to redirect users to the Hotspot portal before allowing access from an existing local interface / connection.

See:

- Other "`set`" commands
- *"show interface" on page 156*
- *"delete interface" on page 166*

Syntax

```
set interface <name> hotspot {on | off}
```

Parameters

Parameter	Description
name	Specifies the interface / connection. Press the TAB key to see the available options.
hotspot	Controls whether to redirect (`on`) or not (`off`) users to the Hotspot portal.

Example Command

```
set interface My_Network hotspot on
```

set interface is-prefix-delegation

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the prefix delegation for an IPv6 interface / connection.

See:

- Other "`set`" commands
- *"show interface" on page 156*
- *"delete interface" on page 166*

Syntax

```
set interface <name> is-prefix-delegation true
      [ prefix-delegation-internet-connection <prefix-delegation-
internet-connection> ]
      [ prefix-delegation-prefix-length <prefix-delegation-prefix-
length> ]
      [ prefix-delegation-subnet <prefix-delegation-subnet> ]
```

```
set interface <name> is-prefix-delegation false
```

Parameters

Parameter	Description
is-prefix-delegation	Enables (`true`) or disables (`false`) the IPv6 prefix delegation for this interface / connection.
name	Specifies the interface / connection. Press the TAB key to see the available options.
prefix-delegation-internet-connection	Specifies the IPv6 Internet connection, from which to delegate the IPv6 prefix. Press the TAB key to see the available options.
prefix-delegation-prefix-length	Configures the IPv6 prefix length for prefix delegation.
prefix-delegation-subnet	Configures the IPv6 subnet to add to the delegated IPv6 prefix.

Example Command

```
set interface My_Network is-prefix-delegation true prefix-
delegation-internet-connection MyConnection prefix-delegation-
subnet 2001:db8:3333:4444:5555:6666:7777:0000 prefix-delegation-
prefix-length 64
```

show interface

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration and details of a specified local interface or Internet connection.

See:

- The "set" commands
- *"show interfaces" on page 161*
- *"delete interface" on page 166*

Syntax

```
show interface <name>
```

Parameters

Parameter	Description
name	Specifies the interface / connection. Press the TAB key to see the available options.

Example Command

```
MyAppliance> show interface Internet1
dhcp-exclude-end-range:
vti-is-numbered:
dhcp-range-end:
bond-master:
lan-access-track:
prefix-delegation-subnet:
other-config-flag:            off
alias-physical-port:
bridge-stp-hello-time:        2
managed-config-flag:          off
rts-threshold:                2346
subnet-mask:                  255.255.255.0
alias-id:                     1
ssid:
mac-address:
min-advertisement-interval:
bond-mode:                    802.3ad
dns-primary:
port:
xr:                           off
vti-number:                   0
dhcp-ipv6-range-end:
dns-tertiary:
mac-address-override:
tkip-group-key-update-interval:600
max-advertisement-interval:   600
advertisement-lifetime:
default-gw:
dhcp-ipv6:
type:                         internet
is-mirror-enabled:
internet-connection:          table: 0xf5ac9bb0
mirrored-ports:
network-ports:
bridge-stp-aging-time:        20
802dot1x-authentication:      off
wds-peer-mac-address:
dhcp-options:                 table: 0xf5acbe98
dns-ipv6 secondary:
dhcp-ipv6-exclude-end-range:
interface-type:               internet-connection
```

```
exclude-from-dns-proxy:       off
relay-secondary:
display-name:                 Internet1
dhcp-exclude-start-range:
name:                         Internet1
use-defined-networks:         false
dns-ipv6:                     auto
bond-mii-interval:            100
dhcp-range-start:
guest-wireless:
ipv6-prefix-length:           64
link-speed:
use-router-advertisement:     off
dhcp:                         on
stp-priority:                 128
peer:
bridge-log-dropped-non-iP:    off
station-to-station:           allow
master-key-update-interval:   86400
dns-ipv6 tertiary:
is-bridge-fw-enabled:         on
lan-mac-filtering:            off
ipv6-address:
secondary:
cluster-status:               non-ha
is-prefix-delegation:         false
wireless-radio-mode:
lan-access:
protected-mgmt-frames:        off
description:
vlan:                         1
is-connection-static:         true
mask-length:                  24
password:
interface:                    WAN
include-ip-pool:
exclude-ip-pool:
hop-limit:                    64
wpa-authenticate-using:       password
wmm:                          on
local-bridge-interface-name:
fragmentation-threshold:      2346
dhcp-ipv6-exclude-start-range:
bridge-anti-spoofing:         off
status:                       1/full
```

```
               table: 0xf5acf0d0
802dot1x-re-authentication-frequency:
dtim-period:                   1
bridge-range:
vlan-physical-port:
bridge-stp-forward-delay:      15
stp:                           off
include-ipv6-pool:
inheritSwitchSettings:
wds:                           off

MyAppliance>
```

show interfaces

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the list (or table) with the local interfaces and Internet connections with these details:

- Interface IPv4 address
- Interface IPv6 address
- Interface Status
- Interface Description (use the parameter "`all`")
- Interface IPv4 Mask Length (use the parameter "`table`")
- Interface IPv6 Prefix Length (use the parameter "`table`")
- VLAN Physical Port (use the parameter "`table`")

See:

- The "set" commands
- *"show interface" on page 156*
- *"delete interface" on page 166*

Syntax

```
show interfaces [all | table]
```

Example 1

```
MyAppliance> show interfaces
name:                           myappliance
ipv4-address:                   192.168.252.1
ipv6-address:
status:                         off

name:                           LAN1
ipv4-address:                   192.168.2.1
ipv6-address:
status:                         1/full

name:                           LAN2
ipv4-address:
ipv6-address:
status:                         off

name:                           LAN3
ipv4-address:                   192.168.200.1
ipv6-address:
status:                         disconnected

name:                           LAN4
ipv4-address:
ipv6-address:
status:                         off

name:                           LAN5
ipv4-address:
ipv6-address:
status:                         off

name:                           Internet1
ipv4-address:                   172.30.40.50
ipv6-address:
status:                         1/full

MyAppliance>
```

Example 2

```
MyAppliance> show interfaces all
name:                          myappliance
ipv4-address:                  192.168.252.1
ipv6-address:
status:                        off
mac-address:                   XX:XX:XX:XX:XX:XX
description:

name:                          LAN1
ipv4-address:                  192.168.2.1
ipv6-address:
status:                        1/full
mac-address:                   YY:YY:YY:YY:YY:YY
description:

name:                          LAN2
ipv4-address:
ipv6-address:
status:                        off
mac-address:                   YY:YY:YY:YY:YY:YY
description:

name:                          LAN3
ipv4-address:                  192.168.200.1
ipv6-address:
status:                        disconnected
mac-address:                   YY:YY:YY:YY:YY:YY
description:

name:                          LAN4
ipv4-address:
ipv6-address:
status:                        off
mac-address:                   YY:YY:YY:YY:YY:YY
description:

name:                          LAN5
ipv4-address:
ipv6-address:
status:                        off
mac-address:                   YY:YY:YY:YY:YY:YY
description:

name:                          Internet1
ipv4-address:                  172.30.40.50
ipv6-address:
status:                        1/full
```

```
mac-address:
description:

MyAppliance>
```

Example 3

```
MyAppliance> show interfaces table
name              ipv4-address      mask-length  ipv6-address
                   ipv6-prefix-lengthassignment           status
       mac-address           vlan-physical-port
LAN1              192.168.2.1       24
                   64            ASSIGNMENT.SEPAR...  1/full
  00:50:56:95:c4:5c
LAN2                                 0
                   64            ASSIGNMENT.UNASS...  off
LAN3              192.168.200.1     24
                   64            ASSIGNMENT.SEPAR...  1/full
  00:50:56:95:c4:5c
LAN4                                 0
                   64            ASSIGNMENT.UNASS...  off
LAN5                                 0
                   64            ASSIGNMENT.UNASS...  off
Internet1         172.30.40.50      24
                   64            ASSIGNMENT.SEPAR...  1/full
MyAppliance>
```

Example 4 (for IPv6 loopback)

```
MyAppliance> show interface-loopback
name:                    loop00
ipv4-address:            12.0.0.1
ipv6-address:            12::1
```

delete interface

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing interface / connection.

Syntax

```
delete interface <name>
```

Parameters

Parameter	Description
name	Specifies the interface / connection Press the TAB key to see the available options.

Example Command

```
delete interface My_Network
```

Configuring the WAN Interface

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

This section provides commands to configure the WAN interface.

add interface WAN

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Assign WAN to a separate (LAN) network.

See:

- *"add interface WAN vlan" on the next page*
- *"set interface WAN" on page 168*
- *"set interface WAN vlan" on page 169*

Syntax

```
add interface WAN ipv4-address <ipv4-address> subnet-mask <subnet-mask>
```

Parameters

Parameter	Description
ipv4-address	The IPv4 address
subnet-mask	Subnet mask

Example Command

```
add interface WAN ipv4-address 192.168.20.100 subnet-mask 255.255.255.0
```

add interface WAN vlan

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Create VLAN over flexi-WAN.

See:

- *"add interface WAN vlan" above*
- *"set interface WAN" on the next page*
- *"set interface WAN vlan" on page 169*

Syntax

```
add interface WAN vlan <VLAN_ID> ipv4-address <ip4-address> subnet-mask <subnet-mask>
```

Parameters

Parameter	Description
vlan	VLAN ID
ipv4-address	The IPv4 address of the VLAN interface
subnet-mask	Subnet mask

Example Command

```
add interface WAN vlan 100 ipv4-address 192.168.20.100 subnet-mask
255.255.255.0
```

set interface WAN

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure WAN as a separate (LAN) network.

See:

- *"set interface WAN" above*
- *"add interface WAN vlan" on the previous page*
- *"set interface WAN vlan" on the next page*

Syntax

```
set interface WAN ipv4-address <ipv4-address> subnet-mask <subnet-
mask>
```

Parameters

Parameter	Description
ipv4-address	The IPv4 address
subnet-mask	Subnet mask

Example Command

```
set interface WAN ipv4-address 192.168.20.100 subnet-mask
255.255.0.0
```

set interface WAN vlan

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure settings for VLAN over flexi-WAN.

See:

- *"set interface WAN vlan" above*
- *"add interface WAN vlan" on page 167*
- *"set interface WAN" on the previous page*

Syntax

```
set interface WAN vlan <VLAN_ID> ipv4-address <ip4-address>
subnet-mask <subnet-mask>
```

Parameters

Parameter	Description
vlan	VLAN ID
ipv4-address	The IPv4 address of the VLAN interface
subnet-mask	Subnet mask

Example Command

```
set interface WAN vlan 100 ipv4-address 192.168.20.100 subnet-mask
255.255.255.0
```

Configuring Bond Interfaces

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

This section provides commands to configure Bond interfaces.

add interface-bond

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Create a new bond interface that contains two subordinate interfaces.

Note - The appliance gives names to bond interfaces automatically, starting with 0:

- `LANBOND0`
- `LANBOND1`
- and so on

See:

- *"add interface-bond" above*
- *"set interface-bond add-member" on page 176*
- *"set interface-bond remove-member" on page 177*
- *"show interface-bond" on page 178*
- *"show interfaces-bond" on page 179*
- *"delete interface-bond" on page 180*

Syntax

```
add interface-bond
      slave-port-1 <name-of-interface-1>
      slave-port-2 <name-of-interface-2>
      bond-mode
            802.3ad
                  [ bond-hash-policy <bond-hash-policy> ]
                  [ bond-mii-interval <bond-mii-interval> ]
            high-availability
                  [ bond-master <name-of-subordinate-interface> ]
                  [ bond-mii-interval <bond-mii-interval> ]
            round-robin
                  [ bond-mii-interval <bond-mii-interval> ]
            xor
                  [ bond-hash-policy <bond-hash-policy> ]
                  [ bond-mii-interval <bond-mii-interval> ]
      ipv4-address <ipv4-address> {mask-length <mask-length> |
subnet-mask <subnet-mask>}
```

Notes:

- These parameters are mandatory:
  - `slave-port-1`
  - `slave-port-2`
  - `bond-master` (High Availability mode only)
  - `bond-mode`
  - `ipv4-address`
- When you create a new bond interface, you can add only two subordinate interfaces.
  To add more subordinate interfaces, use the "*"set interface-bond add-member" on page 176*" command.

Parameters

Parameter	Description
slave-port-1	The name of the first subordinate interface. Press the TAB key to see the available options. This interface must be unassigned, disabled, and without VLANs.
slave-port-2	Name of the second subordinate interface. Press the TAB key to see the available options. This interface must be unassigned, disabled, and without VLANs.
bond-mode	The bond operation mode: ■ `802.3ad` - LACP ■ `high-availability` - Active / Backup ■ `round-robin` - Round Robin ■ `xor` - XOR
bond-hash policy	The bond hash policy: ■ `layer2` - Layer 2 only ■ `layer2_3` - Layer 2 and Layer 3 ■ `layer3_4` - Layer 3 and Layer 4 Applies only to these bond modes: ■ `802.3ad` - LACP ■ `xor` - XOR
bond-master	Name of the leading subordinate interface in the bond interface. Applies only to the "`high-availability`" mode.
bond-mii-interval	The bond MII interval (in milliseconds). Range: 0 - 5000 Default: 100
ipv4-address	IPv4 address of the bond interface.
mask-length	IPv4 mask length for the bond interface.
subnet-mask	IPv4 subnet mask for the bond interface.

Example Commands

```
add interface-bond slave-port-1 LAN2 slave-port-2 LAN3 bond-mode
high-availability bond-master LAN2 ipv4-address 172.30.40.50
subnet-mask 255.255.255.0
```

```
add interface-bond slave-port-1 LAN4 slave-port-2 LAN5 bond-mode
xor bond-hash-policy layer2 bond-mii-interval 200 ipv4-address
172.30.50.60 mask-length 24
```

set interface-bond

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the settings for an existing bond interface.

See:

- *"add interface-bond" on page 170*
- *"set interface-bond add-member" on page 176*
- *"set interface-bond remove-member" on page 177*
- *"show interface-bond" on page 178*
- *"show interfaces-bond" on page 179*
- *"delete interface-bond" on page 180*

Syntax

```
set interface-bond <Name of Bond Interface>
      [ bond-mode <bond-mode> ]
      [ bond-master <bond-master> ]
      [ bond-hash-policy <bond-hash-policy> ]
      [ bond-mii-interval <bond-mii-interval> ]
```

Parameters

Parameter	Description
interface-bond	Name of the bond interface. Press the TAB key to see the available options.
bond-mode	The bond operation mode: ■ `8023ad` - LACP ■ `high-availability` - Active / Backup ■ `round-robin` - Round Robin ■ `xor` - XOR
bond-master	Name of the primary subordinate interface. Press the TAB key to see the available options. Applies only to the "`high-availability`" (Active / Backup) mode.

Parameter	Description
bond-hash-policy	The bond hash policy: ■ `layer2` - Layer 2 only ■ `layer2_3` - Layer 2 and Layer 3 ■ `layer3_4` - Layer 3 and Layer 4 Applies only to these bond modes: ■ `8023ad` - LACP ■ `xor` - XOR
bond-mii-interval	The bond MII interval (in milliseconds). Range: 0 - 5000 Default: 100

Example Command

```
set interface-bond LANBOND0 bond-mode 8023ad bond-master LAN2
bond-mii-interval 200 bond-hash-policy layer2
```

set interface-bond add-member

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a specified subordinate interface to an existing bond interface.

See:

- *"add interface-bond" on page 170*
- *"set interface-bond add-member" above*
- *"set interface-bond remove-member" on page 177*
- *"show interface-bond" on page 178*
- *"show interfaces-bond" on page 179*
- *"delete interface-bond" on page 180*

Syntax

```
set interface-bond <Name of Bond Interface> add-member <interface>
```

Parameters

Parameter	Description
interface-bond	Name of the bond interface. Press the TAB key to see the available options.
add-member	Name of the subordinate interface to add. Press the TAB key to see the available options. This interface must be unassigned, disabled, and without VLANs.

Example Command

```
set interface-bond LANBOND0 add-member LAN5
```

set interface-bond remove-member

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Removes a specified subordinate interface from an existing bond interface.

See:

- *"add interface-bond" on page 170*
- *"set interface-bond remove-member" above*
- *"set interface-bond add-member" on page 176*
- *"show interface-bond" on page 178*
- *"show interfaces-bond" on page 179*
- *"delete interface-bond" on page 180*

Syntax

```
set interface-bond <name> remove-member <interface>
```

Parameters

Parameter	Description
name	Name of the bond interface. Press the TAB key to see the available options.
remove-member	Name of the bond interface to remove. Press the TAB key to see the available options.

Example Command

```
set interface-bond My_Network remove-member LAN1
```

show interface-bond

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the settings of a specified bond interface.

See:

- *"add interface-bond" on page 170*
- *"show interface-bond" above*
- *"set interface-bond add-member" on page 176*
- *"set interface-bond remove-member" on page 177*
- *"show interface-bond" above*
- *"show interfaces-bond" on page 179*
- *"delete interface-bond" on page 180*

Syntax

```
show interface-bond <Name of Bond Interface>
```

Parameters

Parameter	Description
interface-bond	Name of the bond interface. Press the TAB key to see the available options.

Example Command

```
MyAppliance> show interface-bond LANBOND0
network-ports:                LAN4,LAN5
bond-mode:                    high-availability
bond-master:                  LAN5
bond-mii-interval:            100
bond-hash-policy:             layer2

MyAppliance>
```

show interfaces-bond

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the interfaces in the bond (LAN).

See:

- *"add interface-bond" on page 170*
- *"show interfaces-bond" above*
- *"set interface-bond add-member" on page 176*
- *"set interface-bond remove-member" on page 177*
- *"show interface-bond" on page 178*
- *"show interfaces-bond" above*
- *"delete interface-bond" on page 180*

Syntax

```
show interfaces-bond
```

Example Command

```
MyAppliance> show interfaces-bond
name      network-ports   bond-mode           bond-master   bond-
mii-interval   bond-hash-policy
LANBOND0  LAN4,LAN5       high-availability   LAN5          100
             layer2
MyAppliance>
```

delete interface-bond

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete a specified bond interface.

See:

- *"add interface-bond" on page 170*
- *"delete interface-bond" above*
- *"set interface-bond add-member" on page 176*
- *"set interface-bond remove-member" on page 177*
- *"show interface-bond" on page 178*
- *"show interfaces-bond" on page 179*
- *"delete interface-bond" above*

Syntax

```
delete interface-bond <Name of Bond Interface>
```

Parameters

Parameter	Description
interface-bond	Specified the name of the bond interface. Press the TAB key to see the available options.

Example Command

```
delete interface-bond LANBOND0
```

Configuring VLAN Interfaces

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

This section provides commands to configure VLAN interfaces.

add interface vlan

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures a new 802.1q tag-based VLAN on an existing physical interface.

Important - To configure an existing VLAN interface, use the "`set interface`" commands.

Syntax

```
add interface <name> vlan 1-4094
```

Parameters

Parameter	Description
name	Specifies the name of the physical interface. Press the TAB key to see the available options.

Example Command

```
add interface LAN5 vlan 12
```

Configuring Bridge Interfaces

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

This section provides commands to configure Bridge interfaces.

add bridge

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new bridge interface.

Syntax

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

Parameters

Parameter	Description
name	Bridge name Must be one of these: `br0`, `br1`, `br2`, ..., or `br9`

Example Command

```
add bridge name br7
```

set bridge add member

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds an existing physical interface (or a network object) to an existing bridge interface.

Syntax

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

Parameters

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

Example Command

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

set bridge remove member

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Removes a physical interface (or a network object) from an existing bridge interface.

Syntax

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

Parameters

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

Example Command

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

set bridge stp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing bridge interface.

Syntax

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

Parameters

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

Example Command

```
set bridge br7 stp on
```

show bridge

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration and statistics of a defined bridge.

Syntax

```
show bridge <name>
```

Parameters

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

Example Command

```
show bridge br7
```

show bridges

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows details of all defined bridges.

Syntax

```
show bridges
```

Parameters

Parameter	Description
n/a	

Example Command

```
show bridges
```

delete bridge

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing bridge interface.

Syntax

```
delete bridge <name>
```

Parameters

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

Example Command

```
delete bridge br7
```

Configuring Alias Interfaces

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

This section provides commands to configure alias interfaces.

add interface-alias

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Associate more than one IP address to a network interface.

Syntax

```
add interface-alias alias-physical-port <alias-physical-port> [
ipv4-address <ipv4-address> ] [ {mask-length <mask-length> |
subnet-mask <subnet-mask> } ]
```

Parameters

Parameter	Description
alias-physical-port	The physical port used by the alias network. Separate networks only A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ '/' (slash)
ipv4-address	Enter the IP address of the interface
mask-length	Represents the network's mask length
subnet-mask	The subnet mask of the specified network A subnet mask, or 255.255.255.255

Example Command

```
add interface-alias alias-physical-port My_Network ipv4-address
192.168.1.1 mask-length 20
```

set interface-alias

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the settings for an alias IP.

Syntax

```
set interface-alias <name> [ ipv4-address <ipv4-address> ] [ {
mask-length <mask-length> | subnet-mask <subnet-mask> } ] [ state
<state> ]
```

Parameters

Parameter	Description
ipv4 address	Enter the IP address of the interface
mask-length	Represents the network's mask length
name	Network name A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ '/' (slash)
state	The mode of the network - enabled or disabled Options: on, off
subnet-mask	The subnet mask of the specified network Type: A subnet mask, or 255.255.255.255

Example Command

```
set interface-alias My_Network ipv4-address 192.168.1.1 mask-
length 20 state on
```

delete interface-alias

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete one of multiple IP addresses associated to a network interface.

Syntax

```
delete interface-alias <name>
```

Parameters

Parameter	Description
name	Network name A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ '/' (slash)

Example Command

```
delete interface-alias My_Network
```

Configuring Loopback Interfaces

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

This section provides commands to configure Loopback interfaces.

add interface-loopback

In the R81.10.X releases, this command for the IPv4 loopback is available starting from the R81.10.00 version. IPv6 loopback is available starting from the R81.10.07 version.

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> }
........ipv6-address <ipv6-address> ipv6-prefix-length
<ipv6prefix-length>
```

Parameters

Parameter	Description
ipv4-address	Enter the IP address of the IPv4 interface
mask-length	Represents the network's mask length
subnet-mask	Enter the Subnet mask of the specified network A subnet mask, or 255.255.255.255
ipv6-address	Enter the IP address of the IPv6 interface
ipv6--prefix-length	Represents the prefix length of the IPv6 address.

Example Command

```
add interface-loopback ipv4-address 192.168.1.1 mask-length 20
```

```
add interface-loopback ipv4-address 12.0.0.1 mask-length 24 ipv6-
address 12::1 ipv6-prefix-length 64
```

delete interface-loopback

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing configured loopback interface.

Syntax

```
delete interface-loopback <name>
```

Parameters

Parameter	Description
name	Network name A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ '/' (slash)

Example Command

```
delete interface-loopback My_Network
```

Configuring VPN Tunnel Interfaces (VTI)

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

This section provides commands to configure VPN Tunnel Interfaces (VTI).

add vpn tunnel (VTI)

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new numbered or 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	The IP address of the interface.
peer	Remote peer name as defined in the VPN community. You must define the two peers in the VPN community before you can configure the VTI. The Peer ID is an alpha-numeric character string. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)
remote	Defines the remote peer IPv4 address, used at the peer gateway's point-to-point virtual interface (numbered VTI only).
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. Press the TAB key to see the available options.

Parameter	Description
vpn tunnel	A number identifying the Virtual Tunnel Interface (VTI).

Example Command

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

set vpn tunnel (VTI)

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing Virtual Tunnel Interface (VTI) for route based VPN.

Syntax

```
set vpn tunnel <tunnel> type
      numbered [ local <local> ] [ remote <remote> ] [ peer <peer>
]
      unnumbered [ peer <peer> ] [ internet-connection <internet-
connection> ]
```

Parameters

Parameter	Description
internet-connection	Specifies the local interface for unnumbered VTI. Press the TAB key to see the available options.
local	Configures the IP address of the interface.
peer	Configures the 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. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)
remote	Configures the remote peer IPv4 address, used at the peer gateway's point-to-point virtual interface (numbered VTI only)
tunnel	Configures a number identifying the Virtual Tunnel Interface (VTI)

Parameter	Description
type	Specifies the type of VTI: ■ Numbered VTI uses a specified, static IPv4 addresses for local and remote connections ■ Unnumbered VTI uses the interface and the remote peer name to get addresses

Example Command

```
set vpn tunnel 15 type unnumbered peer Site17 internet-connection
MyConnection
```

show vpn tunnel (VTI)

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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) A number with no fractional part (integer)

Example Command

```
show vpn tunnel 12
```

show vpn tunnels (VTI)

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows all Virtual Tunnel Interfaces (VTIs).

Syntax

```
show vpn tunnels
```

Example Command

```
show vpn tunnels
```

delete vpn tunnel (VTI)

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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) A number with no fractional part (integer)

Example Command

```
delete vpn tunnel 12
```

Configuring DSL Settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

This section provides commands to configure DSL Settings.

set dsl advanced-settings global-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

set dsl advanced-settings standards

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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.

Parameter	Description
vdsl-8d	Supports VDSL Profile 8d.
vdsl-12a	Supports VDSL Profile 12a.
vdsl-12b	Supports VDSL Profile 12b.
vdsl-17a	Supports VDSL Profile 17a.
vdsl-us0	Enables usage of first upstream band in VDSL2.

Example Command

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

show dsl advanced-setting

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show all DSL advanced settings parameters.

Syntax

```
show dsl advanced-settings
```

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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.

Parameter	Description
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.
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 Command

```
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
```

show adsl statistics

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

```
show adsl statistics
```

Example Command

```
show adsl statistics
```

Configuring WLAN Settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

This section provides commands to configure WLAN (Wireless) settings.

delete wlan

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ '/' (slash)

Example Command

```
delete wlan vap My_Network
```

set wlan

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Configures a Virtual Access Point (VAP) wireless network in appliance models that contain wireless options).

Syntax

```
set wlan
      assignment <options>
      {enable | disable}
      security-type <options>
      radio <options>
      ssid <options>
      vap <options>
      wpa-auth-type <options>
      wpa-encryption-type <options>
      advanced-settings <options>
```

Parameters

Parameter	Description
assignment	See *"set wlan assignment" on page 216*
enable | disable	See *"set wlan enable / disable" on page 214*
security-type	See *"set wlan security-type" on page 217*
radio	See *"wlan radio" on page 227*
ssid	See *"set wlan ssid" on page 215*
vap	See *"wlan vaps" on page 233*
wpa-auth-type	See *"set wlan wpa-auth-type" on page 218*
wpa-encryption-type	See *"set wlan wpa-encryption-type" on page 219*
advanced-settings	See *"set wlan advanced-settings" on page 220*

set wlan enable / disable

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables or disables the first wireless network that was created.

Syntax

```
set wlan { enable | disable }
```

Example Command

```
set wlan enable
```

set wlan ssid

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the SSID of the first wireless network that was created.

Syntax

```
set wlan ssid <ssid>
```

Parameters

Parameter	Description
ssid	Specifies the Wireless network name (SSID). Press the TAB key to see the available options.

Example Command

```
set wlan ssid My wireless
```

set wlan assignment

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Assigns the network to the Virtual Access Point.

Syntax

```
set wlan assignment <assignment>
```

Parameters

Parameter	Description
assignment	Specifies the network assigned to the Virtual Access Point. Press the TAB key to see the available options.

Example Command

```
set wlan assignment My_Network
```

set wlan security-type

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the WLAN security type for the first wireless network that was created.

Syntax

```
set wlan security-type <security-type>
```

Parameters

Parameter	Description
security-type	Specifies the WLAN security type: ■ `WPA/WPA2` - WPA/WPA2 ■ `WPA3` - WPA3 (most secure) **Note** - This value is supported starting from the R81.10.05 version. ■ `WPA2` - WPA2 ■ `none` - None

Example Command

```
set wlan security-type WPA2
```

set wlan wpa-auth-type

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the WPA authentication type for the first wireless network that was created.

Syntax

```
set wlan wpa-auth-type
      password-set-as-mac-with-prefix <password> [ hotspot {on |
off} ]
      password <password> [ hotspot {on | off}
      radius hotspot {on | off} ]
```

Parameters

Parameter	Description
password-set-as-mac-with-prefix	Configures the password with a prefix and the WAN MAC address as suffix. Enter the password in lower case without colons.
password	Configures the password.
radius	Configures WLAN to use a RADIUS server (enterprise mode).
hotspot	Enables (`on`) or disables (`off`) the use of the Hotspot of the Virtual Access Point.

Example Command

```
set wlan wpa-auth-type password gTd&3(gha_ hotspot on
```

set wlan wpa-encryption-type

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the WPA encryption type for the first wireless network that was created.

Configures the WPA encryption type for the Virtual Access Point.

Syntax

```
set wlan wpa-encryption-type <wpa-encryption-type>
```

Parameters

Parameter	Description
wpa-encryption-type	Specifies the WPA encryption type: ■ `CCMP-AES` - CCMP-AES (most secure) ■ `TKIP` - TKIP ■ `Auto` - Auto (AES/TKIP)

Example Command

```
set wlan wpa-encryption-type Auto
```

set wlan advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced WLAN settings.

Syntax

```
set wlan <main-wireless-name> advanced-settings
      hide-ssid {on | off}
      protected-mgmt-frames { on | off }
      station-to-station {allow | block}
      wds {on | off}
```

Parameters

Parameter	Description
main-wireless-name	Specifies the name of the main wireless access point. Press the TAB key to see the available options.
hide-ssid	Enables (`on`) or disables (`off`) the broadcasting of the WLAN Service Set Identifier (SSID).
protected-mgmt-frames	Enables (`on`) or disables (`off`) the protection of 802.11 management frames.
station-to-station	Accepts (`allow`) or drops (`block`) the Station-to-Station traffic.
wds	Enables (`on`) or disables (`off`) the Wireless Distribution System.

Example Command

```
set wlan My_Network advanced-settings hide-ssid on station-to-
station allow wds on
```

```
set wlan My_Network advanced-settings protected-mgmt-frames off
```

show wlan

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Shows configuration for wireless networks (relevant to hardware models with wireless).

show wlan

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration of the wireless radio.

Syntax

```
show wlan
```

Example Command

```
show wlan
```

show wlan statistics

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows statistics of the wireless radio.

Syntax

```
show wlan statistics
```

Parameters

Parameter	Description
n/a	

Example Command

```
show wlan statistics
```

wireless-scheduler

Configure the settings for the wireless scheduler.

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

add wireless-scheduler

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add specific times for the wireless scheduler.

Important - During these time periods, the WLAN radio transmitter is active or inactive.

- You control the state of the scheduler with the "`set wlan radio scheduler-mode {off | on}`" command.
- You control the state of the WLAN radio transmitter with the "`set wlan radio scheduler-inactive-period {off | on}`" command.

Syntax

```
add wireless-scheduler time-window radio-band {2.4GHz | 5GHz}
start-time <start-time> end-time <end-time> [ monday {on | off} ]
[ tuesday {on | off} ] [ wednesday {on | off} ] [ thursday {on |
off} ] [ friday {on | off} ] [ saturday {on | off} ] [ sunday {on
| off} ]
```

Parameters

Parameter	Description
radio-band	Specifies the WLAN band. Press the TAB key to see the available options.
start-time	Specifies the start time of the time interval (on the specified day of the week) in format HH:MM.
end-time	Specifies the end time of the time interval (on the specified day of the week) in format HH:MM.
monday	Enables (`on`) or disables (`off`) the time period on this day of the week.
tuesday	Enables (`on`) or disables (`off`) the time period on this day of the week.
wednesday	Enables (`on`) or disables (`off`) the time period on this day of the week.
thursday	Enables (`on`) or disables (`off`) the time period on this day of the week.
friday	Enables (`on`) or disables (`off`) the time period on this day of the week.
saturday	Enables (`on`) or disables (`off`) the time period on this day of the week.
sunday	Enables (`on`) or disables (`off`) the time period on this day of the week.

Example Command

```
add wireless-scheduler time-window radio-band 5GHz start-time
22:00 end-time 23:00 monday on tuesday on wednesday on thursday on
friday on saturday on sunday on
```

set wireless-scheduler

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the wireless scheduler time period.

Important - During these time periods, the WLAN radio transmitter is active or inactive.

- You control the state of the scheduler with the "`set wlan radio scheduler-mode {off | on}`" command.
- You control the state of the WLAN radio transmitter with the "`set wlan radio scheduler-inactive-period {off | on}`" command.

Syntax

```
set wireless-scheduler band {2.4GHz | 5GHz} time-window index
<index> [ start-time <start-time> ] [ end-time <end-time> ] [
monday {on | off} ] [ tuesday {on | off} ] [ wednesday {on | off}
] [ thursday {on | off} ] [ friday {on | off} ] [saturday {on |
off} ] [ sunday {on | off} ]
```

Parameters

Parameter	Description
band	Specifies the WLAN band. Press the TAB key to see the available options.
index	Specifies the number of the configured time period. Press the TAB key to see the available options.
start-time	Specifies the start time of the time interval (on the specified day of the week) in format HH:MM.
end-time	Specifies the end time of the time interval (on the specified day of the week) in format HH:MM.
monday	Enables (`on`) or disables (`off`) the time period on this day of the week.
tuesday	Enables (`on`) or disables (`off`) the time period on this day of the week.
wednesday	Enables (`on`) or disables (`off`) the time period on this day of the week.
thursday	Enables (`on`) or disables (`off`) the time period on this day of the week.
friday	Enables (`on`) or disables (`off`) the time period on this day of the week.
saturday	Enables (`on`) or disables (`off`) the time period on this day of the week.

Parameter	Description
sunday	Enables (`on`) or disables (`off`) the time period on this day of the week.

Example Command

```
set wireless-scheduler band 2.4GHz time-window index 1 start-time
22:00 end-time 23:00 monday on tuesday on wednesday on thursday on
friday on saturday on sunday on
```

delete wireless-scheduler

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes the configured time period in the wireless scheduler.

Syntax

```
delete wireless-scheduler band {2.4GHz | 5GHz} time-window index
<index>
```

Parameters

Parameter	Description
band	Specifies the WLAN band Press the TAB key to see the available options.
index	Specifies the number of the configured time period Press the TAB key to see the available options.

Example Command

```
delete wireless-scheduler band 2.4GHz time-window index 2
```

wlan radio

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

set wlan radio

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the radio settings of wireless antennas.

Syntax

```
set wlan radio [ band {2.4GHz | 5GHz} ]
      channel-width <channel-width>
      channel <channel-number>
      country <country>
      operation-mode <mode>
      scheduler-inactive-period {off | on}
      scheduler-mode {off | on}
      off
      on
```

Parameters

Parameter	Description
band	Specifies the WLAN band. Applies to wireless models that contain a concurrent dual band option using two radio antennas. Press the TAB key to see the available options.
channel-width	Configures the WLAN channel width: ■ `20` - 20 MHz ■ `40` - 40 MHz ■ `80` - 80 MHz ■ `80+80` - 80+80 MHz ■ `160` - 160 MHz ■ `auto` - Automatic
channel	Configures the WLAN channel number: ■ `1 - 165` ■ `auto` - Automatic
country	Configures the WLAN country.

Parameter	Description
operation-mode	Configures the WLAN 802.11 operation mode: ■ `11ac` - 802.11ac (5GHz) ■ `11b` - 802.11b ■ `11n` - 802.11n ■ `11bg` - 802.11bg ■ `11ng` - 802.11ng ■ `11nac` - 802.11n/ac (5GHz) ■ `11g` - 802.11g ■ `11bgnax` - 802.11bgnax (2.4GHz) **Note** - This value is supported starting from the R81.10.05 version. ■ `11anacax` - 802.11anacax (5GHz) **Note** - This value is supported starting from the R81.10.05 version.
scheduler-inactive-period	Controls the WLAN radio transmitter during the configured time periods: ■ `on` - Do not disable the WLAN radio transmitter (make it active) ■ `off` - Disable the WLAN radio transmitter (make it inactive)
scheduler-mode	Enables (`on`) or disables (`off`) the WLAN scheduler.
off	Disables the WLAN radio transmitter (for all WLAN bands, or for the specified WLAN band).
on	Enables the WLAN radio transmitter (for all WLAN bands, or for the specified WLAN band).

Examples

```
set wlan radio country italy operation-mode 11b channel auto
channel-width auto
```

```
set wlan radio band 2.4GHz country italy operation-mode 11b
channel auto channel-width auto
```

```
set wlan radio band 5GHz off
```

set wlan radio advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for the wireless radio.

Syntax

```
set wlan radio [ band {2.4GHz | 5GHz} ] advanced-settings
      [ antenna <antenna> ]
      [ guard-interval <guard-interval> ]
      [ transmitter-power <transmitter-power> ]
```

Parameters

Parameter	Description
band	Specifies the WLAN band. Applies to wireless models that contain a concurrent dual band option using two radio antennas. Press the TAB key to see the available options.
antenna	Specifies the WLAN antenna: ■ `right` - Right ■ `left` - Left ■ `auto` - Automatic Press the TAB key to see the available options.
guard-interval	Specifies the WLAN throughput: ■ `short` - Short ■ `normal` - Normal Press the TAB key to see the available options.
transmitter-power	Specifies the WLAN transmit power (transmit range): ■ `minimum` - Minimum ■ `eighth` - Eighth (12.5%) ■ `quarter` - Quarter (25%) ■ `half` - Half (50%) ■ `full` - Full (100%) Press the TAB key to see the available options. Lower power can help reduce interference to nearby access points.

Example Command

```
set wlan radio advanced-settings antenna auto guard-interval short
transmitter-power minimum
```

show wlan radio

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration of the wireless radio.

Syntax

```
show wlan radio
```

Parameters

Parameter	Description
n/a	

Example Command

```
show wlan radio
```

wlan vaps

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

add wlan vap

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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) A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)

Example Command

```
add wlan vap ssid My wireless band 5GHz
```

set wlan vap enable / disable

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables or disables an existing wireless Virtual Access Point network (VAP).

Syntax

```
set wlan vap <vap>{ enable | disable }
```

Parameters

Parameter	Description
vap	Specifies the name of the Virtual Access Point. Press the TAB key to see the available options.

Example Command

```
set wlan vap My_Network enable
```

set wlan vap ssid

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the SSID of an existing wireless network (VAP).

Syntax

```
set wlan vap <vap> ssid <ssid>
```

Parameters

Parameter	Description
vap	The name of the Virtual Access Point. Press the TAB key to see the available options.
ssid	Configures the Wireless network name (SSID). A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)

Example Command

```
set wlan vap My_Network ssid "My Wireless"
```

set wlan vap assignment

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Assigns the network to the Virtual Access Point.

Syntax

```
set wlan vap <vap> assignment <assignment>
```

Parameters

Parameter	Description
vap	Specifies the name of the Virtual Access Point. Press the TAB key to see the available options.
assignment	Specifies the network assigned to WLAN. Press the TAB key to see the available options.

Example Command

```
set wlan vap My_Network assignment My_Network
```

set wlan vap security-type

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the WLAN security type for the Virtual Access Point.

Syntax

```
set wlan vap <vap> security-type <security-type>
```

Parameters

Parameter	Description
vap	Specifies the name of the Virtual Access Point. Press the TAB key to see the available options.
security-type	Specifies the WLAN security type: ▪ `WPA/WPA2` - WPA/WPA2 ▪ `WPA3` - WPA3 (most secure) **Note** - This value is supported starting from the R81.10.05 version. ▪ `WPA2` - WPA2 ▪ `none` - None

Example Command

```
set wlan vap My_Network security-type WPA2
```

set wlan vap wpa-auth-type

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the WPA authentication type for the Virtual Access Point.

Syntax

```
set wlan vap <vap> wpa-auth-type
      password-set-as-mac-with-prefix <password> [ hotspot {on |
off} ]
      password <password> [ hotspot {on | off}
      radius hotspot {on | off} ]
```

Parameters

Parameter	Description
password-set-as-mac-with-prefix	Configures the password with a prefix and the WAN MAC address as suffix. Enter the password in lower case without colons.
password	Configures the password.
radius	Configures WLAN to use a RADIUS server (enterprise mode).
hotspot	Enables (`on`) or disables (`off`) the use of the Hotspot of the Virtual Access Point.

Example Command

```
set wlan vap My_Network wpa-auth-type password gTd&3(gha_ hotspot
on
```

set wlan vap wpa-encryption-type

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the WPA encryption type for the Virtual Access Point.

Syntax

```
set wlan vap <vap> wpa-encryption-type <wpa-encryption-type>
```

Parameters

Parameter	Description
vap	Specifies the name of the Virtual Access Point. Press the TAB key to see the available options.
wpa-encryption-type	Specifies the WPA encryption type: ■ `CCMP-AES` - CCMP-AES (most secure) ■ `TKIP` - TKIP ■ `Auto` - Auto (AES/TKIP)

Example Command

```
set wlan vap My_Network wpa-encryption-type Auto
```

set wlan vap advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced WLAN settings for the Virtual Access Point.

Syntax

```
set wlan vap <vap> advanced-settings
      hide-ssid {on | off}
      protected-mgmt-frames { on | off }
      station-to-station {allow | block}
      wds {on | off}
```

Parameters

Parameter	Description
vap	Specifies the name of the Virtual Access Point. Press the TAB key to see the available options.
hide-ssid	Enables (`on`) or disables (`off`) the broadcasting of the WLAN Service Set Identifier (SSID).
protected-mgmt-frames	Enables (`on`) or disables (`off`) the protection of 802.11 management frames.
station-to-station	Accepts (`allow`) or drops (`block`) the Station-to-Station traffic.
wds	Enables (`on`) or disables (`off`) the Wireless Distribution System.

Examples

```
set wlan vap My_Network advanced-settings hide-ssid on station-to-station allow wds on
```

```
set wlan vap My_Network advanced-settings protected-mgmt-frames off
```

delete wlan vaps

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all existing wireless Virtual Access Points (VAP).

Syntax

```
delete wlan vaps
```

show wlan vap

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the 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. Press the TAB key to see the available options.

Example Command

```
show wlan vap My_Network
```

show wlan vaps

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows all Virtual Access Points (VAPs or wireless network).

Syntax

```
show wlan vaps
```

show wlan vaps statistics

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the wireless radio statistics for each Virtual Access Point.

Syntax

```
show wlan vaps statistics
```

Working with GRE Tunnels

In the R81.10.X releases, this feature is available starting from the R81.10.07 version.

This section provides commands to work with GRE Tunnels.

Users can create GRE (Generic Routing Encapsulation) tunnels as a LAN interface with a remote peer and route all traffic through them. GRE tunnels can connect to any peer on the cloud and route all traffic from there.

Note - GRE is not secure (by design).

add gre id

In the R81.10.X releases, this command is available starting from the R81.10.07 version.

Description

Create GRE (Generic Routing Encapsulation) tunnel as a LAN interface with a remote peer and route all traffic between the two sites.

Each site has its own routable physical IP address. The GRE tunnel is created on top of a physical network interface, and each tunnel side is assigned a tunnel IP which is different than the physical IP.

Because the GRE tunnel connects two remote sites over the internet, Quantum Spark appliances must support such interfaces.

See also:

- *"show gre tunnels" on page 248*
- *"delete gre tunnel id" on the next page*

Syntax

```
add gre tunnel id <id> local-ip <physical-local-ip> remote-ip
<physical-remote-ip> gre-ip <virtual-local-ip> gre-peer-ip
<virtual-remote-ip> ttl <seconds>
```

Parameters

Parameter	Description
gre-id	The ID that will be part of the GRE interface name. For example, if id is "4", the interface name is "gre4"
physical-local-ip	The IP address on a local interface.
physical-remote-ip	The IP address of the peer.
ttl	Time to Live, how many times to route through the network. The value is usually 255.
virtual-local-ip	The IP address that will be assigned to the GRE interface
virutal-remote-ip	The IP address of the peer on the gre interface

Example Command

```
add gre tunnel id 1 local-ip 172.28.4.172 remote-ip 201.105.75.2
gre-ip 1.1.1.1 gre-peer-ip 1.1.1.2 ttl 255
```

delete gre tunnel id

In the R81.10.X releases, this command is available starting from the R81.10.07 version.

Description

Delete the GRE tunnel.

See also:

- *"add gre id" on the previous page*
- *"show gre tunnels" on the next page*

Syntax

```
delete gre tunnel id <ID>
```

Parameters

Parameter	Description
id	The ID of the GRE interface

Example Command

```
delete gre tunnel id 4
```

show gre tunnels

In the R81.10.X releases, this command is available starting from the R81.10.07 version.

Description

Show the existing GRE tunnels.

See also:

- *"add gre id" on page 246*
- *"delete gre tunnel id" on the previous page*

Syntax

```
show gre tunnels
```

Example Command

```
> show gre tunnels
id    ttl    remote-ip        local-ip         gre-ip     gre-peer-ip
2     255    172.28.4.175     172.28.4.170     5.5.5.1    5.5.5.2
3     255    172.28.4.176     172.28.4.170     7.7.7.1    7.7.7.2
>
```

Configuring the Internet Connections

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the Internet connections.

Configuring the Internet Mode

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the Internet mode when multiple ISP internet connections are configured.

set internet mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures how to use multiple ISP internet connections.

Determines whether the appliance:

- Uses the default High Availability behavior based on priorities of each Internet connection.
- Uses the Load Sharing behavior - distributes the traffic automatically between the configured active Internet connections according to the configured load balancing weights

Syntax

```
set internet mode { load-balancing | high-availability }
```

Example Command

```
set internet mode load-balancing
```

show internet mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configured Internet mode (High Availability or Load Sharing).

Syntax

```
show internet mode
```

Example Output

```
HostName> show internet mode
Load Balancing mode
```

Adding Internet Connections

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

Adds a new internet connection.

add internet-connection interface WAN

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new internet connection using the WAN physical interface (multiple internet connection can engage in High Availability/Load Sharing).

WAN - DHCP

Syntax

```
add internet-connection name "<name>" interface WAN type dhcp
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
vlan-id	VLAN ID A number with no fractional part (integer)
conn-test-timeout	Connection test timeout - When configuring a connection you can define that the command does not return until the connection was established successfully or when a timeout is reached (on failure). The conn-test-timeout is the maximum amount of time (in seconds) to wait until checking the status of the configured Internet connection. ■ If the Internet connection status is "Connected" - The output is "Connection successful." ■ If the Internet connection status is not connected - The output is "Connection failed." By default, there is no check and the output is "Skipped connection test."

WAN - Static IP Address

Syntax

```
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
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
default-gw	WAN default gateway (in the advanced section of PPTP and L2TP)
ipv4-address	IP address field (for static IP and bridge settings)
mask-length	Subnet mask length
subnet-mask	Subnet mask A subnet mask, or 255.255.255.255
dns-primary	First DNS server IP address
dns-secondary	Second DNS server IP address
dns-tertiary	Third DNS server IP address
vlan-id	VLAN ID A number with no fractional part (integer)
conn-test-timeout	Connection test timeout A number with no fractional part (integer)

WAN - L2TP

Syntax

```
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>} { local-ipv4-address <local-ipv4-address> }
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
server	Server IP address
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
username	User name for PPP connection or cellular modem settings Usually <*username*>@<*ISP*>
local-ipv4-address	Local tunnel IP address or Auto for automatic An IP address, or '`auto`'
wan-ipv4-address	WAN IP address wrapper An IP address, or '`auto`'
wan-mask-length	WAN subnet mask length

Parameter	Description
wan-subnet-mask	WAN subnet mask (in the advanced section)
default-gw	WAN default gateway (in the advanced section of PPTP and L2TP)
vlan-id	VLAN ID A number with no fractional part (integer)
conn-test-timeout	Connection test timeout A number with no fractional part (integer)

WAN - PPPoE

Syntax

```
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
{true | false} local-ipv4-address <local-ipv4-address> }
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection 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 An IP address, or '`auto`'
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
username	User name for PPP connection or cellular modem settings Usually <*username*>@<*ISP*>
vlan-id	VLAN ID A number with no fractional part (integer)
conn-test-timeout	Connection test timeout A number with no fractional part (integer)

WAN - PPTP

Syntax

```
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>
```

```
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>} { local-ipv4-address <local-ipv4-address> }
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
server	Server IP address
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
username	User name for PPP connection or cellular modem settings Usually <*username*>@<*ISP*>
local-ipv4-address	Local tunnel IP address or Auto for automatic An IP address, or '`auto`'
wan-ipv4-address	WAN IP address wrapper An IP address, or '`auto`'
wan-mask-length	WAN subnet mask length

Parameter	Description
wan-subnet-mask	WAN subnet mask (in the advanced section)
default-gw	Default Gateway
vlan-id	VLAN ID
conn-test-timeout	Connection test timeout (in seconds)

Example Command

```
add internet-connection name "My connection" interface WAN true
vlan-id 200 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
50
```

add internet-connection interface ADSL

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new internet connection using the ADSL physical interface (multiple internet connection can engage in High Availability/Load Sharing).

ADSL - EoA

Syntax

```
add internet-connection name "<name>" interface ADSL type eoa
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
encapsulation	Encapsulation type for the ADSL connection
vci	VCI value for the ADSL connection A number between 0 and 65535
vpi	VPI value for the ADSL connection A number between 0 and 255
conn-test-timeout	Connection test timeout A number with no fractional part (integer)
standard	The ADSL standard to use Options: multimode, t1413, glite, gdmt, adsl2, adsl2+

ADSL - PPPoE

Syntax

`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 {llc | vcmux} is-unnumbered-pppoe {true | false} local-ipv4-address <local-ipv4-address> vci <vci> vpi <vpi> }`
`add internet-connection name "<name>" interface ADSLtype pppoe username <username> password <password> { encapsulation {llc | vcmux} vci <vci> vpi <vpi>} { conn-test-timeout <conn-test-timeout> standard <standard> }`

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
username	User name for PPP connection or cellular modem settings Usually <*username*>@<*ISP*>
encapsulation	Encapsulation type for the ADSL connection
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 An IP address, or '`auto`'

Parameter	Description
vci	VCI value for the ADSL connection A number between 0 and 65535
vpi	VPI value for the ADSL connection A number between 0 and 255
conn-test-timeout	Connection test timeout A number with no fractional part (integer)
standard	The ADSL standard to use Options: multimode, t1413, glite, gdmt, adsl2, adsl2+

add internet-connection interface DSL

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new internet connection using the DSL physical interface (multiple internet connection can engage in High Availability/Load Sharing).

DSL - IPoE Dynamic

Syntax

```
add internet-connection name "<name>" interface DSL type ipoe-
dynamic
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
conn-test-timeout	Connection test timeout A number with no fractional part (integer)
encapsulation	Encapsulation type for the ADSL connection
vci	VCI value for the ADSL connection A number between 0 and 65535
vlan-id	VLAN ID A number with no fractional part (integer)
vpi	VPI value for the ADSL connection A number between 0 and 255

DSL - IPoE Static

Syntax

```
add internet-connection name "<name>" interface DSL type ipoe-static default-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 <subnet-mask> { dns-primary <dns-primary> dns-secondary <dns-secondary> dns-tertiary <dns-tertiary> }
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
default-gw	WAN default gateway (in the advanced section of PPTP and L2TP)
ipv4-address	IP address field (for static IP and bridge settings)
mask-length	Subnet mask length
subnet-mask	Subnet mask A subnet mask, or 255.255.255.255
dns-primary	First DNS server IP address
dns-secondary	Second DNS server IP address
dns-tertiary	Third DNS server IP address
conn-test-timeout	Connection test timeout A number with no fractional part (integer)
encapsulation	Encapsulation type for the ADSL connection
vci	VCI value for the ADSL connection A number between 0 and 65535

Parameter	Description
vlan-id	VLAN ID A number with no fractional part (integer)
vpi	VPI value for the ADSL connection A number between 0 and 255

DSL - PPPoE

Syntax

```
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 {llc |
vcmux} is-unnumbered-pppoe {true | false} local-ipv4-address
<local-ipv4-address> vci <vci> vpi <vpi> } { encapsulation {llc |
vcmux} vci <vci> vpi <vpi> } { use-connection-as-vlan vlan-id
<vlan-id> } { conn-test-timeout <conn-test-timeout>}
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
username	User name for PPP connection or cellular modem settings Usually *<username>@<ISP>*
encapsulation	Encapsulation type for the ADSL connection
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once
local-ipv4-address	Local tunnel IP address or Auto for automatic An IP address, or '`auto`'
vci	VCI value for the ADSL connection A number between 0 and 65535
vpi	VPI value for the ADSL connection A number between 0 and 255

Parameter	Description
vlan-id	VLAN ID A number with no fractional part (integer)
conn-test-timeout	Connection test timeout A number with no fractional part (integer)

add internet-connection interface DMZ

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new internet connection using the DMZ physical interface (multiple internet connection can engage in High Availability/Load Sharing).

See *"set internet-connection interface DMZ" on page 323*.

DMZ - DHCP

Syntax

```
add internet-connection name "<name>" interface DMZ type dhcp
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options

DMZ - Static IP Address

Syntax

```
add internet-connection name "<name>" interface DMZ type static
ipv4-address <ipv4-address> mask-length <mask-length> default-gw
<default-gw>
```

```
add internet-connection name "<name>" interface DMZ type static
ipv4-address <ipv4-address> subnet-mask <subnet-mask> default-gw
<default-gw> [ 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> ]
[ probe-next-hop {on | off} ] [ probe-servers {on | off} ]
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
ipv4-address	IP address field (for static IP and bridge settings)
mask-length	Subnet mask length
subnet-mask	Subnet mask A subnet mask, or 255.255.255.255
default-gw	WAN default gateway (in the advanced section of PPTP and L2TP)
dns-primary	First DNS server IP address
dns-secondary	Second DNS server IP address
dns-tertiary	Third DNS server IP address
vlan-id	VLAN ID
conn-test-timeout	Connection test timeout

Parameter	Description
probe-next-hop	Automatically detect loss of connectivity to the default gateway
probe-servers	Monitor connection state by sending probe packets to one or more servers on the Internet

DMZ - SFP-DSL - PPPoE

Syntax

```
add internet-connection name interface DMZ dmz-connection sfp-dsl
type pppoe username <username> password <password>
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
username	User name for PPP connection settings Usually <username>@<ISP>
password	Password for PPP connection settings
password-hash	The hash of the user password

Example Command

```
add internet-connection name "My connection" interface DMZ dmz-
connection sfp-dsl type pppoe username admin@exampleisp password
12345
```

DMZ - SFP-DSL - IPoE Dynamic

Syntax

```
add internet-connection name "<name>" interface DMZ dmz-connection
sfp-dsl type ipoe-dynamic
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
conn-test-timeout	Connection test timeout A number with no fractional part (integer)
vci	VCI value for the ADSL connection A number between 0 and 65535
vpi	VPI value for the ADSL connection A number between 0 and 255
encapsulation	Encapsulation type for the ADSL connection Options: ■ llc ■ vcmux

Example Command

```
add internet-connection name "My connection" interface DMZ dmz-
connection sfp-dsl type ipoe-dynamic
```

DMZ - SFP-DSL - IPoE Static

Syntax

```
add internet-connection name "<name>" interface DMZ dmz-connection
sfp-dsl type ipoe-static default-gw ipv4-address <ipv4-address>
mask-length <mask-length>
```

```
add internet-connection name "<name>" interface DMZ dmz-connection
sfp-dsl type ipoe-static default-gw ipv4-address <ipv4-address>
subnet-mask <subnet-mask> { dns-primary <dns-primary> dns-
secondary <dns-secondary> dns-tertiary <dns-tertiary> }
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
ipv4-address	IP address field (for static IP and bridge settings)
default-gw	WAN default gateway (in the advanced section of PPTP and L2TP)
mask-length	Subnet mask length
subnet-mask	Subnet mask Type: A subnet mask, or 255.255.255.255
dns-primary	First DNS server IP address
dns-secondary	Second DNS server IP address
dns-tertiary	Third DNS server IP address

Example Command

```
add internet-connection name "My connection" interface DMZ dmz-
connection sfp-dsl type ipoe-static default-gw ipv4-address
172.15.47.4 mask-length 255.255.255.
```

DMZ - L2TP

Syntax

```
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>} local-ipv4-address <local-ipv4-address> }
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
server	Server IP address
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
username	User name for PPP connection or cellular modem settings Usually <*username*>@<*ISP*>
local-ipv4-address	Local tunnel IP address or Auto for automatic An IP address, or '`auto`'
wan-ipv4-address	WAN IP address wrapper An IP address, or '`auto`'
wan-subnet-mask	WAN subnet mask (in the advanced section)

Parameter	Description
wan-mask-length	WAN subnet mask length
default-gw	WAN default gateway (in the advanced section of PPTP and L2TP)

DMZ - PPPoE

Syntax

```
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
{true | false} local-ipv4-address <local-ipv4-address> }
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once
local-ipv4-address	Local tunnel IP address or Auto for automatic An IP address, or 'auto'
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
username	User name for PPP connection or cellular modem settings Usually <*username*>@<*ISP*>
vlan-id	VLAN ID A number with no fractional part (integer)

DMZ - PPTP

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>
} { local-ipv4-address <local-ipv4-address> }
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
server	Server IP address
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
username	User name for PPP connection or cellular modem settings Usually <*username*>@<*ISP*>
local-ipv4-address	Local tunnel IP address or Auto for automatic An IP address, or '`auto`'
wan-ipv4-address	WAN IP address wrapper An IP address, or '`auto`'
wan-mask-length	WAN subnet mask length

Parameter	Description
wan-subnet-mask	WAN subnet mask (in the advanced section)
default-gw	WAN default gateway (in the advanced section of PPTP and L2TP)

add internet-connection interface DMZ - RJ45/SFP-Fiber

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add a DMZ interface connection of type RJ45/SFP fiber.

See *"set internet-connection dmz-connection rj45/sfp-fiber / sfp-dsl" on page 346*.

RJ45/SFP-Fiber - Static IP Address

Syntax

```
add internet-connection name "<name>" interface DMZ dmz-connection
rj45/sfp-fiber 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
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
default-gw	WAN default gateway (in the advanced section of PPTP and L2TP)
dns-primary	First DNS server IP address
dns-secondary	Second DNS server IP address
dns-tertiary	Third DNS server IP address
ipv4-address	IP address field (for static IP and bridge settings)
mask-length	Subnet mask length
subnet-mask	Subnet mask A subnet mask, or 255.255.255.255
vlan-id	VLAN ID A number with no fractional part (integer)
conn-test-timeout	Connection test timeout A number with no fractional part (integer)

RJ45/SFP-Fiber - DHCP - VLAN

Syntax

```
add internet-connection name "<name>" interface DMZ dmz-connection
rj45/sfp-fiber type dhcp { use-connection-as-vlan vlan-id <vlan-
id> }
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
vlan-id	VLAN ID A number with no fractional part (integer)

RJ45/SFP-Fiber - Bridge - DHCP

Syntax

```
add internet-connection name "<name>" interface DMZ dmz-connection
rj45/sfp-fiber type bridge bridge-name <bridge-name> bridge-type
dhcp { use-connection-as-vlan vlan-id <vlan-id> }
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
vlan-id	VLAN ID A number with no fractional part (integer)
conn-test-timeout	Connection test timeout A number with no fractional part (integer)

RJ45/SFP-Fiber - Bridge - Static IP Address

Syntax

```
add internet-connection name "<name>" interface DMZ dmz-connection
rj45/sfp-fiber type bridge bridge-name <bridge-name> bridge-type
static
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
bridge-name	Name of the bridge interface
default-gw	Default gateway
dns-primary	First DNS server IP address
dns-secondary	Second DNS server IP address
dns - tertiary	Third DNS server IP address

RJ45/SFP-Fiber - L2TP

Syntax

```
add internet-connection name "<name>" interface DMZ dmz-connection
rj45/sfp-fiber 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> } { local-ipv4-address <local-ipv4-
address> }
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
default-gw	WAN default gateway (in the advanced section of PPTP and L2TP)
local-ipv4-address	Local tunnel IP address or Auto for automatic An IP address, or '`auto`'
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
server	Server IP address
username	User name for PPP connection or cellular modem settings Usually *<username>@<ISP>*
wan-ipv4-address	WAN IP address wrapper An IP address, or '`auto`'
wan-mask-length	WAN subnet mask length
wan-subnet-mask	WAN subnet mask (in the advanced section)
vlan-id	VLAN ID A number with no fractional part (integer)

Parameter	Description
conn-test-timeout	Connection test timeout A number with no fractional part (integer)

RJ45/SFP-Fiber - PPPoE

Syntax

```
add internet-connection name "<name>" interface DMZ dmz-connection
rj45/sfp-fiber type pppoe username <username> password <password>
{ is-unnumbered-pppoe {true | false} local-ipv4-address <local-
ipv4-address> }
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
username	User name for PPP connection or cellular modem settings Usually *<username>@<ISP>*
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once
local-ipv4-address	Local tunnel IP address or Auto for automatic An IP address, or '`auto`'
vlan-id	VLAN ID A number with no fractional part (integer)
conn-test-timeout	Connection test timeout A number with no fractional part (integer)

RJ45/SFP-Fiber - PPTP

Syntax

```
add internet-connection name "<name>" interface DMZ dmz-connection
rj45/sfp-fiber 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> } { local-ipv4-address <local-ipv4-
address> }
```

Parameters

Parameter	Description
name	Connection name
interface	Interface name Press TAB to see available options
type	Connection type Press TAB to see available options
server	Server IP address
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
username	User name for PPP connection or cellular modem settings Usually <*username*>@<*ISP*>
local-ipv4-address	Local tunnel IP address or Auto for automatic An IP address, or '`auto`'
wan-ipv4-address	WAN IP address wrapper An IP address, or '`auto`'
wan-mask-length	WAN subnet mask length
wan-subnet-mask	WAN subnet mask (in the advanced section)
default-gw	WAN default gateway (in the advanced section of PPTP and L2TP)
isVlan	This interface is VLAN

Parameter	Description
ipv4-address	IP address field (for static IP and bridge settings)
mask-length	Subnet mask length
subnet-mask	Subnet mask A subnet mask, or 255.255.255.255
dns-primary	First DNS server IP address
dns-secondary	Second DNS server IP address
dns-tertiary	Third DNS server IP address
encapsulation	Encapsulation type for the ADSL connection
vci	VCI value for the ADSL connection A number between 0 and 65535
vpi	VPI value for the ADSL connection A number between 0 and 255
vlan-id	VLAN ID A number with no fractional part (integer)
con-test-timeout	Connection test timeout A number with no fractional part (integer)
standard	The ADSL standard to use Options: multimode, t1413, glite, gdmt, adsl2, adsl2+

Example Command

```
add internet-connection name "My connection" interface DMZ dmz-
connection rj45/sfp-fiber type static ipv4-address 172.15.47.4
subnet-mask 255.255.255.0 default-gw 172.15.2.2
```

add internet-connection interface cellular

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add a new cellular (LTE) internet connection.

See also: *"set internet-connection type cellular" on page 339*

Syntax

```
add internet-connection interface cellular [apn <VALUE>] [pin
<VALUE>] [apn-sim1-authentication-method <VALUE>] [apn-sim1-
password <VALUE>] [apn-sim2-username <VALUE>] [apn-sim2-
authentication-method <VALUE>] [apn-sim2-password <VALUE>] [apn-
sim2-username <VALUE>] [apn-sim2 <VALUE>] [pin-sim2 <VALUE>]
[primary-sim {sim1 | sim2}] [disable-sim {sim1 | sim2 | none}]
[name <VALUE>]
```

Parameters

Parameter	Description
apn	APN (Access Point Name) of SIM 1(optional).
pin	PIN (Personal Identification Number) of SIM 1(optional).
apn-sim1-authentication-method	The APN authentication method provided by your cellular network carrier for SIM1. Supported values are: ■ pap ■ chap ■ none
apn-sim1-password	The APN password provided by your cellular network carrier for SIM1. Password string. Maximum length of 15 characters. Required when "`apn-sim1-authentication-method`" is "`pap`" or "`chap`".
apn-sim1-username	The APN username provided by your cellular network carrier for SIM1. Maximum length of 59 characters. Required when "`apn-sim1-authentication-method`" is "`pap`" or "`chap`".
apn-sim2-authentication-method	The APN authentication method provided by your cellular network carrier for SIM2. Supported values are: ■ pap ■ chap ■ none

Parameter	Description
apn-sim2-password	The APN password provided by your cellular network carrier for SIM2. Password string. Maximum length of 15 characters. Required when "`apn-sim2-authentication-method`" is "`pap`" or "`chap`".
apn-sim2-username	The APN username provided by your cellular network carrier for SIM2. Maximum length of 59 characters. Required when "`apn-sim2-authentication-method`" is "`pap`" or "`chap`".
apn-sim2	APN (Access Point Name) of SIM 2 (optional).
pin-sim2	PIN number of SIM 2 (optional).
primary-sim	The preferred SIM to use for the connection.
disable-sim	Allows disabling of one of the SIM cards.
name	The name of the internet connection.
sim1-carrier-configuation-package	Predefined configuration and firmware package required for specific cellular network carriers for SIM1.
sim2-carrier-configuation-package	Predefined configuration and firmware package required for specific cellular network carriers for SIM2.

Example Command

```
add internet-connection interface cellular apn sim1apn.com pin
1111 apn-sim1-authentication-method pap apn-sim1-username my_sim1_
username apn-sim1-password my_sim1_password apn-sim2-
authentication-method none apn-sim2 sim2apn.com pin-sim2 2222
disable-sim none primary-sim sim1 name Internet1
```

add internet-connection type analog / cellular

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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

`add internet-connection name "<name>" type **analog** use-serial-port {**true | false**} number <number> { username <username> password-hash <password-hash> }`
`add internet-connection name "<name>" type **analog** use-serial-port **false** number <number> { username <username> password <password> }`
`add internet-connection name "<name>" type **analog** use-serial-port **true** 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>" type **cellular** number <number> { conn-test-timeout <conn-test-timeout> } name "<name>" } { apn <apn> username <username> password-hash <password-hash> }`
`add internet-connection name "<name>" type **cellular** number <number> { conn-test-timeout <conn-test-timeout> name "<name>" } { apn <apn> username <username> password <password> }`

Parameters

Parameter	Description
apn	APN (cellular modem settings) A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus)
conn-test-timeout	Connection test timeout A number with no fractional part (integer)

Parameter	Description
flow-control	Flow control (serial port settings) Options: rts-cts, xon-xoff
name	Connection name A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)
number	Dialed number of the cellular modem settings Type: A sequence of numbers and #,* characters
password	Password for PPP connection settings
password-hash	The hash of the user password
port-speed	Port speed (serial port settings) Options: 9600, 19200, 38400, 57600, 115200, 230400
type	Connection type Press TAB to see available options
use-serial-port	Use serial port
username	User name for PPP connection settings Usually <*username*>@<*ISP*>

Example Command

```
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
```

add internet-connection new-link-aggregation

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add new internet connection (new link aggregation).

Syntax

```
add internet-connection [ name "<name>" ] interface
{
new-link-aggregation slave-port-1 <slave-port-1> slave-port-2
<slave-port-2> [ bond-mode { xor [ bond-hash-policy <bond-hash-
policy> ] [bond-mii-interval <bond-mii-interval> ] | round-robin [
bond-mii-interval <bond-mii-interval> ] | high-availability bond-
master <bond-master> [ bond-mii-interval <bond-mii-interval> ] |
802.3ad [ bond-hash-policy <bond-hash-policy> ] [ bond-mii-
interval <bond-mii-interval> ] } ] [ { use-connection-as-vlan }
vlan-id <vlan-id> ] type { dhcp | static ipv4-address <ipv4-
address> { subnet-mask <subnet-mask> | mask-length <mask-length> }
[ default-gw <default-gw> ] [ probe-next-hop {true | false} ] [
probe-servers {true | false} ] [ 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 {true | false} ] 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> ] | bridge bridge-name
<bridge-name> bridge-type { static default-gw <default-gw> [ dns-
primary <dns-primary> ] [ dns-secondary <dns-secondary> ] [ dns-
tertiary <dns-tertiary> ] | dhcp } | pptp username <username> {
password <password> | password-hash <password-hash> } [ local-
ipv4-address <local-ipv4-address> ] [ is-unnumbered-pppoe {true |
false} ] 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> ] | pppoe username <username> { password <password> |
password-hash <password-hash> } [ local-ipv4-address <local-ipv4-
address> ] [ is-unnumbered-pppoe {true | false} ] | ds-lite
linked-ipv6-connection <linked-ipv6-connection> [ aftr-address
<aftr-address> ] [ dns-primary <dns-primary> ] [ dns-secondary
<dns-secondary> ] [ dns-tertiary <dns-tertiary> ] } [ conn-test-
timeout <conn-test-timeout> ]

 |
```

WAN [{ use-connection-as-vlan } vlan-id <*vlan-id*>] type { dhcp | static ipv4-address <*ipv4-address*> { subnet-mask <*subnet-mask*> | mask-length <*mask-length*> } [default-gw <*default-gw*>] [probe-next-hop {true | false}] [probe-servers {true | false}] [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 {true | false}] 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*>] | bridge bridge-name <*bridge-name*> bridge-type { static default-gw <*default-gw*> [dns-primary <*dns-primary*>] [dns-secondary <*dns-secondary*>] [dns-tertiary <*dns-tertiary*>] | dhcp } | pptp username <*username*> { password <*password*> | password-hash <*password-hash*> } [local-ipv4-address <*local-ipv4-address*>] [is-unnumbered-pppoe {true | false}] 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*>] | pppoe username <*username*> { password <*password*> | password-hash <*password-hash*> } [local-ipv4-address <*local-ipv4-address*>] [is-unnumbered-pppoe {true | false}] | ds-lite linked-ipv6-connection <*linked-ipv6-connection*> [aftr-address <*aftr-address*>] [dns-primary <*dns-primary*>] [dns-secondary <*dns-secondary*>] [dns-tertiary <*dns-tertiary*>] } [conn-test-timeout <*conn-test-timeout*>]

|

ADSL type { pppoa username <*username*> { password <*password*> | password-hash <*password-hash*> } [local-ipv4-address <*local-ipv4-address*>] [is-unnumbered-pppoe {true | false}] [vpi <*vpi*>] [vci <*vci*>] [encapsulation {llc | vcmux}] | pppoe username <*username*> { password <*password*> | password-hash <*password-hash*> } [local-ipv4-address <*local-ipv4-address*>] [is-unnumbered-pppoe {true | false}] [vpi <*vpi*>] [vci <*vci*>] [encapsulation {llc | vcmux}] | eoa } [vpi <*vpi*>] [vci <*vci*>] [encapsulation {llc | vcmux}] [standard <*standard*>] [conn-test-timeout <*conn-test-timeout*>]

|

```
DSL [ { use-connection-as-vlan } vlan-id <vlan-id> ] type { pppoe
username <username> { password <password> | password-hash
<password-hash> } [ local-ipv4-address <local-ipv4-address> ] [
is-unnumbered-pppoe {true | false} ] [ vpi <vpi> ] [ vci <vci> ] [
encapsulation {llc | vcmux} ] | ipoe-dynamic | ipoe-static ipv4-
address <ipv4-address>{ subnet-mask <subnet-mask> | mask-length
<mask-length> } [ default-gw <default-gw> ] [ probe-next-hop {true
| false} ] [ probe-servers {true | false} ] [ dns-primary <dns-
primary> ] [ dns-secondary <dns-secondary> ] [ dns-tertiary <dns-
tertiary> ] } [ vpi <vpi> ] [ vci <vci> ] [ encapsulation {llc |
vcmux} ] [ conn-test-timeout <conn-test-timeout> ]

 |
```

Parameters

Parameter	Description
aftr-address	Hostname or IPv6 address for DS-Lite tunnel
apn	The Access Point Name given to you by your cellular network carrier for SIM1. A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus)
apn-sim1-authentication-method	The APN authentication method given to you by your cellular network carrier for SIM1 Options: none, pap, chap
apn-sim1-password	The APN password given to you by your cellular network carrier for SIM1.
apn-sim1-username	The APN username given to you by your cellular network carrier for SIM1. Usually <*username*>@<*ISP*>
apn-sim2	The Access Point Name given to you by your cellular network carrier for SIM2. A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus)
apn-sim2-authentication-method	The APN authentication method given to you by your cellular network carrier for SIM2. Options: none, pap, chap
apn-sim2-password	The APN password given to you by your cellular network carrier for SIM2.
apn-sim2-username	The APN username given to you by your cellular network carrier for SIM2. Usually <*username*>@<*ISP*>

Parameter	Description
bond-hash-policy	The bond hash policy Options: layer2, layer2_3, layer3_4
bond-master	The bond Master port A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '_' (underscore) ■ '/' (slash)
bond-mii-interval	The bond MII interval A number with no fractional part (integer)
bond-mode	The bond operation mode policy Press TAB to see available options
bridge-name	The name of the bridge this connection is bridged to A bridge name should be br0-9
bridge-type	The type of the bridge for this connection: DHCP or static Press TAB to see available options
conn-test-timeout	Connection test timeout A number with no fractional part (integer)
default-gw	WAN default gateway (in the advanced section of PPTP and L2TP)
default-gw-ipv6	IPv6 default gateway
disable-sim	Indicates which SIM, if any, is disabled. Options: sim1, sim2, none
dmz-connection	For DMZ connections, select RJ45/SFP-Fiber or SFP-DSL Press TAB to see available options
dns-primary	First DNS server IP address
dns-primary-ipv6	First DNS server IPv6 address
dns-secondary	Second DNS server IP address
dns-secondary-ipv6	Second DNS server IPv6 address

Parameter	Description
dns-tertiary	Third DNS server IP address
dns-tertiary-ipv6	Third DNS server IPv6 address
encapsulation	Encapsulation type for the ADSL connection
initialization-string	The initialization string for the cellular modem settings A string that contains only upper-case letters (`A-Z`).
interface-ipv6	Interface name for IPv6 Internet connection Press TAB to see available options
ipv4-address	IP address field (for static IP and bridge settings)
ipv6-address	IPv6 address field (for static IP settings)
is-prefix-delegation	Indicates whether prefix delegation is enabled (true) or disabled (false) for this Internet connection
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once
isVlan	This interface is VLAN
linked-connection	An IPv4 Internet connection with shared credentials A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)
linked-ipv6-connection	IPv6 internet connection name which the DS-Lite tunnel is defined on
local-ipv4-address	Local tunnel IP address or auto for automatic An IP address, or '`auto`'
mask-length	Subnet mask length
method	Authentication method Options: auto, pap, chap

Parameter	Description
name	Connection name A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)
number	Dialed number of the cellular modem settings Type: A sequence of numbers and #,* characters
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
pin	The Personal Identification Number code given to you by your cellular network carrier for SIM1.
pin-sim2	The Personal Identification Number code given to you by your cellular network carrier for SIM2.
prefix-delegation-prefix-length	Prefix length for prefix delegation
prefix-length	Prefix length field (for IPv6 static IP settings)
primary-sim	Indicates the preferred SIM for the cellular internet connection. Options: sim1, sim2
probe-next-hop	Automatically detect loss of connectivity to the default gateway
probe-servers	Monitor the connection state (if set to 'true') by sending probe packets to one or more servers on the Internet
server	Server IP address
sim1-carrier-configuation-package	Predefined configuration and firmware package required for specific cellular net-work carriers for SIM1. Options: att, generic, rogers, sprint, verizon, verizon-alo, bell, vodafone, telus, us-cellular, sierra-wireless, docomo, kddi, softbank, telstra

Parameter	Description
sim2-carrier-configuation-package	Predefined configuration and firmware package required for specific cellular net-work carriers for SIM2. Options: att, generic, rogers, sprint, verizon, verizon-alo, bell, vodafone, telus, us-cellular, sierra-wireless, docomo, kddi, softbank, telstra
subnet-mask	Subnet mask A subnet mask, or 255.255.255.255
type	Connection type Press TAB to see available options
type-ipv6	Connection type for IPv6 Internet connection Press TAB to see available options
username	User name for PPP connection or cellular modem settings Usually <*username*>@<*ISP*>
vci	VCI value for the ADSL connection A number between 0 and 65535
vlan-id	VLAN ID A number with no fractional part (integer)
vpi	VPI value for the ADSL connection A number between 0 and 255
wan-ipv4-address	WAN IP address wrapper An IP address, or '`auto`'
wan-mask-length	WAN subnet mask length
wan-subnet-mask	WAN subnet mask (in the advanced section)

Example Command

```
add internet-connection name "My connection" interface new-link-
aggregation slave-port-1 My_Network slave-port-2 My_Network bond-
mode xor bond-hash-policy layer2 bond-mii-interval zzzMUST_ENTER_
REAL_EXAMPLE_VALUEzzz true vlan-id zzzMUST_ENTER_REAL_EXAMPLE_
VALUEzzz type dhcp conn-test-timeout zzzMUST_ENTER_REAL_EXAMPLE_
VALUEzzz
```

add internet-connection interface USB type usb-cellular

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new cellular interface (USB).

Syntax

```
add internet-connection interface USB type usb-cellular
<parameters>
```

Parameters

Parameter	Description
apn	The Access Point Name given to you by your cellular network carrier for SIM1.
password-hash	The hash of the user password.
password	Password for PPP connection or cellular modem settings.
username	User name for PPP connection or cellular modem settings.
initialization-string	The initialization string for the cellular modem settings.
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once.
local-ipv4-address	Local tunnel IP address or auto for automatic.
method	Authentication method.
number	Dialed number of the cellular modem settings.
conn-test-timeout	Connection test timeout.

add internet-connection interface type ipip

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds an internet connection of type IPIP to the specified interface.

IPIP, a variation of DS-Lite, is used to tunnel IPv4 traffic over IPv6-only networks. As in DS-Lite, the IPv4 traffic is tunneled over an existing IPv6 connection. The DS-Lite/IPIP tunnel is created between the client (gateway) and a peer (AFTR which resides on the ISP and is configured statically or acquired via DHCPv6).

Important - Before you can run this command, you must enable the IPIP feature. See *"set advanced-settings ipip-enabled" on page 1708*.

See also:

- *"set internet-connection interface type ipip" on page 327*

Syntax

```
add internet-connection interface <interface name> type ipip
linked-ipv6-connection <name of IPv6 connection> aftr-address
<AFTR address> vne-service-name <VNE service name> vne-update-
server-url <VNE server URL> vne-update-server-username <VNE server
user name> vne-update-server-password <vne server password> ipv4-
address <IPv4 address> subnet-mask <subnet mask>
```

```
add internet-connection interface <interface name> type ipip ipv4-
address <ipv4 address> subnet-mask <subnet mask> linked-ipv6-
connection <ipv6 internet connection name> aftr-address <AFTR-
address (ipv6 address)> vne-service-name xpass vne-update-server-
url <server url> vne-update-server-username <VNE server user name>
vne-update-server-password <VNE server user password> vne-fqdn
<VNE fqdn> vne-ddns-id <VNE ddns id> vne-ddns-password <VNE ddns
password> enable-vne-unnumbered-ip { on | off }
```

Parameters

Parameter	Description
interface	Specifies the interface. Press the TAB key to see the available options.
linked-ipv6-connection	Name of the IPv6 connection.
aftr-address	Hostname or IPv6 address.
vne-service-name	Specifies the VNE service: ■ transix - Transix service ■ v6 connect - v6 Connect service ■ v6-plus - v6plus Static IP service ■ xpass - Xpass service
vne-update-server-url	URL of server
vne-update-server-username	Password should contain only these characters: ■ A string that contains only lower-case letters (`a-z`). ■ A string that contains only upper-case letters (`A-Z`). ■ A string that contains only digits (`0-9`). ■ A string that contains only an underscore ('_ ').
vne-update-server-password	Password should contain only these characters: ■ English alphanumeric ■ `( ) ! @ # $ % ^ & * ? - _ = + : ; . ,`
vne-fqdn	The user's URL which maps to the gateway
vne-ddns-id	ID for the DDNS service

Parameter	Description
vne-ddns-password	Password for the DDNS service
enable-vne-unnumbered-ip	Options: ■ on ■ off
ipv4-address	IPv4 address
subnet-mask	Subnet Mask for the IPv4 address

Example Command

```
add internet-connection interface WAN type ipip linked-ipv6-
connection Internet2 aftr-address ::abcd vne-service-name transix
vne-update-server-url https://mysite.com vne-update-server-
username myuserName vne-update-server-password pass12345678 ipv4-
address 1.1.1.1 subnet-mask 255.255.255.0
```

```
add internet-connection interface WAN type ipip ipv4-address
1.2.3.4 subnet-mask 255.255.255.0 linked-ipv6-connection Internet3
aftr-address 12::1 vne-service-name xpass vne-update-server-url
https://myserverurl.com vne-update-server-username myUser vne-
update-server-password mypassword1 vne-fqdn myurl.com vne-ddns-id
myurl vne-ddns-password myddnspassword1 enable-vne-unnumbered-ip
on
```

Deleting Internet Connections

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

Deletes an existing internet connection or internet connection related configuration.

delete internet-connection

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing internet connection by name.

Syntax

```
delete internet-connection "<name>"
```

Parameters

Parameter	Description
name	Connection name A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)

Example Command

```
delete internet-connection "My connection"
```

delete internet-connections

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all existing internet connections.

Syntax

```
delete internet-connections
```

Example Command

```
delete internet-connections
```

delete internet-connection probe-icmp-servers

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)

Example Command

```
delete internet-connection "My connection" probe-icmp-servers
first second third
```

Viewing Internet Connections

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

Shows configuration and details of defined internet connections.

show internet-connection

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration and details of a defined internet connection.

Syntax

```
show internet-connection "<name>"
```

Parameters

Parameter	Description
name	Connection name

Example Command

```
> show internet-connection Internet1
high-availability-recovery-time:60
load-balancing-weight: 10
operator: MyISP
signal-strength: -61
bond-master:
username:
isVlan: false
conn-test-timeout:
local-tunnel-ip-assignment: automatic
subnet-mask: 255.255.255.240
alias-id: 0
mac-addr:
custom-mtu: true
access-point-security-type:
idle-time: 20
dns-primary: 172.16.30.1
apn-sim2-password:
dns-secondary: 172.16.30.2
probe-next-hop: true
dns-tertiary:
is-bond: false
lan-default-mac-address: 00:1C:7F:95:E8:26
username:
qos-download: false
third: dns.opendns.com
username:
number: *99#
pin-sim2:
second: b.resolvers.Level3.net
max-latency-allowed: 900
probing-window-size: 10
use-default-mac-addr: on
link-status: internet
type: cellular
wan-ip-address:
signal-strength-level: 5
local-tunnel-ip:
wan-ipv4-address: auto
initialization-string:
password:
first: dns.google.com
link-speed: 10/half
password-hash:
dns-tertiary-ipv6:
```

```
first-name: Google Public DNS
number: *99#
is-active: true
wan-subnet-mask:
is-unnumbered-pppoe: false
type: cellular
access-point-ssid:
prefix-length: 64
dns-secondary-ipv6:
type: pppoa
qos-upload: false
ipv6-address: ::
apn-sim2:
failover-after-ping-failure-percent:63
local-ipv4-address: auto
cellular-generation: 4g
bridge-name:
bridge-type: dhcp
interface-ipv6: WAN
type: usb-cellular
cluster-status: non-ha
interface: cellular
disable-sim: none
hostname-via-dhcp: false
ip-version: ipv4
inbound-bandwidth: 1000000
probing-method: icmp
mask-length: 28
ipv6-address:
state: true
type: pppoe
name: Internet1
primary-sim: sim1
wan-ip-assignment: automatic
country:
dns-primary-ipv6:
probingStatus: table: 0xf6dd0a48
username:
vci: 0
access-point-password:
status:
bond-id:
second-name: Level 3 Communications
connect-on-demand: false
access-point-signal-strength:
```

```
apn-sim1-authentication-method:none
route-traffic-through-default-gateway:true
use-serial-port: false
pin:
interface: cellular
server:
default-gw: 172.16.30.10
apn-sim1-username:
dmz-link-speed: 10/half
mtu: 1500
wan-default-mac-address: 00:1C:7F:95:E8:25
standard:
sim1-carrier-configuation-package:
bond-slaves:
access-point-wpa-password:
probe-servers: true
disable-nat: false
dmz-default-mac-address: 00:1C:7F:95:E8:27
apn:
bond-hash-policy: layer2
active-sim: sim2
default-gw:
auto-negotiation: on
ipv4-address: 172.16.30.40
apn-sim2-username:
ip-address: 172.16.30.40
password:
access-point-radio-type:
number: *99#
vlan-id: 0
failover-after-ping-failures: 1
apn-sim2-authentication-method:none
lan-link-speed:
linked-connection-id:
access-point-operation-mode:
wan-mask-length:
conn-duration: 3396
cellularRadioMode: on
password:
outbound-bandwidth: 1000000
status-type:
username:
type-ipv6: auto-obtain
wan-link-speed: 10/half
bond-mode: 802.3ad
```

```
password:
access-point-user-name:
mtu: 1500
apn-sim1-password:
ha-priority: 1
port-speed: 115200
type-ipv6: pppoe-ipv6
vpi: 0
encapsulation: llc
service-rovider:
third-name: OpenDNS
service-name:
mac-addr: default
dial: tone
bond-mii-interval: 100
password:
probing-frequency: 3
flow-control: rts-cts
method: auto
sim2-carrier-configuation-package:
linked-connection:
default-gw-ipv6:
```

show internet-connection icmp-servers

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configured IPv4 and IPv6 probing servers for health monitoring of defined internet connection.

If there is no connectivity to these servers, the connection reports its status as failed.

In Web UI, this corresponds to:

1. Click the **Device** view > **Network** section > **Internet** page.
2. Click the **Configure monitoring** link.
3. Click **Cancel**.

See:

- *"set internet-connection probe-icmp-servers" on page 359*
- *"set internet-connection probe-icmp6-servers" on page 629*

Syntax

```
show internet-connection <name> icmp-servers
```

Parameters

Parameter	Description
name	Specifies the connection name. Press the TAB key to see the available options.

Example Output

```
HostName> show internet-connection Internet2 icmp-servers
first: cloudflare.com
second: dns.opendns.com
third: dns.opendns.com
first-ipv6: 2001:4860:4860::8888
second-ipv6: dns.cloudflare.com
third-ipv6: dns.opendns.com
```

show internet-connection type cellular

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the carrier connection name for LTE internal modem.

Syntax

```
show internet-connection "<name>" type cellular
```

Example Command

```
show internet-connection Internet1 type cellular
```

show internet-connections

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows details and configuration of all internet connections.

Syntax

```
show internet-connections
```

Example Command

```
show internet-connections
```

show internet-connections table

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows details and configuration of all internet connections in a table.

Syntax

```
show internet-connections table
```

Example Command

```
show internet-connections table
```

Setting Internet Connections

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

Configures internet connections settings.

set internet-connection - enable / disable

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enable or disable an existing internet connection.

Syntax

```
set internet-connection "<name>" { enable | disable }
```

Parameters

Parameter	Description
name	Connection name

Example Command

```
set internet-connection "My connection" true
```

set internet-connection - auto negotiation, speed, MTU

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing internet connection.

In Web UI, this corresponds to:

1. Click the **Device** view > **Network** section > **Internet** page.
2. Edit an Internet connection.
3. Click the **Advanced** tab.
4. To configure the MTU manually, select **Use custom MTU value**.
5. To configure the MAC Address manually, select **Override default MAC Address**.
6. To configure the Speed and Duplex manually, select **Disable auto negotiation**.
7. Click **Save**.

Syntax

```
set internet-connection "<name>" [ auto-negotiation <auto-negotiation> ] [ link-speed <link-speed> ] [ mtu <mtu> ] [ mac-addr <mac-addr> ]
```

Parameters

Parameter	Description
name	Connection name A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)
auto-negotiation	Disable auto negotiation and manually define negotiation link speed Options: on, off

Parameter	Description
link-speed	Link speed Options: { 10/full, 10/half, 100/full, 100/half, 1/full, 1/half, 100BaseFx }
mac-addr	Default mac address wrapper A MAC address, or '`default`'
mtu	MTU size. Select '`default`' for default value

Example Command

```
set internet-connection "My connection" auto-negotiation on link-
speed 100/full mtu 1500 mac-addr 00:1C:7F:21:05:BE
```

set internet-connection connect-on-demand

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for an existing internet connection.

Syntax

```
set internet-connection "<name>" connect-on-demand {true | false}
```

Parameters

Parameter	Description
connect-on-demand	Configures the status of the "connect on demand" feature
name	Connection name

Example Command

```
set internet-connection "My connection" connect-on-demand true
```

set internet-connection interface DMZ

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure settings for an SFP DSL internet connection over the DMZ port in 1570 / 1590 appliances that do not have an internal DSL port.

See *"add internet-connection interface DMZ" on page 268*.

DMZ - SFP-DSL - PPPoE

Syntax

```
set internet-connection "<name>" dmz-connection sfp-dsl type pppoe
username <username> password <password>
```

Parameters

Parameter	Description
name	Connection name
ls-unnumbered-ppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once
local-ipv4-address	Local tunnel IP address or Auto for automatic An IP address, or '`auto`'
username	User name for PPP connection settings Usually <username>@<ISP>
password	Password for PPP connection settings
password-hash	The hash of the user password
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
conn-test-timeout	Connection test timeout A number with no fractional part (integer)

Example Command

```
set internet-connection name interface DMZ dmz-connection sfp-dsl
type pppoe username admin@isp password XXXXXX
```

DMZ - SFP-DSL - IPoE - Dynamic

Syntax

```
set internet-connection "<name>" dmz-connection sfp-dsl type ipoe-dynamic
```

Parameters

Parameter	Description
name	Connection name
encapsulation	Encapsulation type for the ADSL connection Options: ■ llc ■ vcmux
vci	VCI value for the ADSL connection A number between 0 and 65535
vpi	VPI value for the ADSL connection A number between 0 and 255
conn-test-timeout	Connection test timeout A number with no fractional part (integer)

Example Command

```
set internet-connection name interface DMZ dmz-connection sfp-dsl type ipoe-dynamic
```

DMZ - SFP-DSL - IPoE - Static

Syntax

```
set internet-connection "<name>" dmz-connection sfp-dsl type ipoe-
static default-gw ipv4-address <ipv4-address> subnet-mask <subnet-
mask> { dns-primary <dns-primary> dns-secondary <dns-secondary>
dns-tertiary <dns-tertiary> }
```

Parameters

Parameter	Description
name	Connection name
default-gw	WAN default gateway (in the advanced section of PPTP and L2TP)
ipv4-address	IP address field (for static IP and bridge settings)
mask-length	Subnet mask length
subnet-mask	Subnet mask Type: A subnet mask, or 255.255.255.255
dns-primary	First DNS server IP address
dns-secondary	Second DNS server IP address
dns-tertiary	Third DNS server IP address
vci	VCI value for the ADSL connection A number between 0 and 65535
vpi	VPI value for the ADSL connection A number between 0 and 255
conn-test-timeout	Connection test timeout A number with no fractional part (integer)

Example Command

```
set internet-connection name interface DMZ dmz-connection sfp-dsl
type ipoe-static default-gw ipv4-address 172.15.47.4 mask-length
255.255.255.
```

set internet-connection interface type ipip

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures settings for an internet connection of type IPIP.

See:

- *"set advanced-settings ipip-enabled" on page 1708*
- *"add internet-connection interface type ipip" on page 301*

Syntax

```
set internet-connection <interface name> type ipip linked-ipv6-
connection <name of IPv6 connection> aftr-address <AFTR address>
vne-service-name <VNE service name> vne-update-server-url <VNE
server URL> vne-update-server-username <VNE server user name> vne-
update-server-password <vne server password> ipv4-address <IPv4
address> subnet-mask <subnet mask>
```

Parameters

Parameter	Description
interface	Specifies the interface. Press the TAB key to see the available options.
linked-ipv6-connection	Name of the IPv6 connection. Press the TAB key to see the available options.
aftr-address	Hostname of IPv6 address
vne-service-name	Specifies the VNE service Press the TAB key to see the available options.
vne-update-server-url	URL of server
vne-update-server-username	■ A string that contains only lower-case letters (a-z). ■ A string that contains only upper-case letters (A-Z). ■ A string that contains only digits (0-9). ■ A string that contains only an underscore ('_ ').
vne-update-server-password	Password should contain only these characters : ■ English alphanumeric ■ ( ) ! @ # $ % ^ & * ? - _ = + : ; . ,
ipv4-address	IPv4 address
subnet-mask	Subnet Mask for the IPv4 address

Example Command

```
set internet-connection Internet3 type ipip linked-ipv6-connection
Internet2 aftr-address ::abcd vne-service-name transix vne-update-
server-url https://mysite.com vne-update-server-username
myuserName vne-update-server-password pass12345678 ipv4-address
1.1.1.1 subnet-mask 255.255.255.0
```

set internet-connection type dhcp / static

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures settings for an existing internet connection.

Syntax

```
set internet-connection "<name>" type dhcp
```

```
set internet-connection "<name>" type 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> ] [ probe-next-hop {on | off} ] [ probe-servers {on | off} ]
```

Parameters

Parameter	Description
name	Connection name
type	Connection type Press TAB to see available options
ipv4-address	IP address field (for static IP and bridge settings)
mask-length	Subnet mask length
subnet-mask	Subnet mask A subnet mask, or 255.255.255.255
default-gw	Default gateway
dns-primary	First DNS server IP address
dns-secondary	Second DNS server IP address
dns-tertiary	Third DNS server IP address
probe-next-hop	Automatically detect loss of connectivity to the default gateway
probe-servers	Monitor connection state by sending probe packets to one or more servers on the Internet

Example Commands

```
set internet-connection "My connection" type dhcp
```

```
set internet-connection "My connection" type static ipv4-address
192.168.22.33 mask-length 24 default-gw 192.168.22.1 dns-primary
192.168.22.251 dns-secondary 192.168.22.252 probe-next-hop on
probe-servers on
```

set internet-connection type l2tp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures settings for an existing internet connection.

Syntax

```
set internet-connection "<name>" type l2tp username <username> {
password <password> | password-hash <password-hash> } [ local-
ipv4-address <local-ipv4-address>] 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
name	Connection name
type	Connection type Press TAB to see available options
ipv4-address	IP address field (for static IP and bridge settings)
mask-length	Subnet mask length
subnet-mask	Subnet mask A subnet mask, or 255.255.255.255
default-gw	Default gateway
local-ipv4-address	Local tunnel IP address or Auto for automatic An IP address, or '`auto`'

Parameter	Description
server	Server IP address
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
username	User name for PPP connection or cellular modem settings Usually <*username*>@<*ISP*>
wan-ipv4-address	WAN IP address wrapper An IP address, or '`auto`'
wan-mask-length	WAN subnet mask length
wan-subnet-mask	WAN subnet mask (in the advanced section)

set internet-connection type pptp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures settings for an existing internet connection.

Syntax

```
set internet-connection "<name>" type pptp username <username> {
password <password> | password-hash <password-hash> } [ local-
ipv4-address <local-ipv4-address> ] 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
name	Connection name
type	Connection type Press the TAB key to see the available options.
ipv4-address	IP address field (for static IP and bridge settings)
mask-length	Subnet mask length

Parameter	Description
subnet-mask	Subnet mask A subnet mask, or 255.255.255.255
default-gw	Default gateway
local-ipv4-address	Local tunnel IP address or Auto for automatic An IP address, or '`auto`'
server	Server IP address
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
username	User name for PPP connection or cellular modem settings Usually <*username*>@<*ISP*>
wan-ipv4-address	WAN IP address wrapper An IP address, or '`auto`'
wan-mask-length	WAN subnet mask length
wan-subnet-mask	WAN subnet mask (in the advanced section)
vci	VCI value for the ADSL connection A number between 0 and 65535
vpi	VPI value for the ADSL connection A number between 0 and 255
encapsulation	Encapsulation type for the ADSL connection

set internet-connection type pppea / eoa

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 {true |
false} ] [ vpi <vpi> ] [ vci <vci> ] [ encapsulation {llc | vcmux}
]
```

```
set internet-connection "<name>" type eoa
```

Parameters

Parameter	Description
name	Connection name
type	Connection type Press TAB to see available options
local-ipv4-address	Local tunnel IP address or Auto for automatic An IP address, or 'auto'
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once.
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password.
username	User name for PPP connection or cellular modem settings Usually <*username*>@<*ISP*>
vci	VCI value for the ADSL connection A number between 0 and 65535
vpi	VPI value for the ADSL connection A number between 0 and 255
encapsulation	Encapsulation type for the ADSL connection

Example Command

```
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 type pppoa / eoa

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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> ]
```

```
set internet-connection "<name>" type eoa [ vpi <vpi> ] [ vci
<vci> ] [ encapsulation {llc | vcmux} ] [ 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
name	Connection name
type	Connection type Press TAB to see available options
default-gw	WAN default gateway (in the advanced section of PPTP and L2TP)
idle-time	Disconnect idle time in seconds
method	Authentication method Options: auto, pap, chap
wan-ipv4-address	WAN IP address wrapper An IP address, or '`auto`'
wan-mask-length	WAN subnet mask length
wan-subnet-mask	WAN subnet mask (in the advanced section)
encapsulation	Encapsulation for the ADSL connection

Parameter	Description
vci	VCI value for the ADSL connection A number between 0 and 65535
vpi	VPI value for the ADSL connection A number between 0 and 255
standard	The ADSL standard to use Options: multimode, t1413, glite, gdmt, adsl2, adsl2+

Example Command

```
set internet-connection "My connection" type pppoa method auto
idle-time 60 standard multimode
```

set internet-connection type pppoe / ipoe

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 {true | false} ] [
vpi <vpi> ] [ vci <vci> ] [ encapsulation {llc | vcmux} ] [ method
<method> ] [ idle-time <idle-time> ] [ standard <standard> ]
```

```
set internet-connection "<name>" type 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 {llc | vcmux} ]
```

```
set internet-connection "<name>" type ipoe-dynamic [ use-
connection-as-vlan vlan-id <vlan-id> ] [ vpi <vpi>] [ vci <vci> ]
[ encapsulation {llc | vcmux} ]
```

Parameters

Parameter	Description
name	Connection name
type	Connection type Press TAB to see available options
default-gw	Default gateway
dns-primary	First DNS server IP address
dns-secondary	Second DNS server IP address
dns-tertiary	Third DNS server IP address

Parameter	Description
idle-time	Disconnect idle time in seconds
ipv4-address	IP address field (for static IP and bridge settings)
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once
username	User name for PPP connection or cellular modem settings Usually <username>@<ISP>
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
local-ipv4-address	Local tunnel IP address or Auto for automatic An IP address, or '`auto`'
mask-length	Subnet mask length
subnet-mask	Subnet mask A subnet mask, or 255.255.255.255
isVlan	This interface is VLAN
method	Authentication method Options: auto, pap, chap
encapsulation	Encapsulation type for the ADSL connection
vci	VCI value for the ADSL connection A number between 0 and 65535
vpi	VPI value for the ADSL connection A number between 0 and 255
vlan-id	VLAN ID A number with no fractional part (integer)
standard	The ADSL standard to use Options: multimode, t1413, glite, gdmt, adsl2, adsl2+

Example Command

```
set internet-connection "My connection" type pppoe username
MyUsername@MyISP password internetPassword true vlan-id 200 local-
ipv4-address auto is-unnumbered-pppoe true vpi 42 vci 42
encapsulation llc method auto idle-time 60 standard multimode
```

set internet-connection type-ipv6 pppoe-ipv6 / pppoe-ipv6-4

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure IPv6 internet connection.

Syntax

```
set internet-connection "<name>" type-ipv6 pppoe-ipv6 [ method
{auto | pap | chap} ]
```

```
set internet-connection "<name>" type-ipv6 pppoe-ipv6-4 [ method
{auto | pap | chap} ]
```

Parameters

Parameter	Description
name	Connection name. Press the TAB key to see the available options.

Example Command

```
set internet-connection "My connection" type-ipv6 pppoe-ipv6
method auto
```

set internet-connection type cellular

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures settings for an existing internet connection.

See also: *"add internet-connection interface cellular" on page 284*

Syntax

```
set internet-connection "<name>" type cellular number <number> [
username <username> { password <password> | password-hash
<password-hash> } ] [ apn <apn> ]
```

```
set internet-connection "<name>" type cellular [ primary-sim
<primary-sim> ] [ apn-sim1-username <apn-sim1-username> ] [apn-
sim1-password <apn-sim1-password> ] [ apn-sim1-authentication-
method <apn-sim1-authentication-method> ] [ apn-sim2-username
<apn-sim2-username> ] [ apn-sim2-password <apn-sim2-password> ] [
apn-sim2-authentication-method <apn-sim2-authentication-method> ]
[ sim1-carrier-configuation-package <sim1-carrier-configuation-
package> ] [ sim2-carrier-configuation-package <sim2-carrier-
configuation-package> ] [ apn <apn> ] [ pin <pin> ] [ apn-sim2
<apn-sim2> ] [ pin-sim2 <pin-sim2> ] [ disable-sim {true | false}
]
```

Parameters

Parameter	Description
name	Connection name
type	Connection type Press TAB to see available options
apn	The Access Point Name (cellular modem settings) given to you by your cellular network carrier A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus)

Parameter	Description
number	Dialed number of the cellular modem settings A sequence of numbers and #,* characters
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
username	User name for PPP connection or cellular modem settings Usually <*username*>@<*ISP*>
apn-sim1-authentication-method	The APN authentication method given to you by your cellular network carrier for SIM1. Options: none, pap, chap
apn-sim1-password	The APN password given to you by your cellular network carrier for SIM1.
apn-sim1-username	The APN username given to you by your cellular network carrier for SIM1. Usually <*username*>@<*ISP*>
apn-sim2	The Access Point Name given to you by your cellular network carrier for SIM2. A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus)
apn-sim2-authentication-method	The APN authentication method given to you by your cellular network carrier for SIM2. Options: none, pap, chap
apn-sim2-password	The APN password given to you by your cellular network carrier for SIM2.
apns-im2-username	The APN username given to you by your cellular network carrier for SIM2. Usually <*username*>@<*ISP*>
pin	The Personal Identification Number code given to you by your cellular network carrier for SIM1.

Parameter	Description
pin-sim2	The Personal Identification Number code given to you by your cellular network carrier for SIM2.
primary-sim	Indicates the preferred SIM for the cellular internet connection. Options: sim1, sim2
sim1-carrierconfiguation-package	Predefined configuration and firmware package required for specific cellular network carriers for SIM1. Options: att, generic, rogers, sprint, verizon, verizon-alo, bell, vodafone, telus, us-cellular, sierra-wireless, docomo, kddi, softbank, telstra
sim2-carrierconfiguation-package	Predefined configuration and firmware package required for specific cellular network carriers for SIM2. Options: att, generic, rogers, sprint, verizon, verizon-alo, bell, vodafone, telus, us-cellular, sierra-wireless, docomo, kddi, softbank, telstra

Example Command

```
set internet-connection "My connection" type cellular number
758996 username MyUsername@MyISP password internetPassword apn my-
apn
```

set internet-connection type usb-cellular

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the settings for a new cellular interface (USB).

Syntax

```
set internet-connection "<name>" type usb-cellular
```

Parameters

Parameter	Description
name	Connection name.
apn	The Access Point Name given to you by your cellular network carrier for SIM1.
password-hash	The hash of the user password.
password	Password for PPP connection or cellular modem settings.
initialization-string	The initialization string for the cellular modem settings.
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once.
local-ipv4-address	Local tunnel IP address or auto for automatic.
method	Authentication method.
number	Dialed number of the cellular modem settings.
username	User name for PPP connection or cellular modem settings.
conn-test-timeout	Connection test timeout.

Example Command

```
set internet-connection Internet2 type usb-cellular
```

set internet-connection type bridge

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure an IPv6 internet connection.

Syntax

```
set internet-connection "<name>" type bridge bridge-name <bridge-name> bridge-type static [ default-gw <default-gw> ] [ dns-primary <dns-primary> ] [ dns-secondary <dns-secondary> ] [ dns-tertiary <dns-tertiary> ]
```

```
set internet-connection "<name>" type bridge bridge-name <bridge-name> bridge-type dhcp
```

Parameters

Parameter	Description
name	Connection name
type	Connection type Press TAB to see available options
bridge-name	The name of the bridge this connection is bridged to A bridge name should be br0-9
bridge-type	The type of the bridge for this connection: DHCP or static Press TAB to see available options
dns-primary	First DNS server IP address
dns-secondary	Second DNS server IP address
dns-tertiary	Third DNS server IP address

set internet-connection type ds-lite

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure an IPv6 internet connection.

Syntax

```
set internet-connection "<name>" type ds-lite [ linked-ipv6-
connection <linked-ipv6-connection> ] [ aftr-address <aftr-
address> ] [ dns-primary <dns-primary> ] [ dns-secondary <dns-
secondary> ] [ dns-tertiary <dns-tertiary> ]
```

Parameters

Parameter	Description
name	Connection name
type	Connection type Press TAB to see available options
linked-ipv6-connection	IPv6 internet connection name which the DS-Lite tunnel is defined on
aftr-address	Hostname or IPv6 address or DS-Lite tunnel
dns-primary	First DNS server IP address
dns-secondary	Second DNS server IP address
dns-tertiary	Third DNS server IP address
bridge-name	The name of the bridge this connection is bridged to A bridge name should be br0-9
bridge-type	The type of the bridge for this connection: DHCP or static Press TAB to see available options
default-gw	Default gateway
ipv4-address	IP address field (for static IP and bridge settings)

Parameter	Description
local-ipv4-address	Local tunnel IP address or auto for automatic An IP address, or '`auto`'
mask-length	Subnet mask length
subnet-mask	Subnet mask A subnet mask, or 255.255.255.255

Example Command

```
set internet-connection "My connection" type ds-lite linked-ipv6-
connection "My connection" aftr-address "My-DS-Lite-Tunnel" dns-
primary 192.168.1.1 dns-secondary 192.168.1.1 dns-tertiary
192.168.1.1
```

set internet-connection dmz-connection rj45/sfp-fiber / sfp-dsl

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure an RJ45/SFP-Fiber or SFP-DSL internet connection.

Syntax for RJ45/SFP-Fiber

```
set internet-connection "<Name>" dmz-connection rj45/sfp-fiber
      type
            bridge bridge-name <Name> bridge-type
                  dhcp
                  static
                        default-gw <IPv4-of-Default-Gateway>
                        [ dns-primary <Primary-DNS-Server> ]
                        [ dns-secondary <Secondary-DNS-Server> ]
                        [ dns-tertiary <Tertiary-DNS-Server> ]
            dhcp
            ds-lite
                  aftr-address <IPv6-Tunnel-Address>
                  linked-ipv6-connection <Name>
                  [ dns-primary <Primary-DNS-Server> ]
                  [ dns-secondary <Secondary-DNS-Server>]
                  [ dns-tertiary <Tertiary-DNS-Server> ]
                  [ probe-servers {on | off} ]
            ipip
                  ipv4-address <IPv4-Address>
                        mask-length <Subnet-Mask-Length>
                        subnet-mask <Subnet-Mask> }
                  aftr-address <IPv6-Tunnel-Address>
                  linked-ipv6-connection <Name>
                  vne-service-name
                        [ transix ]
                              vne-update-server-password <VNE-
Update-Password>
                              vne-update-server-url <VNE-Update-
URL> ]
                              vne-update-server-username <VNE-
Update-Username>
                        [ v6-connect
                              vne-update-server-password <VNE-
Update-Password>
                              vne-update-server-url <VNE-Update-
URL> ]
                              vne-update-server-username <VNE-
Update-Username>
                        [ xpass ]
                              enable-vne-unnumbered-ip {on | off}
                              vne-ddns-id <DDNS-ID>
                              vne-ddns-password <DDNS-Password>
                              vne-fqdn <FQDN>
                              vne-update-server-password <VNE-
Update-Password>
```

```
                              vne-update-server-url <VNE-Update-
URL>
                              vne-update-server-username <VNE-
Update-Username>
                  [ dns-primary <Primary-DNS-Server> ]
                  [ dns-secondary <Secondary-DNS-Server>]
                  [ dns-tertiary <Tertiary-DNS-Server> ]
                  [ probe-servers {on | off} ]
            l2tp
                  username <Username>
                  password <Password>
                  password-hash <Password-Hash>
                  server <IPv4-Address>
                  [ local-ipv4-address { <Local-IPv4-Address> |
auto} ]
                  [ wan-ipv4-address <IPv4-Address> ]
                        wan-mask-length <Subnet-Mask-Length>
                        wan-subnet-mask <Subnet-Mask> }
                        default-gw <IPv4-of-Default-Gateway>
            pppoe
                  username <Username>
                  { password <Password> | password-hash <Password-
Hash> }
                  [ is-unnumbered-pppoe {true | false} ]
                  [ local-ipv4-address { <Local-IPv4-Address> |
auto }]
                  [ wan-ipv4-address ]
                         auto
                        <IPv4-Address>
                              wan-mask-length <Subnet-Mask-Length>
                              wan-subnet-mask <Subnet-Mask>
                              default-gw <IPv4-of-Default-Gateway>
            pptp
                  username <Username>
                  { password <Password> | password-hash <Password-
Hash> }
                  server <IPv4-Address>
                  [ local-ipv4-address { <Local-IPv4-Address> |
auto }]
                  [ wan-ipv4-address
                       auto
                       <IPv4-Address>
                              wan-mask-length <Subnet-Mask-Length>
                              wan-subnet-mask <Subnet-Mask>
                              default-gw <IPv4-of-Default-Gateway>
```

```
            static
                  ipv4-address <IPv4-Address>
                  mask-length <Subnet-Mask-Length>
                  subnet-mask <Subnet-Mask>
                  default-gw <IPv4-of-Default-Gateway>
                  [ dns-primary <Primary-DNS-Server> ]
                  [ dns-secondary <Secondary-DNS-Server>]
                  [ dns-tertiary <Tertiary-DNS-Server> ]
                  [ probe-next-hop {on | off} ]
                  [ probe-servers {on | off} ]
      [ use-connection-as-vlan vlan-id <VLAN-ID> ]
      [ conn-test-timeout <Timeout> ]
```

Syntax for SFP-DSL

```
set internet-connection "<Name>" dmz-connection sfp-dsl
      type
            ipoe-dynamic
                  [ encapsulation {llc | vcmux} ]
                  [ vci <0-65535> ]
                  [ vpi <0-255> ]
            ipoe-static
                  ipv4-address <IPv4-Address>
                  mask-length <Subnet-Mask-Length>
                  subnet-mask <Subnet-Mask> }
                  default-gw <IPv4-of-Default-Gateway>
                  [ dns-primary <Primary-DNS-Server> ]
                  [ dns-secondary <Secondary-DNS-Server>]
                  [ dns-tertiary <Tertiary-DNS-Server> ]
                  [ encapsulation {llc | vcmux} ]
                  [ vci <0-65535> ]
                  [ vpi <0-255> ]
            pppoe
                  username <Username>
                  password <Password>
                  password-hash <Password-Hash>
                  [ encapsulation {llc | vcmux} ]
                  [ idle-time <0-1440> ]
                  [ is-unnumbered-pppoe {true | false} ]
                  [ local-ipv4-address { <Local-IPv4-Address> |
auto } ]
                  [ method {auto | chap | pap} ]
                  [ standard <ADSL-standard> ]
                  [ vci <0-65535> ]
                  [ vpi <0-255> ]
      [ use-connection-as-vlan vlan-id <VLAN-ID> ]
```

Parameters

Parameter	Description
internet-connection	The name of the Internet connection. Press the TAB key to see the available options.
dmz-connection	The type of the Internet connection: ■ `rj45/sfp-fiber` ■ `sfp-dsl`
type	The type of the connection: ■ `bridge` - Bridge ■ `dhcp` - DHCP IPv4 ■ `ds-lite` - Dual-Stack Lite (DS-Lite) ■ `ipip` - IPv4 over IPv6 (IPIP) ■ `l2tp` - L2TP ■ `pppoe` - PPPoE ■ `pptp` - PPTP ■ `static` - Static IPv4 address
bridge-name	The name of the Bridge connection. A bridge name should from `br0` to `br9`.
bridge-type	The type of the bridge for this connection: ■ `dhcp` - IP address is assigned automatically by a DHCP server ■ `static` - IP address is assigned manually
ipv4-address	IPv4 address (for a static IP configuration).
mask-length	IPv4 subnet mask length.
subnet-mask	IPv4 subnet mask (X.X.X.X, or 255.255.255.255).
default-gw	IPv4 address of the default gateway.
dns-primary	IPv address of the Primary DNS server.
dns-secondary	IPv address of the Secondary DNS server.
dns-tertiary	IPv address of the Tertiary DNS server.
aftr-address	IPv6 address or Hostname for the DS-Lite / IPIP tunnel.

Parameter	Description
linked-ipv6-connection	IPv6 internet connection name, on which the DS-Lite / IPIP tunnel is configured. Press the TAB key to see the available options.
probe-next-hop	Enables (`on`) or disables (`off`) automatic detection of connectivity to the default gateway.
probe-servers	Enables (`on`) or disables (`off`) automatic detection of connectivity to one or more specified servers on the Internet. You configure these servers with this command: `set internet-connection <Name> {probe-icmp-servers | probe-icmp6-servers}`
vne-service-name	The VNE provider name: ▪ `transix` - Transix ▪ `v6-connect` - v6 Connect ▪ `xpass` - Xpass
enable-vne-unnumbered-ip	Enables (`on`) or disables (`off`) the assignment of a public IP address to a single LAN interface or to a LAN switch.
vne-ddns-id	DDNS ID of the VNE provider.
vne-ddns-password	DDNS password of the VNE provider.
vne-fqdn	FQDN of the VNE provider.
vne-update-server-password	The password for the VNE provider update server.
vne-update-server-url	The URL for the VNE provider update server.
vne-update-server-username	The username for the VNE provider update server.
server	Server IPv4 address.
username	User name.
password	User password in plain text.
password-hash	The hash of the user password

Parameter	Description
local-ipv4-address	Local IPv4 address for the tunnel. The option "`auto`" assigns an IP address automatically.
is-unnumbered-ppoe	Enables (`true`) or disables (`false`) the unnumbered tunnel. With an unnumbered PPPoE you can manage a range of IP addresses and dial only once.
wan-ipv4-address	WAN wrapper IPv4 address. The option "`auto`" assigns an IP address automatically.
wan-mask-length	WAN wrapper subnet mask length.
wan-subnet-mask	WAN wrapper subnet mask.
encapsulation	Encapsulation type for the ADSL connection: ■ `llc` - LLC ■ `vcmux` - VCMUX
idle-time	Disconnect idle time 0-1440 seconds.
method	Authentication protocol: ■ `auto` - Auto ■ `chap` - CHAP ■ `pap` - PAP
standard	The ADSL standard to use: ■ `adsl2` - ADSL2 ■ `adsl2+` - ADSL2+ ■ `gdmt` - G.DMT ■ `glite` - G.lite ■ `multimode` - Multimode ■ `t1413` - T.1413
vci	The VCI value (0-65535) for the ADSL connection.
vpi	The VPI value (0-255) for the ADSL connection.
use-connection-as-vlan vlan-id	Configures this connection as VLAN.
conn-test-timeout	Connection test timeout in seconds.

Example Commands

- Configure a static IPv4 address:

```
set internet-connection Internet1 dmz-connection rj45/sfp-
fiber type static ipv4-address 192.168.20.33 subnet-mask
255.255.255.0 default-gw 192.168.20.1
```

- Configure a VLAN:

```
set internet-connection "My connection" dmz-connection
rj45/sfp-fiber true vlan-id 200 type dhcp conn-test-timeout 50
```

set internet-connection probe-next-hop

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables or disables the probing of the next hop (default gateway) for an existing internet connection.

In Web UI, this corresponds to:

1. Click the **Device** view > **Network** section > **Internet** page.
2. Edit an Internet connection.
3. Click the **Connection Monitoring** tab.
4. Refer to the checkbox **Automatically detect loss of connectivity to the default gateway**.
5. Click **Save**.

See:

- *"set internet-connection probe-servers" on page 357*
- *"set internet-connection probe-icmp-servers" on page 359*
- *"set internet-connection probe-icmp6-servers" on page 629*
- *"set internet-connection probing-method" on page 361*

Syntax

```
set internet-connection "<Name>" probe-next-hop {true | false}
```

Parameters

Parameter	Description
name	Name of the Internet connection. Press the TAB key to see the available options.
probe-next-hop	Enables (`true`) or disables (`false`) the probing of the next hop.

Example Command

```
set internet-connection "My connection" probe-next-hop true
```

set internet-connection probe-servers

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables or disables the probing of the configured servers on the Internet for an existing internet connection.

Note - You configure the probing servers with these commands:

- *"set internet-connection probe-icmp-servers" on page 359*
- *"set internet-connection probe-icmp6-servers" on page 629*

In Web UI, this corresponds to:

1. Click the **Device** view > **Network** section > **Internet** page.
2. To configure the probing servers, click the **Configure monitoring** link.
3. Edit an Internet connection.
4. Click the **Connection Monitoring** tab.
5. Refer to the checkbox **Monitor connection state by sending probe packets to the specified server on the Internet**.
6. Click **Save**.

See:

- *"set internet-connection probe-servers" above*
- *"set internet-connection probe-icmp-servers" on page 359*
- *"set internet-connection probe-icmp6-servers" on page 629*
- *"set internet-connection probing-method" on page 361*

Syntax

```
set internet-connection <Name> probe-servers {on | off}
```

Parameters

Parameter	Description
name	Name of the Internet connection. Press the TAB key to see the available options.
probe-next-hop	Enables (`on`) or disables (`off`) the probing of the servers.

Example Command

```
set internet-connection "My connection" probe-servers on
```

set internet-connection probe-icmp-servers

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the probing IPv4 addresses (or hostnames) to monitor an existing internet connection.

If there is no connectivity to these servers, the connection reports its status as failed.

In Web UI, this corresponds to:

1. Click the **Device** view > **Network** section > **Internet** page.
2. Click the **Configure monitoring** link.
3. Click **Save**.

See:

- *"show internet-connection icmp-servers" on page 635*
- *"set internet-connection probe-icmp-servers" above*
- *"set internet-connection probe-servers" on page 357*
- *"set internet-connection probe-icmp6-servers" on page 629*
- *"set internet-connection probing-method" on page 361*

Syntax

```
set internet-connection <Name>
      probe-icmp-servers
            first <IPv4-Address>
            [ second <IPv4-Address> ]
            [ third <IPv4-Address> ]
```

Parameters

Parameter	Description
name	Name of the Internet connection. Press the TAB key to see the available options.
first	First IPv4 address (or hostname) for the probing method (when using connection monitoring).
second	Second IPv4 address (or hostname) for the probing method (when using connection monitoring).
third	Third IPv4 address (or hostname) for the probing method (when using connection monitoring).

Example Command

```
set internet-connection "My connection" probe-icmp-servers first
dns.google.com second dns.cloudflare.com third dns.opendns.com
```

set internet-connection probing-method

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the probing method for an existing internet connection.

See:

- *"set internet-connection probing-method" above*
- *"set internet-connection probe-icmp-servers" on page 359*
- *"set internet-connection probe-icmp6-servers" on page 629*

Syntax

```
set internet-connection "<Name>" probing-method dns
```

Parameters

Parameter	Description
name	Name of the Internet connection. Press the TAB key to see the available options.
probing-method	Configures the probing method: ■ `dns` - DNS query

Example Command

```
set internet-connection "My connection" probing-method dns
```

set internet-connection qos-download

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for an existing internet connection.

Configures the QoS blade to run on this Internet connection (for download) in Locally Managed, SMP-managed, or Centrally Managed mode using a SmartLSM profile.

Syntax

```
set internet-connection "<name>" qos-download { true [ bandwidth
<bandwidth> ] | false }
```

Parameters

Parameter	Description
name	Connection name
bandwidth	ISP download bandwidth A number with no fractional part (integer)

Example Command

```
set internet-connection "My connection" qos-download true
bandwidth 100
```

set internet-connection qos-upload

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for an existing internet connection.

Configures the QoS blade to run on this Internet connection (for upload) in Locally Managed, SMP-managed, or Centrally Managed mode using a SmartLSM profile.

Syntax

```
set internet-connection "<name>" qos-upload { true [ bandwidth
<bandwidth> ] | false }
```

Parameters

Parameter	Description
name	Connection name
bandwidth	ISP upload bandwidth A number with no fractional part (integer)

Example Command

```
set internet-connection "My connection" qos-upload true bandwidth
5
```

set internet-connection disable-nat

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 {true | false}
```

Parameters

Parameter	Description
name	Connection name

Example Command

```
set internet-connection "My connection" disable-nat true
```

set internet-connection ha-priority

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
name	Connection name
ha-priority	Priority of the connection in HA A number with no fractional part (integer)
load-balancing-weight	Internet connection weight for load balancing configuration A number with no fractional part (integer)

Example Command

```
set internet-connection "My connection" ha-priority 2 load-
balancing-weight 15
```

set internet-connection route-traffic-through-default-gateway

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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.

To route traffic through this connection you need to add specific routes through it.

Syntax

```
set internet-connection "<name>" route-traffic-through-default-
gateway {true | false}
```

Parameters

Parameter	Description
name	Connection name A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)

Example Command

```
set internet-connection "My connection" route-traffic-through-
default-gateway true
```

Configuring Internet Connection Bond for IPv4

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

set internet-connection-bond

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure a link aggregation (bond) between two or more interfaces (WAN).

Syntax

```
set internet-connection-bond <name> [ bond-mode <bond-mode> ] [
bond-mii-interval <bond-mii-interval> ] [ bond-hash-policy <bond-
hash-policy> ] [ bond-master <bond-master> ]
```

Parameters

Parameter	Description
bond-hash-policy	The bond hash policy Options: layer2, layer2_3,layer3_4
bond-master	The bond Master port A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ '/' (slash)
bond-mii-interval	The bond MII interval between 0 and 5000 seconds (default 100 seconds)
bond-mode	The bond operation mode policy Options: 802.3ad, round-robin, xor, high-availability

Parameter	Description
name	Connection name A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)

Example Command

```
set internet-connection-bond "My connection" bond-mode 802.3ad
bond-master My_Network bond-mii-interval 200 bond-hash-policy
layer2
```

set internet-connection-bond

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure a link aggregation (bond) between two or more interfaces (WAN).

Syntax

```
set internet-connection-bond <name> add-member <add-member>
```

Parameters

Parameter	Description
add-member	bondPort1 A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ '/' (slash)
name	Connection name A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)

Example Command

```
set internet-connection-bond "My connection" add-member My_Network
```

set internet-connection-bond

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure a link aggregation (bond) between two or more interfaces (WAN).

Syntax

```
set internet-connection-bond <name> remove-member <remove-member>
```

Parameters

Parameter	Description
name	Connection name A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)
remove-member	List of interfaces that are part of the WAN link aggregation (Bond) Type: String

Example Command

```
set internet-connection-bond "My connection" remove-member My_
Network
```

delete internet-connection-bond

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete a link aggregation (bond) between two or more interfaces (WAN).

Syntax

```
delete internet-connection-bond <name>
```

Parameters

Parameter	Description
name	Connection name A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)

Example Command

```
delete internet-connection-bond My connection
```

show internet-connection-bond

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the link aggregation (bond) between two or more interfaces. (WAN).

Syntax

```
show internet-connection-bond <name>
```

Parameters

Parameter	Description
name	Connection name A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)

Example Command

```
show internet-connection-bond My connection
```

show internet-connections-bond

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the link aggregations (bond) between two or more interfaces (WAN).

Syntax

```
show internet-connections-bond
```

Example Command

```
show internet-connections-bond
```

Configuring Internet Connection Bond for IPv6

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

add internet-connection-ipv6 interface-ipv6

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add an internet connection of type IPv6.

Syntax for the WAN interface

```
add internet-connection-ipv6 [ name <name> ] interface-ipv6
   WAN [ { use-connection-as-vlan } vlan-id <vlan-id> ]
      type-ipv6 static-ipv6 ipv6-address <ipv6-address> prefix-
length <prefix-length> default-gw-ipv6 <default-gw-ipv6> [ dns-
primary-ipv6 <dns-primary-ipv6> ] [ dns-secondary-ipv6 <dns-
secondary-ipv6> ] [ dns-tertiary-ipv6 <dns-tertiary-ipv6> ] [
conn-test-timeout <conn-test-timeout> ]
      type-ipv6 pppoe-ipv6 username <username> { password
<password> | password-hash <password-hash> } [ is-prefix-
delegation {true | false} [ prefix-delegation-prefix-length
<prefix-delegation-prefix-length> ] ] [ conn-test-timeout <conn-
test-timeout> ]
      type-ipv6 pppoe-ipv6-4 linked-connection <linked-connect
ion> [ is-prefix-delegation {true | false} [ prefix-delegation-
prefix-length <prefix-delegation-prefix-length> ] ] [ conn-test-
timeout <conn-test-timeout> ]
      type-ipv6 bridge-ipv6 bridge-name <bridge-name> [ default-gw
<default-gw> ] default-gw-ipv6 <default-gw-ipv6> | auto-obtain [
is-prefix-delegation {true | false} [ prefix-delegation-prefix-
length <prefix-delegation-prefix-length> ] ] [ conn-test-timeout
<conn-test-timeout> ]
```

Syntax for the LAN interfaces

```
add internet-connection-ipv6 [ name <name> ] interface-ipv6
   LAN<X> [ { use-connection-as-vlan } vlan-id <vlan-id> ]
      type dhcp
      type static ipv4-address <ipv4-address> { subnet-mask
<subnet-mask> | mask-length <mask-length> } [ default-gw <default-
gw> ] [ probe-next-hop {true | false} ] [ probe-servers {true |
false} ] [ dns-primary <dns-primary> ] [ dns-secondary <dns-
secondary> ] [ dns-tertiary <dns-tertiary> ] [ conn-test-timeout
<conn-test-timeout> ]
      type bridge bridge-name <bridge-name> bridge-type { static
default-gw <default-gw> [ dns-primary <dns-primary> ] [ dns-
secondary <dns-secondary> ] [ dns-tertiary <dns-tertiary> ] | dhcp
} [ conn-test-timeout <conn-test-timeout> ]
      type l2tp username <username> { password <password> |
password-hash <password-hash> } [ local-ipv4-address <local-ipv4-
address> ] 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> ] [ conn-test-timeout <conn-test-timeout> ]
      type pptp username <username> { password <password> |
password-hash <password-hash> } [ local-ipv4-address <local-ipv4-
address> ] 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> ] [ conn-test-timeout <conn-test-timeout> ]
      type pppoe username <username> { password <password> |
password-hash <password-hash> } [ local-ipv4-address <local-ipv4-
address> ] [ is-unnumbered-pppoe {true | false} ] [ conn-test-
timeout <conn-test-timeout> ]
      type ds-lite linked-ipv6-connection <linked-ipv6-connection>
[ aftr-address <aftr-address> ] [ dns-primary <dns-primary> ] [
dns-secondary <dns-secondary> ] [ dns-tertiary <dns-tertiary> ] [
conn-test-timeout <conn-test-timeout> ]
```

Syntax for the DMZ interface

```
add internet-connection-ipv6 [ name <name> ] interface-ipv6
   DMZ [ { use-connection-as-vlan } vlan-id <vlan-id> ]
      type-ipv6 static-ipv6 ipv6-address <ipv6-address> prefix-
length <prefix-length> default-gw-ipv6 <default-gw-ipv6> [ dns-
primary-ipv6 <dns-primary-ipv6> ] [ dns-secondary-ipv6 <dns-
secondary-ipv6> ] [ dns-tertiary-ipv6 <dns-tertiary-ipv6> ] [
conn-test-timeout <conn-test-timeout> ]
      type-ipv6 pppoe-ipv6 username <username> { password
<password> | password-hash <password-hash> } [ is-prefix-
delegation {true | false} [ prefix-delegation-prefix-length
<prefix-delegation-prefix-length> ] ] [ conn-test-timeout <conn-
test-timeout> ]
      type-ipv6 pppoe-ipv6-4 linked-connection <linked-connection>
[ is-prefix-delegation {true | false} [ prefix-delegation-prefix-
length <prefix-delegation-prefix-length> ] ] [ conn-test-timeout
<conn-test-timeout> ]
      type-ipv6 bridge-ipv6 bridge-name <bridge-name> [ default-gw
<default-gw> ] default-gw-ipv6 <default-gw-ipv6> | auto-obtain [
is-prefix-delegation {true | false} [ prefix-delegation-prefix-
length <prefix-delegation-prefix-length> ] ] [ conn-test-timeout
<conn-test-timeout> ]
```

Syntax for the DSL interface

```
add internet-connection-ipv6 [ name <name> ] interface-ipv6
   DSL [ { use-connection-as-vlan } vlan-id <vlan-id> ]
      type-ipv6 pppoe-ipv6 username <username> { password
<password> | password-hash <password-hash> } [ local-ipv4-address
<local-ipv4-address> ] [ is-unnumbered-pppoe {true | false} ] [
vpi <vpi> ] [ vci <vci> ] [ encapsulation <encapsulation> ] [
conn-test-timeout <conn-test-timeout> ]
      type-ipv6 pppoe-ipv6-4 linked-connection <linked-connection>
[ is-prefix-delegation {true | false} [ prefix-delegation-prefix-
length <prefix-delegation-prefix-length> ] ] [ conn-test-timeout
<conn-test-timeout> ]
```

Syntax for the Cellular interface

```
add internet-connection-ipv6 [ name <name> ] interface-ipv6
   cellular [ primary-sim <primary-sim> ] [ apn-sim1-username
<apn-sim1-username> ] [ apn-sim1-password <apn-sim1-password> ] [
apn-sim1-authentication-method <apn-sim1-authentication-method> ]
[ apn-sim2-username <apn-sim2-username> ] [ apn-sim2-password
<apn-sim2-password> ] [ apn-sim2-authentication-method <apn-sim2-
authentication-method> ] [ sim1-carrier-configuation-package
<sim1-carrier-configuation-package> ] [ sim2-carrier-configuation-
package <sim2-carrier-configuation-package> ] [ apn <apn> ] [ pin
<pin> ] [ apn-sim2 <apn-sim2> ] [ pin-sim2 <pin-sim2> ] [ disable-
sim <disable-sim> ]
```

Parameters

Parameter	Description
aftr-address	Hostname or IPv6 address for DS-Lite tunnel
apn	The Access Point Name given to you by your cellular network carrier for SIM1 A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus)
apn-sim1-authentication-method	The APN authentication method given to you by your cellular network carrier for SIM1 Options: `none`, `pap`, `chap`
apn-sim2-authentication-method	The APN authentication method given to you by your cellular network carrier for SIM2 Options: `none`, `pap`, `chap`
apn-sim1-password	The APN password given to you by your cellular network carrier for SIM1
apn-sim2-password	The APN password given to you by your cellular network carrier for SIM2
apn-sim1-username	The APN username given to you by your cellular network carrier for SIM1 Usually, `<`*`username`*`>@<`*`ISP`*`>`
apn-sim2-username	The APN username given to you by your cellular network carrier for SIM2 Usually, `<`*`username`*`>@<`*`ISP`*`>`
apn-sim2	The Access Point Name given to you by your cellular network carrier for SIM2 A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus)

Parameter	Description
bridge-name	The name of the bridge this connection is bridged to A bridge name should be `br0-9`
bridge-type	The type of the bridge for this connection: DHCP or static Press TAB to see available options
conn-test-timeout	Connection test timeout in seconds
default-gw	WAN default IPv4 gateway (in the advanced section of PPTP and L2TP)
default-gw-ipv6	Default IPv6 gateway
disable-sim	Indicates which SIM, if any, is disabled Options: `sim1`, `sim2`, `none`
dns-primary	IPv4 address of the first DNSv4 server
dns-primary-ipv6	IPv6 address of the first DNSv6 server
dns-secondary	IPv4 address of the second DNSv4 server
dns-secondary-ipv6	IPv6 address of the second DNSv6 server
dns-tertiary	IPv4 address of the third DNSv4 server
dns-tertiary-ipv6	IPv6 address of the third DNSv6 server
encapsulation	Encapsulation type for the ADSL connection
initialization-string	The initialization string for the cellular modem settings A string that contains only upper-case letters (`A-Z`).
interface-ipv6	Interface name for IPv6 Internet connection Press TAB to see available options
ipv6-address	IPv6 address (for static IPv6 settings)
ipv4-address	IPv4 address (for static IPv4 and bridge settings)
is-prefix-delegation	Indicates whether prefix delegation is enabled for this Internet connection
is-unnumbered-pppoe	With unnumbered PPPoE you manage a range of IP addresses and dial only once

Parameter	Description
isVlan	This interface is VLAN
linked-connection	An IPv4 Internet connection with shared credentials A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)
linked-ipv6-connection	IPv6 internet connection name, which the DS-Lite tunnel is defined on
local-ipv4-address	Local tunnel IPv4 address, or automatic An IPv4 address, or '`auto`'
mask-length	IPv4 subnet mask length
method	Authentication method Options: `auto`, `pap`, `chap`
name	Connection name A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)
number	Dialed number of the cellular modem settings A sequence of numbers and #,* characters
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
pin	The Personal Identification Number code given to you by your cellular network carrier for SIM1

Parameter	Description
pin-sim2	The Personal Identification Number code given to you by your cellular network carrier for SIM2
prefix-delegation-prefix-length	IPv6 prefix length for prefix delegation
prefix-length	IPv6 prefix length field (for IPv6 static IP settings)
primary-sim	Indicates the preferred SIM for the cellular internet connection Options: `sim1`, `sim2`
probe-next-hop	Controls whether to detect (`true`) or not (`false`) automatically the loss of connectivity to the default gateway
probe-servers	Monitor connection state by sending probe packets to one or more servers on the Internet
server	Server IP address
sim1-carrier-configuation-package	Predefined configuration and firmware package required for specific cellular net-work carriers for SIM1 Options: `att`, `generic`, `rogers`, `sprint`, `verizon`, `verizon-alo`, `bell`, `vodafone`, `telus`, `us-cellular`, `sierra-wireless`, `docomo`, `kddi`, `softbank`, `telstra`
sim2-carrier-configuation-package	Predefined configuration and firmware package required for specific cellular net-work carriers for SIM2 Options: `att`, `generic`, `rogers`, `sprint`, `verizon`, `verizon-alo`, `bell`, `vodafone`, `telus`, `us-cellular`, `sierra-wireless`, `docomo`, `kddi`, `softbank`, `telstra`
subnet-mask	IPv4 subnet mask A subnet mask, or 255.255.255.255
type	Connection type Press TAB to see available options
type-ipv6	Connection type for IPv6 Internet connection Press TAB to see available options
username	User name for PPP connection or cellular modem settings Usually, `<`*`username`*`>@<`*`ISP`*`>`
vci	VCI value for the ADSL connection A number between 0 and 65535

Parameter	Description
vlan-id	VLAN ID
vpi	VPI value for the ADSL connection A number between 0 and 255
wan-ipv4-address	IPv4 address wrapper for the WAN interface An IP address, or '`auto`'
wan-mask-length	IPv4 subnet mask length for the WAN interface
wan-subnet-mask	IPv4 subnet mask (in the advanced section) for the WAN interface

Example Command

```
add internet-connection-ipv6 name "My connection" interface-ipv6
LAN4 true vlan-id 200 type dhcp conn-test-timeout 50
```

add internet-connection-ipv6 interface-ipv6 WAN type-ipv6 bridge-ipv6 bridge type dhcp

In the R81.10.X releases, this command is available starting from the R81.10.08 version.

Description

When you create a new IPv6 internet connection, you can create a connection type IPv6 Bridge and select type DHCP/SLAAC instead of just Static IP.

Note - When an IPv6 bridge internet connection is defined, no additional internet connections can be defined.

Syntax

```
add internet-connection-ipv6 interface-ipv6 WAN type-ipv6 bridge-
ipv6 bridge-name <bridge_name> bridge type { static-ipv6 | dhcp }
```

Parameters

Parameter	Description
bridge-name	Name of the IPv6 bridge
bridge type	Options: ■ `static-ipv6` ■ `dhcp`

Example Command

```
add internet-connection-ipv6 interface-ipv6 WAN type-ipv6 bridge-
ipv6 bridge-name br0 bridge type dhcp
```

set internet-connection-ipv6 auto-negotiation link-speed mtu

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure an existing IPv6 internet connection.

Syntax

```
set internet-connection-ipv6 <name> [ auto-negotiation {on | off}
] [ link-speed link-speed ] [ mtu 68-1500 ] [ mac-addr <mac-
address> ]
```

Parameters

Parameter	Description
auto-negotiation	Controls whether the interface configures the link speed automatically (`on`) or manually (`off`).

Parameter	Description
link-speed	Configures the link speed of the interface manually: ■ `1/full` - 1 Gbps/Full duplex ■ `1/half` - 1 Gbps/Half duplex ■ `100/full` - 100 Mbps/Full duplex ■ `100/half` - 100 Mbps/Half duplex ■ `100BaseFx` - 100Base-FX ■ `10/full` - 10 Mbps/Full duplex ■ `10/half` - 10 Mbps/Half duplex
mac-addr	Configures the MAC Address.
mtu	Configures the Maximum Transmission Unit size (in bytes).
name	Specifies the interface / connection. Press the TAB key to see the available options.

Example Command

```
set internet-connection-ipv6 "My connection" auto-negotiation on
link-speed 100/full mtu 1460 mac-addr 00:1C:7F:21:05:BE
```

set internet-connection-ipv6

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure an IPv6 internet connection.

Syntax

```
set internet-connection-ipv6 <name> { enable | disable }
```

Parameters

Parameter	Description
name	Connection name A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)
state	Connection enabled/disabled Type: Boolean (true/false)

Example Command

```
set internet-connection-ipv6 "My connection" true
```

set internet-connection-ipv6

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure an IPv6 internet connection.

Syntax

```
set internet-connection-ipv6 <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)

Parameter	Description
name	Connection name A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)

Example Command

```
set internet-connection-ipv6 "My connection" disable-nat true
```

set internet-connection-ipv6

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure an IPv6 internet connection.

Syntax

```
set internet-connection-ipv6 <name> type-ipv6 { pppoe-ipv6-4
linked-connection <linked-connection> [ is-prefix-delegation {true
| false} [ prefix-delegation-prefix-length <prefix-delegation-
prefix-length> ] ] | usb-cellular-ipv6 [ number <number> ] [
username <username> ] [ { password <password> | password-hash
<password-hash> } ] [ apn <apn> ] [ local-ipv4-address <local-
ipv4-address> ] [ is-unnumbered-pppoe {true | false} ] [ method
<method> ] [ initialization-string <initialization-string> ] [
conn-test-timeout <conn-test-timeout> ] | auto-obtain [ is-prefix-
delegation {true | false} [ prefix-delegation-prefix-length
<prefix-delegation-prefix-length> ] ] | bridge-ipv6 bridge-name
<bridge-name> [ default-gw <default-gw> ] [ default-gw-ipv6
<default-gw-ipv6> ] | pppoe-ipv6 username <username> { password
<password> | password-hash <password-hash> } [ is-prefix-
delegation {true | false} [ prefix-delegation-prefix-length
<prefix-delegation-prefix-length> ] ] | static-ipv6 ipv6-address
<ipv6-address> prefix-length <prefix-length> default-gw-ipv6
<default-gw-ipv6> [ dns-primary-ipv6 <dns-primary-ipv6> ] [ dns-
secondary-ipv6 <dns-secondary-ipv6> ] [ dns-tertiary-ipv6 <dns-
tertiary-ipv6> ] }
```

Parameters

Parameter	Description
apn	The Access Point Name given to you by your cellular network carrier for SIM1. A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus)
bridge-name	The name of the bridge this connection is bridged to A bridge name should be br0-9
conn-test-timeout	Connection test timeout A number with no fractional part (integer)
default-gw	Default gateway

Parameter	Description
default-gw-ipv6	Default gateway
dns-primary-ipv6	First DNS server IPv6 address
dns-secondary-ipv6	Second DNS server IPv6 address
dns-tertiary-ipv6	Third DNS server IPv6 address
initialization-string	The initialization string for the cellular modem settings A string that contains only upper-case letters (`A-Z`).
ipv6-address	IPv6 address field (for static IP settings)
is-prefix-delegation	Indicates whether prefix delegation is enabled for this Internet connection Type: Boolean (true/false)
is-unnumbered-pppoe	Unnumbered PPPoE lets you manage a range of IP addresses and dial only once Type: Boolean (true/false)
linked-connection	An IPv4 Internet connection with shared credentials A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)
local-ipv4-address	Local tunnel IP address or auto for automatic An IP address, or '`auto`'
method	Authentication method Options: auto, pap, chap

Parameter	Description
name	Connection name A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)
password	Password for PPP connection or cellular modem settings
password-hash	The hash of the user password
prefix-delegation-prefix-length	Prefix length for prefix delegation
prefix-length	Prefix length field (for IPv6 static IP settings)
type-ipv6	Connection type for IPv6 Internet connection Press TAB to see available options
username	User name for PPP connection or cellular modem settings Usually <username>@<ISP>

Example Command

```
set internet-connection-ipv6 "My connection" type-ipv6 pppoe-ipv6-
4 linked-connection "My connection" is-prefix-delegation true
prefix-delegation-prefix-length ipv6prefixLength
```

set internet-connection-ipv6

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure an IPv6 internet connection.

Syntax

```
set internet-connection-ipv6 <name> probe-next-hop {true | false}
```

Parameters

Parameter	Description
name	Connection name A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ ' ' (space)
probe-next-hop	Automatically detect loss of connectivity to the default gateway Type: Boolean (true/false)

Example Command

```
set internet-connection-ipv6 "My connection" probe-next-hop true
```

Working with Internet Advanced Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure and view the Internet advanced settings.

set internet-advanced-settings reset-sierra-usb

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure advanced global internet settings.

Syntax

```
set internet advanced-settings reset-sierra-usb-on-lsi-event {true
| false}
```

Parameters

Parameter	Description
reset-sierra-usb-on-lsi-event	Indicates whether Sierra type USB modems will be reset when they send an Invalid LSI signal

Example Command

```
set internet advanced-settings reset-sierra-usb-on-lsi-event true
```

show internet-advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show internet advanced global settings.

Syntax

```
show internet advanced-settings
```

Example Command

```
show internet advanced-settings
```

Configuring the Date, Time, Timezone

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the date, time, and timezone settings.

set date

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Manually configure the device's date.

Syntax

```
set date <date>
```

Parameters

Parameter	Description
date	Date in the format YYYY-MM-DD

Example Command

```
set date 2021-01-30
```

set time

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Manually configure the device's time.

Syntax

```
set time <time>
```

Parameters

Parameter	Description
time	Time in the format HH:MM

Example Command

```
set time 23:20
```

set timezone

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Manually configure the device's time zone.

Syntax

```
set timezone <timezone>
```

Parameters

Parameter	Description
timezone	Specifies the timezone. Press the TAB key to see the available options.

Example Command

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

set time-zone

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Manually configure the device's time zone location.

Syntax

```
set timezone <timezone>
```

Parameters

Parameter	Description
timezone	Timezone Press the TAB key to see the available options.

Example Command

```
set time-zone GMT-11:00(Midway-Island)
```

set timezone-dst

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the appliance whether to use the daylight savings automatically.

Syntax

```
set timezone-dst automatic {on | off}
```

Parameters

Parameter	Description
timezone-dst automatic	Configures the appliance to use (`on`) or not (`off`) the daylight savings automatically.

Example Command

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

set auto-timeZone

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the appliance to determine the time zone automatically without user input in the First Time Configuration Wizard.

Note - To enable this feature, you must run the *"set privacy-settings advanced-settings customer-consent" on page 587* command to set the consent flags to "`true`":

```
set privacy-settings advanced-settings customer-consent
true location-service-consent true
```

Syntax

```
set auto-timeZone { on | off }
```

Example Command

```
set auto-timeZone on
```

show clock

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the current system date, time, and time zone.

Syntax

```
show clock
```

Example Output

```
HostName> show clock
Fri Sep 17 12:39:24 GMT+0200 2021
HostName>
```

show date

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows current date of the appliance.

Syntax

```
show date
```

Example Command

```
show date
```

show time

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows current time of the appliance.

Syntax

```
show time
```

Example Output

```
HostName> show time
time:                           19:52:24
```

show timezone

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows current time zone of the appliance.

Syntax

```
show timezone
```

Example Command

```
show timezone
```

show timezone-dst

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows current daylight savings configuration of the appliance.

Syntax

```
show timezone-dst
```

Example Output

```
HostName> show timezone-dst
timezone-dst:                   on
```

show auto-timeZone

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows if the automatic detection of the timezone is turned on or off (see *"set auto-timeZone" on page 398*).

Syntax

```
show autogmt
```

Example Output

```
HostName> show auto-timeZone
auto-timeZone:                  off
```

Firewall 'Access' Rules for Incoming, Internal, and VPN Traffic

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Firewall 'Access' rules for incoming, internal, and VPN Traffic.

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new Firewall Access rule to the incoming / internal / VPN traffic policy.

Syntax

```
add access-rule type incoming-internal-and-vpn
      [ action <action> ]
      [ comment "<comment>"]
      [ destination <destination> ]
      [ destination-negate <destination-negate> ]
      [ disabled <disabled> ]
      [ hours-range-enabled { false | true hours-range-from
<hours-range-from> hours-range-to <hours-range-to> } ]
      [ log <log> ]
      [ name <name> ]
      [ service <service> ]
      [ service-negate <service-negate> ]
      [ source <source> ]
      [ source-negate <source-negate> ]
      [ { position <position> | position-above <position-above> |
position-below <position-below>} ]
      [ 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 A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
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
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

Parameter	Description
name	name A string of alphanumeric characters **without** space between them: ▪ `a-z` (lower-case letters) ▪ `A-Z` (upper-case letters) ▪ `0-9` (digits)
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 Command

```
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 MyRule vpn true
```

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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

Parameter	Description
comment	Description of the rule A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
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
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 A string of alphanumeric characters **without** space between them: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits)
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)
vpn	Indicates if traffic is matched on encrypted traffic only or all traffic Type: Boolean (true/false)

Example Command

```
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 MyRule vpn
true
```

```
set access-rule type incoming-internal-and-vpn name MyRule 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 vpn true
```

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
position	The order of the rule in comparison to other manual rules Type: Decimal number

Example Command

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

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

delete access-rules type incoming-internal-and-vpn all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

One of the commands that allows the user to delete manual access rules configured on the Firewall Access Policy page in the WebUI.

See *"delete access-rules type outgoing-all" on page 420*.

This command specifically deletes incoming, internal and VPN traffic.

Syntax

```
delete access-rules type incoming-internal-and-vpn all
```

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)

Example Command

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

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

Firewall 'Access' Rules for Outgoing Traffic

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Firewall 'Access' rules for outgoing traffic.

add access-rule type outgoing

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 {
false | true hours-range-from <hours-range-from> hours-range-to
<hours-range-to> } ] [ { 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 A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
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) A number with no fractional part (integer)
limit-application-download	If true, download is limited Type: Boolean (true/false)

Parameter	Description
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 A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
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 Command

```
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 MyRule application-name hasOne
application-negate true limit-application-download true limit 200
limit-application-upload true limit 5
```

set access-rule type outgoing

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
application-negate	If true, the rule accepts or blocks all applications but the selected application Type: Boolean (true/false)
comment	Description of the rule A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
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

Parameter	Description
hours-range-to	Time in the format HH:MM Type: A time format hh:mm
limit	Applications traffic upload limit (in kbps) 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 A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
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 Command

```
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 MyRule application-name
hasOne application-negate true limit-application-download true
limit 100 limit-application-upload true limit 5
```

```
set access-rule type outgoing name MyRule 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 application-name hasOne
application-negate true limit-application-download true limit 100
limit-application-upload true limit 5
```

delete access-rules type outgoing-all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

One of the commands that allows the user to delete manual access rules configured on the Firewall Access Policy page in the WebUI.

This commands deletes outgoing access to the Internet.

See *"delete access-rules type incoming-internal-and-vpn all" on page 412*.

Syntax

```
delete access-rules type outgoing all
```

delete access-rule type outgoing

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)

Example Command

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

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

show access-rule type outgoing

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
position	The order of a manual rule in comparison to other manual rules Type: Decimal number

Example Command

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

Additional Management Settings

This section provides commands to configure additional management settings.

set additional-management-settings install-temporary-policy-to-storage

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure additional management settings.

Syntax

```
set additional-management-settings advanced-settings install-
temporary-policy-to-storage { true | false }
```

Parameters

Parameter	Description
install-temporary-policy-to-storage	Controls whether the temporary policy installation files are be saved (`true`) or not (`false`) in the "`/storage`" partition

Example Command

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

show additional-management-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the additional management settings and their status.

Syntax

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

Example Output

```
HostName> show additional-management-settings
advanced-settings install-temporary-policy-to-storage:false
```

Configuring DNS Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure DNS settings.

set dns

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
secondary ipv4- address	Second global DNS IP address
tertiary ipv4-address	Third global DNS IP address

Example Command

```
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-ipv6 ipv6-proxy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables or disables the IPv6 DNS Proxy to relay DNSv6 requests from internal network clients to the DNSv6 servers.

Syntax

```
set dns-ipv6 ipv6-proxy {enable [ ipv6-resolving {on \| off}] |
disable}
```

Parameters

Parameter	Description
ipv6-proxy	Enables or disables the IPv6 DNS Proxy. Press TAB to see available options.
ipv6-resolving	Enables or disables the use of network objects as a host list to translate names to their IP addresses.

Example Command

```
set dns-ipv6 ipv6-proxy enable ipv6-resolving on
```

set dns-ipv6 ipv6-mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the DNS and Domain settings for an IPv6 connection.

Syntax

```
set dns-ipv6 ipv6-mode {global | internet}
```

Parameters

Parameter	Description
ipv6-mode	■ `internet` - The equivalent of selecting the radio button **Use DNS servers configured for the active Internet connection(s)** in the WebUI. ■ `global` - The equivalent of selecting the radio button **Configure DNS servers in the WebUI**.

Example Command

```
set dns-ipv6 ipv6-mode global
```

```
set dns-ipv6 ipv6-mode internet/global primary ipv6-address
<Primary_IPv6_address>
```

is the equivalent of selecting the radio button **Configure DNS servers** and sets the **Primary DNS server**. The same flow occurs for the **Second DNS server** and **Third DNS server**.

set dns-ipv6

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the IPv6 DNS Servers.

Syntax

```
set dns-ipv6 [ primary ipv6-address <IPv6-Address> ] [ secondary
ipv6-address <IPv6-Address> ] [ tertiary ipv6-address <IPv6-
Address> ]
```

Parameters

Parameter	Description
primary ipv6-address	First global DNS IPv6 address
secondary ipv6-address	Second global DNS IPv6 address
tertiary ipv6-address	Third global DNS IPv6 address

Example Command

```
set dns-ipv6 primary ipv6-address 2001:4860:4860::8888 secondary
ipv6-address 2001:4860:4860::8844
```

set dns mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set dns mode global
```

set dns proxy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 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 Command

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

set domainname

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the domain settings for the device.

Syntax

```
set domainname <domainname>
```

Parameters

Parameter	Description
domainname	A Fully Qualified Domain Name (FQDN)

Example Command

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

show dns

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration for DNS.

Syntax

```
show dns
```

Example Command

```
show dns
```

show domainname

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration for domain name.

Syntax

```
show domainname
```

delete dns

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes the configured IPv4 DNS server.

Syntax

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

Parameters

Parameter	Description
ipv4-address	IP address of the applicable DNS server

Example Command

```
delete dns primary 192.168.3.1
```

delete dns-ipv6

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes the configured IPv6 DNS Servers.

Syntax

```
delete dns-ipv6 [ primary ipv6-address ] [ secondary ipv6-address
] [ tertiary ipv6-address ]
```

Example Command

```
delete dns-ipv6 primary ipv6-address
```

delete domainname

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes configured domain name of the appliance.

Syntax

```
delete domainname
```

Configuring Dynamic-DNS (DDNS) Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Dynamic-DNS (DDNS) settings - a persistent domain name for the appliance.

set dynamic-dns

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures a persistent domain name for the device.

Syntax

```
set dynamic-dns {enable | disable} 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
password	The password of the account 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 Command

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

set dynamic-dns

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure advanced settings for the DDNS service.

Syntax

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

Parameters

Parameter	Description
n/a	

Example Command

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

show dynamic-dns

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration for DDNS service.

Syntax

```
show dynamic-dns
```

Parameters

Parameter	Description
n/a	

Example Command

```
show dynamic-dns
```

show dynamic-dns

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced settings for DDNS service.

Syntax

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

Parameters

Parameter	Description
n/a	

Example Command

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

Configuring NTP Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure NTP (Network Time Protocol) settings.

set ntp active

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables or disables the NTP configuration.

Syntax

```
set ntp active {on | off}
```

Example Command

```
set ntp active on
```

set ntp interval

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures how frequently to update the time from the NTP servers.

Syntax

```
set ntp interval <1-999>
```

Parameters

Parameter	Description
interval	Configures the frequency (in minutes) of updates from the NTP servers.

Example Command

```
set ntp interval 15
```

set ntp auth

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures authentication settings with NTP servers.

Syntax

```
set ntp auth { off | on secret-id <secret-id> secret <secret> }
```

Parameters

Parameter	Description
auth	Enables (`on`) or disables (`off`) the authentication with NTP servers.
secret	Configures the key for authentication with the NTP servers. A string that contains alphanumeric and special characters.
secret-id	Configures the authentication key identifier (between -4,503,599,627,370,495 and 4,503,599,627,370,495).

Example Command

```
set ntp auth on secret-id 455397 secret a(&7Ba
```

set ntp local-time-zone

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the local time zone.

Syntax

```
set ntp local-time-zone <local-time-zone>
```

Parameters

Parameter	Description
local-time-zone	Specifies the time zone. See the available options in *"set timezone" on page 396*.

Example Command

```
set ntp local-time-zone GMT-11:00(Midway-Island)
```

set ntp auto-adjust-daylight-saving

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables or disables the automatic daylight saving (DST).

Syntax

```
set ntp auto-adjust-daylight-saving {on | off}
```

Example Command

```
set ntp auto-adjust-daylight-saving on
```

set ntp local-server

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables and disables a local NTP server on the appliance.

Computers connected to the appliance can use this NTP server to synchronize their clocks.

The default configuration for the NTP server allows all connected devices on internal networks to synchronize over NTP. To restrict access to the NTP server, the user must create additional security rules.

Syntax

```
set ntp local-server {on | off}
```

Parameters

Parameter	Description
n/a	

Example Command

```
set ntp local-server on
```

set ntp server primary

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set ntp server primary myHost.com
```

set ntp server secondary

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set ntp server secondary myHost.com
```

show ntp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows NTP configuration.

Syntax

```
show ntp
```

Example Command

```
show ntp
```

show ntp active

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows NTP activation status.

Syntax

```
show ntp active
```

Example Command

```
show ntp active
```

show ntp servers

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows all defined NTP servers.

Syntax

```
show ntp servers
```

Example Command

```
show ntp servers
```

Configuring DHCP Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure DHCP settings.

dhcp-bridge-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

show dhcp-bridge-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the MAC address for the DHCP bridge.

Syntax

```
show dhcp-bridge-settings
```

Example Command

```
show dhcp-bridge-settings
```

set dhcp-bridge-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the MAC address for the DHCP bridge from an internal (LAN) or external port (WAN, DMZ).

Syntax

```
set dhcp-bridge-settings mac-assignment <mac-assignment>
```

Parameters

Parameter	Description
mac-assignment	Indicates whether the MAC address for the DHCP bridge is taken from an internal (LAN) or external port (WAN, DMZ). Options: use-internal-interfaces-mac, use-external-interfaces-mac

Example Command

```
set dhcp-bridge-settings mac-assignment use-internal-interfaces-
mac
```

dhcp-relay

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

set dhcp-relay

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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>
```

Example Command

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

show dhcp-relay

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced settings for DHCP relay.

Syntax

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

Example Command

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

show dhcp servers

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration for all DHCP servers.

Syntax

```
show dhcp servers
```

Parameters

Parameter	Description
n/a	

Example Command

```
show dhcp servers
```

dhcp-ipv6-server-interface

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

set dhcp-ipv6-server-interface

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the DHCP IPV6 server interface.

Syntax

```
set dhcp-ipv6 server interface <name> [ {disable | enable } ] [
dns-ipv6 { none | manual [primary <primary> ] [ secondary
<secondary> ] [ tertiary <tertiary> ] | auto } ] [ include-ipv6-
pool <include-ipv6-pool> ] [ exclude-ipv6-pool <exclude-ipv6-pool>
] [ relay relay-to <relay relay-to> [ secondary <secondary> ]
```

Parameters

Parameter	Description
dhcp-ipv6	Use DHCPv6 Server with a specified IP address range Options: off, on, relay, slaac
dns-ipv6	Configure the DNS Server Press TAB to see available options
exclude-ipv6-pool	DHCPv6 exclude range (IPv6 address range format) Type: ipv6range
include-ipv6-pool	DHCPv6 range Type: ipv6range
name	Network name A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ '/' (slash)
primary	Configure the IPv6 address for the first DNS server
relay relay-to	Configure DHCPv6 server IP address

Parameter	Description
secondary	Configure the IPv6 address for the second DNS server
tertiary	Configure the IPv6 address for the third DNS server

Example Command

```
set dhcp-ipv6 server interface My_Network off dns-ipv6 none
include-ipv6-pool ipv6range exclude-ipv6-pool ipv6range relay
relay-to ipv6addr secondary ipv6addr
```

delete dhcp-ipv6-server-interface

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete the DHCP IPV6 server interface.

Syntax

```
delete dhcp-ipv6 server interface <name> exclude-range
```

Parameters

Parameter	Description
name	Network name A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ '/' (slash)

Example Command

```
delete dhcp-ipv6 server interface My_Network exclude-range
```

show dhcp-ipv6-server-interface

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the DHCP IPV6 server interface.

Syntax

```
show dhcp-ipv6 server interface <name>
```

Parameters

Parameter	Description
name	Network name A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ '/' (slash)

Example Command

```
show dhcp-ipv6 server interface LAN8
```

Example Output

DHCPv6 Server

```
dhcp-ipv6: on
include-ipv6-pool: 2620:0:2a03:83::-
2620:0:2a03:83:ffff:ffff:ffff:ffff
exclude-ipv6-pool:
relay relay-to:
secondary:
dns-ipv6: auto
dns-ipv6 primary:
dns-ipv6 secondary:
dns-ipv6 tertiary:
```

DHCPv6 Server Relay

```
dhcp-ipv6: relay
include-ipv6-pool: 2620:0:2a03:83::-
2620:0:2a03:83:ffff:ffff:ffff:ffff
exclude-ipv6-pool:
relay relay-to: 2620:0:2a03:83::
secondary: 2620:0:2a03:84::
dns-ipv6: auto
dns-ipv6 primary:
dns-ipv6 secondary:
dns-ipv6 tertiary:
```

dhcp server interface

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

set dhcp server interface {enable | disable}

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables and disables DHCP server on an existing interface / connection.

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.

Example Command

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

set dhcp server interface default-gateway

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
default-gateway	A virtual field calculated by the values of the fields: dhcpGwMode & dhcpGw

Example Command

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

set dhcp server interface domain

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
domain	The domain name of the DHCP

Example Command

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

set dhcp server interface dns

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the DNS servers provided by a DHCP server on an existing interface / connection.

In the automatic mode the device provides 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
      auto
      manual [ primary <primary> ] [ secondary <secondary> ] [
tertiary <tertiary> ]
      none
```

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
dns	Configure the DNS Server
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 Command

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

set dhcp server interface dns primary

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
dns primary	Configure the IP address for the first DNS server

Example Command

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

set dhcp server interface dns secondary

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
dns secondary	Configure the IP address for the second DNS server

Example Command

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

set dhcp server interface dns tertiary

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
dns tertiary	Configure the IP address for the third DNS server

Example Command

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

set dhcp server interface dns quaternary

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
dns quaternary	Configure the IP address for the third DNS server

Example Command

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

set dhcp server interface lease-time

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
lease-time	Configure the timeout in hours for a single device to retain a dynamically acquired IP address

Example Command

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

set dhcp server interface include-ip-pool

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
include-ip-pool	DHCP range Type: A range of IP addresses

Example Command

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

set dhcp server interface ntp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
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 Command

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

set dhcp server interface tftp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
tftp	Configure TFTP server to be distributed to DHCP client

Example Command

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

set dhcp server interface file

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

```
set dhcp server interface <name> file <Absolute path to bootfile
on TFTP server>
```

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
file	Configure TFTP bootfile to be distributed to DHCP client

Example Command

```
set dhcp server interface My_Network file /storage/tftp_boot.txt
```

set dhcp server interface relay

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures DHCP relay functionality on an existing interface / connection.

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
relay relay-to	Enter the DHCP server IP address
relay-secondary	This field is deprecated. Please use field 'secondary'
secondary	Enter the secondary DHCP server IP address

Example Command

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

set dhcp server interface remove custom-option

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
custom-option	Set the name of the object

Example Command

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

set dhcp server interface custom-option

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures a custom DHCP option.

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
custom-option name	Set the name of the object A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '-' (minus)
data	Set the desired value of the object Type: String
tag	Select a unique tag for the object 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 Command

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

set dhcp server interface callmgr

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
callmgr	Configure the first Call manager server to be distributed to DHCP client
secondary	Configure the second Call manager server to be distributed to DHCP client

Example Command

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

set dhcp server interface avaya-voip

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
avaya-voip	Configure Avaya IP phone to be distributed to DHCP client

Example Command

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

set dhcp server interface nortel-voip

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
nortel-voip	Configure Nortel IP phone to be distributed to DHCP client

Example Command

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

set dhcp server interface thomson-voip

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
thomson-voip	Configure Thomson IP phone to be distributed to DHCP client

Example Command

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

set dhcp server interface xwin-display-mgr

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
xwin-display-mgr	Configure X-Windows display manager to be distributed to a DHCP client

Example Command

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

set dhcp server interface wins-mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
wins-mode	Configure the WINS Server

Example Command

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

set dhcp server interface wins primary

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.
secondary	Configure the IP address for the second WINS server
wins primary	Configure the IP address for the first WINS server

Example Command

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

delete dhcp server interface

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Network name A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ '/' (slash)

Example Command

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

show dhcp server interface ip-pool

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Specifies the name of the interface / connection. Press the TAB key to see the available options.

Example Command

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

show dhcp server interface

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
name	Specifies the name of the interface / connection. Press the TAB key to see the available options.

Example Command

```
show dhcp server interface My_Network
```

Configuring SNMP Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure SNMP settings.

add snmp user

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new user to be used by SNMPv3 protocol.

See:

- *"show snmp user" on page 534*
- *"show snmp users" on page 535*
- *"set snmp user" on page 514*
- *"delete snmp user" on page 520*
- *"delete snmp users all" on page 521*

Syntax

```
add snmp user <user> security-level
      authPriv auth-pass-type <auth-pass-type> auth-pass-phrase
<auth-pass-phrase> privacy-pass-type <privacy-pass-type> privacy-
pass-phrase <privacy-pass-phrase>
      authNoPriv auth-pass-type <auth-pass-type> auth-pass-phrase
<auth-pass-phrase>
```

Parameters

Parameter	Description
auth-pass-phrase	Configures the authentication password for the SNMP v3 user. A string that contains alphanumeric and special characters.
auth-pass-type	Configures the authentication protocol type for the SNMP v3: ■ `SHA512` ■ `SHA256` ■ `SHA1` ■ `MD5`
privacy-pass-phrase	Configures the privacy authentication password for the SNMP v3 user. A string that contains alphanumeric and special characters.

Parameter	Description
privacy-pass-type	Configures the privacy protocol for the SNMP v3 user: ■ `AES256` ■ `AES` ■ `DES`
security-level	Controls whether to configure (`authPriv`) or not (`authNoPriv`) the privacy protocol for this SNMP v3 user.
user	Configures the SNMP v3 user name. A string that contains up to 64 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '@' (at)

Example Command

```
add snmp user SnmpUser security-level authNoPriv auth-pass-type
MD5 auth-pass-phrase 12345689
```

add snmp traps-receiver

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new SNMP trap receiver by IP address.

See:

- *"show snmp traps receivers" on page 529*
- *"set snmp traps receiver" on page 512*
- *"delete snmp traps-receiver" on page 518*
- *"delete snmp traps-receivers all" on page 519*

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 A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
traps-receiver	Configures the trap receiver IP address.
user	Configures the SNMP v3 user.

Example Command

```
add snmp traps-receiver 192.168.1.1 version v2 community
MySnmpCommunity
```

set snmp agent

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables or disables (this is the default) the SNMP Agent.

See *"show snmp agent" on page 522*.

Syntax

```
set snmp agent {on | off}
```

Example Command

```
set snmp agent on
```

set snmp agent-version

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the SNMP Agent version.

See *"show snmp agent-version" on page 523*.

Syntax

```
set snmp agent-version agent-version {v3-only | any}
```

Example Command

```
set snmp agent-version agent-version v3-only
```

set snmp community

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the SNMP v2 community name.

See *"show snmp community" on page 524*.

Syntax

```
set snmp community <community>
```

Parameters

Parameter	Description
community	Configures the SNMP v2 community name. The default name is "`public`". A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ '@' (at)

Example Command

```
set snmp community MySnmpCommunity
```

set snmp contact

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the SNMP contact.

See *"show snmp contact" on page 525*.

Syntax

```
set snmp contact <contact>
```

Parameters

Parameter	Description
contact	Configures the SNMP contact name. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)

Example Command

```
set snmp agent contact MyContact
```

set snmp location

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the SNMP location.

See *"show snmp location" on page 526*.

Syntax

```
set snmp location <location>
```

Parameters

Parameter	Description
location	Configures the SNMP location name. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)

Example Command

```
set snmp agent location MyLocation
```

set snmp traps enable/disable

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables or disables the SNMP traps functionality.

See *"show snmp traps status" on page 528*.

Syntax

```
set snmp traps { enable | disable }
```

Example Command

```
set snmp traps enable
```

set snmp traps trap-name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an SNMP trap.

See *"show snmp traps enabled-traps" on page 530*.

Syntax

```
set snmp traps trap-name <trap-name> [ enable {on | off} ] [
severity <1-4> ] [ repetitions <1-10> ] [ repetitions-delay <30-
3600> ] [ threshold <threshold-value> ]
```

Parameters

Parameter	Description
enable	Enables or disables this SNMP trap.
repetitions	Configures the number of repetitions for sending the SNMP trap during the event.
repetitions-delay	Configures the time (in seconds) between sending each SNMP trap during the event.
severity	Configures the severity for the SNMP trap.
threshold	Configures the threshold value, above / below which to start sending the SNMP trap.
trap-name	Specifies the SNMP trap.

Supported SNMP Traps

Trap Name in Gaia Clish	Monitored Object	Description	Default Trap State	Threshold Operand	Threshold Default Value	Threshold Valid Values	Trap Default Severity	Trap Default Repetitions	Default Repetition Delay	Trap SNMP OID
`interface-disconnected`	Interface disconnected	Either network cable was disconnected, ICMP monitor failed to reach a monitored server, or LAN interface was manually disabled	Enabled	N/A	N/A	N/A	4	1	30	1.3.6.1.4.1.2620.1.2000.1.1
`"VLAN removed"`	VLAN removed	VLAN was removed from a physical interface	Enabled	N/A	N/A	N/A	4	1	30	1.3.6.1.4.1.2620.1.2000.1.2

Trap Name in Gaia Clish	Monitored Object	Description	Default Trap State	Threshold Operand	Threshold Default Value	Threshold Valid Values	Trap Default Severity	Trap Default Repetitions	Default Repetition Delay	Trap SNMP OID
high-connections-rate	High connection rate	New connection rate is above the configured threshold value (connections / second)	Enabled	eq_gt	3000	1 - 10000	4	1	30	1.3.6.1.4.1.2620.1.2000.1.3
high-concurrent-connections	High concurrent connections	The number of concurrent connections is above the configured threshold value	Enabled	eq_gt	50000	0 - 300000	4	1	30	1.3.6.1.4.1.2620.1.2000.1.4

Trap Name in Gaia Clish	Monitored Object	Description	Default Trap State	Threshold Operand	Threshold Default Value	Threshold Valid Values	Trap Default Severity	Trap Default Repetitions	Default Repetition Delay	Trap SNMP OID
`low-disk-space`	Free disk space	Free space on a disk partition free space is below the configured threshold value (%)	Enabled	eq_lt	10	0 - 100	4	1	30	1.3.6.1.4.1.2620.1.2000.2.1
`high-cpu-utilization`	CPU utilization	CPU usage is above the configured threshold value (%)	*Disabled*	eq_gt	95	0 - 100	4	1	30	1.3.6.1.4.1.2620.1.2000.3.1

Trap Name in Gaia Clish	Monitored Object	Description	Default Trap State	Threshold Operand	Threshold Default Value	Threshold Valid Values	Trap Default Severity	Trap Default Repetitions	Default Repetition Delay	Trap SNMP OID
`high-cpu-interrupts-rate`	High CPU interrupts rate	Accepted packet rate is above the configured threshold value (interrupts / seconds)	*Disabled*	eq_gt	20000000	0 - 214748364 0	4	1	30	1.3.6.1.4.1.2620.1.2000.3.2
`high-memory-utilization`	Memory utilization	Memory utilization is above the configured threshold value (%)	Enabled	gt	90	0 - 100	4	1	30	1.3.6.1.4.1.2620.1.2000.4.2

Trap Name in Gaia Clish	Monitored Object	Description	Default Trap State	Threshold Operand	Threshold Default Value	Threshold Valid Values	Trap Default Severity	Trap Default Repetitions	Default Repetition Delay	Trap SNMP OID
high-firewall-throughput	High Firewall throughput	Firewall throughput is above the configured threshold value (megabytes / second)	Enabled	eq_gt	1000	0 - 3000	4	1	30	1.3.6.1.4.1.2620.1.2000.1.5
high-accepted-packet-rate	High accepted packet rate	Accepted packet rate is above the configured threshold value (packets / second)	Enabled	eq_gt	100000	0 - 300000	4	1	30	1.3.6.1.4.1.2620.1.2000.1.6

Trap Name in Gaia Clish	Monitored Object	Description	Default Trap State	Threshold Operand	Threshold Default Value	Threshold Valid Values	Trap Default Severity	Trap Default Repetitions	Default Repetition Delay	Trap SNMP OID
`cluster-member-state-changed`	Cluster member state changed	Cluster member state changed (the cluster member identifier is provided in the trap)	*Disabled*	N/A	N/A	N/A	4	1	30	1.3.6.1.4.1.2620.1.2000.6.1
`cluster-member-severe-active`	Cluster member severe problem	Cluster member suffers from a severe problem that prevents it from handling traffic (even when the other cluster member is down)	*Disabled*	N/A	N/A	N/A	4	1	30	1.3.6.1.4.1.2620.1.2000.6.2

Trap Name in Gaia Clish	Monitored Object	Description	Default Trap State	Threshold Operand	Threshold Default Value	Threshold Valid Values	Trap Default Severity	Trap Default Repetitions	Default Repetition Delay	Trap SNMP OID
`cluster-member-state`	Cluster member state	Cluster member is either in the "Active Attention" state, or in the Blocking state (the cluster member identifier is provided in the trap)	*Disabled*	N/A	N/A	N/A	4	1	30	1.3.6.1.4.1.2620.1.2000.6.3

Trap Name in Gaia Clish	Monitored Object	Description	Default Trap State	Threshold Operand	Threshold Default Value	Threshold Valid Values	Trap Default Severity	Trap Default Repetitions	Default Repetition Delay	Trap SNMP OID
`cluster-member-device-status-problem`	Cluster device status	One of the Critical Devices on the cluster member (for example, "Synchronization") reported its state as "problem"	*Disabled*	N/A	N/A	N/A	4	1	30	1.3.6.1.4.1.2620.1.2000.6.4
`cluster-interface-problem`	Cluster interface problem	Cluster member detected a problem with one of the cluster interfaces (the interface name is provided in the trap)	*Disabled*	N/A	N/A	N/A	4	1	30	1.3.6.1.4.1.2620.1.2000.6.5

Trap Name in Gaia Clish	Monitored Object	Description	Default Trap State	Threshold Operand	Threshold Default Value	Threshold Valid Values	Trap Default Severity	Trap Default Repetitions	Default Repetition Delay	Trap SNMP OID
`connection-with-log-server-error`	Connection with log server error	Unable to send logs to the configured Log Server	Enabled	N/A	N/A	N/A	4	1	30	1.3.6.1.4.1.2620.1.2000.7.2
`vpn-tunnels-down`	VPN tunnels are down	VPN tunnels are down (names of VPN peer are provided in the trap)	*Disabled*	N/A	N/A	N/A	4	0	300	1.3.6.1.4.1.2620.1.2000.8.1
`temperature-sensor`	Temperature Sensor Status	Temperature is above the threshold required by vendor	Enabled	N/A	N/A	N/A	4	1	30	1.3.6.1.4.1.2620.1.2000.5.1.1

Trap Name in Gaia Clish	Monitored Object	Description	Default Trap State	Threshold Operand	Threshold Default Value	Threshold Valid Values	Trap Default Severity	Trap Default Repetitions	Default Repetition Delay	Trap SNMP OID
fan-speed	Fan Speed Status	Fan speed is above or below the threshold required by vendor	Enabled	N/A	N/A	N/A	4	1	30	1.3.6.1.4.1.2620.1.2000.5.2.1
voltage-sensor	Voltage Sensor Status	Voltage is above or below the threshold required by vendor	Enabled	N/A	N/A	N/A	4	1	30	1.3.6.1.4.1.2620.1.2000.5.3.1
power-supply	Power Supply Status	Power supply status changed	Enabled	N/A	N/A	N/A	4	1	30	1.3.6.1.4.1.2620.1.2000.5.4.1

Example Command

```
set snmp traps trap-name high-memory-utilization enable on
severity 1 repetitions 3 repetitions-delay 2 threshold 70
```

set snmp traps receiver

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing SNMP trap receiver.

See:

- *"add snmp traps-receiver" on page 494*
- *"show snmp traps receivers" on page 529*

Syntax

```
set snmp traps receiver <receiver>
      version v2 [ community <community> ]
      version v3 [ user <user> ]
```

Parameters

Parameter	Description
community	Configures the SNMP v2 community name for the trap receiver. A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ '@' (at)
receiver	Specifies the SNMP trap receiver. Press the TAB key to see the available options.
user	Specifies the SNMP v3 user. Press the TAB key to see the available options.
version	Specifies the SNMP version.

Example Command

```
set snmp traps receiver 192.168.1.1 version v2 community
MySnmpCommunity
```

set snmp user

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing SNMP v3 user.

See:

- *"add snmp user" on page 492*
- *"show snmp user" on page 534*
- *"show snmp users" on page 535*
- *"delete snmp user" on page 520*
- *"delete snmp users all" on page 521*

Syntax

```
set snmp user <user-name> security-level
      authPriv [ auth-pass-type <auth-pass-type> ] [ auth-pass-
phrase <auth-pass-phrase> ] [ privacy-pass-type <privacy-pass-
type> ] [ privacy-pass-phrase <privacy-pass-phrase> ]
      authNoPriv [ auth-pass-type <auth-pass-type> ] [ auth-pass-
phrase <auth-pass-phrase> ]
```

Parameters

Parameter	Description
auth-pass-phrase	Configures the authentication password for the SNMP v3 user. A string that contains alphanumeric and special characters.
auth-pass-type	Configures the authentication protocol type for the SNMP v3: ■ `SHA512` ■ `SHA256` ■ `SHA1` ■ `MD5`
privacy-pass-phrase	Configures the privacy authentication password for the SNMP v3 user. A string that contains alphanumeric and special characters.

Parameter	Description
privacy-pass-type	Configures the privacy protocol for the SNMP v3 user: ■ `AES256` ■ `AES` ■ `DES`
security-level	Controls whether to configure (`authPriv`) or not (`authNoPriv`) the privacy protocol for this SNMP v3 user.
user-name	Specifies the SNMP v3 user name. Press the TAB key to see the available options.

Example Command

```
set snmp user SnmpUser security-level authNoPriv auth-pass-type
SHA512 auth-pass-phrase 12345689
```

delete snmp contact

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes a configured SNMP contact.

Syntax

```
delete snmp contact
```

delete snmp location

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes a configured SNMP location.

Syntax

```
delete snmp location
```

delete snmp traps-receiver

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing SNMP trap receiver by IP address.

See:

- *"add snmp traps-receiver" on page 494*
- *"set snmp traps receiver" on page 512*
- *"delete snmp traps-receivers all" on page 519*

Syntax

```
delete snmp traps-receiver <traps-receiver>
```

Parameters

Parameter	Description
traps-receiver	Specifies the trap receiver's IP address.

Example Command

```
delete snmp traps-receiver 192.168.1.1
```

delete snmp traps-receivers all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all configured SNMP trap receivers.

See:

- *"add snmp traps-receiver" on page 494*
- *"set snmp traps receiver" on page 512*
- *"delete snmp traps-receiver" on page 518*

Syntax

```
delete snmp traps-receivers all
```

delete snmp user

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes a configured SNMP v3 user by name.

See:

- *"delete snmp users all" on page 521*
- *"show snmp user" on page 534*
- *"show snmp users" on page 535*
- *"add snmp user" on page 492*
- *"set snmp user" on page 514*

Syntax

```
delete snmp user <user-name>
```

Parameters

Parameter	Description
user-name	Specifies the SNMP v3 user name. Press the TAB key to see the available options.

Example Command

```
delete snmp user SnmpUser
```

delete snmp users all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all configured SNMP v3 users.

See:

- *"delete snmp user" on page 520*
- *"show snmp user" on page 534*
- *"show snmp users" on page 535*
- *"add snmp user" on page 492*
- *"set snmp user" on page 514*

Syntax

```
delete snmp users all
```

show snmp agent

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows whether the SNMP Agent is enabled.

See:

- *"set snmp agent" on page 495*
- *"show snmp-general-all" on page 527*

Syntax

```
show snmp agent
```

Example Output

```
HostName> show snmp agent
agent:                          true

HostName>
```

show snmp agent-version

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows whether SNMPv3 agent version is enabled (`true`) or not (`false`).

See:

- *"set snmp agent-version" on page 496*
- *"show snmp-general-all" on page 527*

Syntax

```
show snmp agent-version
```

Example Output

```
HostName> show snmp agent-version
agent-version:                true

HostName>
```

show snmp community

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the SNMP community name (the default is "`public`").

See:

- *"set snmp community" on page 497*
- *"show snmp-general-all" on page 527*

Syntax

```
show snmp community
```

Example Output

```
HostName> show snmp community
community:                    public

HostName>
```

show snmp contact

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the SNMP contact.

See:

- *"set snmp contact" on page 498*
- *"show snmp-general-all" on page 527*

Syntax

```
show snmp contact
```

Example Output

```
HostName> show snmp contact
contact:                        MyUser

HostName>
```

show snmp location

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the SNMP location.

See:

- *"set snmp location" on page 499*
- *"show snmp-general-all" on page 527*

Syntax

```
show snmp location
```

Example Output

```
HostName> show snmp location
location:                       MyLocation

HostName>
```

show snmp-general-all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the SNMP configuration.

See:

- *"show snmp agent" on page 522*
- *"show snmp agent-version" on page 523*
- *"show snmp community" on page 524*
- *"show snmp contact" on page 525*
- *"show snmp location" on page 526*
- *"show snmp traps status" on page 528*

Syntax

```
show snmp-general-all
```

Example Output

```
HostName> show snmp-general-all
agent:                          true
agent-version:                  v3-only
community:                      public
traps:                          disable
contact:                        MyContact
location:                       MyLocation

HostName>
```

show snmp traps status

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows SNMP traps status.

See *"set snmp traps enable/disable" on page 500*.

Syntax

```
show snmp traps status
```

Example Output

```
HostName> show snmp traps status
traps:                          true

HostName>
```

show snmp traps receivers

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows all configured SNMP trap receivers.

See:

- *"add snmp traps-receiver" on page 494*
- *"set snmp traps receiver" on page 512*
- *"delete snmp traps-receiver" on page 518*
- *"delete snmp traps-receivers all" on page 519*

Syntax

```
show snmp traps receivers
```

Example Output

```
HostName> show snmp traps receivers
traps-receiver   version   community   user
192.168.2.4      v2        public
HostName>
```

show snmp traps enabled-traps

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the supported SNMP traps and their configuration.

See *"show snmp traps enabled-traps" above*.

Syntax

```
show snmp traps enabled-traps
```

Example Output

```
HostName> show snmp traps enabled-traps
trap-name                         monitored-obj   threshold-operand
 threshold   severity   repetitions   repetitions-delay   trap-oid
                       trap-desc

interface-disconnected            Interface l...
             4          1               30
1.3.6.1.4.1.2620.1.2000.1.1      Either network cable was
disconnected, ICMP mon...
VLAN removed                      VLAN removal
             4          1               30
1.3.6.1.4.1.2620.1.2000.1.2      VLAN was removed from interface

high-memory-utilization           emory utili...  gt
 90          4          1               30
1.3.6.1.4.1.2620.1.2000.4.2      Memory utilization exceeded the
threshold value
low-disk-space                    Free disk s...  eq-lt
 10          4          1               30
1.3.6.1.4.1.2620.1.2000.2.1      Disk partition free space went
below the thresh...
high-connections-rate             Connection ...  eq-gt
 3000        4          1               30
1.3.6.1.4.1.2620.1.2000.1.3      New connection rate exceeded the
threshold value
high-concurrent-connections       Concurrent ...  eq-gt
 50000       4          1               30
1.3.6.1.4.1.2620.1.2000.1.4      The number of concurrent
connections exceeded t...
high-firewall-throughput          Firewall th...  eq-gt
 1000        4          1               30
1.3.6.1.4.1.2620.1.2000.1.5      Firewall throughput exceeded the
threshold value
high-accepted-packet-rate         Accepted pa...  eq-gt
 100000      4          1               30
1.3.6.1.4.1.2620.1.2000.1.6      Accepted packet rate exceeded the
threshold value
connection-with-log-server-...    Connection ...
             4          1               30
1.3.6.1.4.1.2620.1.2000.7.2      Unable to send logs to log server


             4          1               30
1.3.6.1.4.1.2620.1.2000.5.1.1
```

```
               4           1               30
1.3.6.1.4.1.2620.1.2000.5.2.1


               4           1               30
1.3.6.1.4.1.2620.1.2000.5.3.1


               4           1               30
1.3.6.1.4.1.2620.1.2000.5.4.1

HostName>
```

show snmp user

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of an SNMP v3 user.

See:

- *"show snmp users" on page 535*
- *"add snmp user" on page 492*
- *"set snmp user" on page 514*
- *"delete snmp user" on page 520*
- *"delete snmp users all" on page 521*

Syntax

```
show snmp user <user-name>
```

Parameters

Parameter	Description
user-name	Specifies the SNMP v3 user name. Press the TAB key to see the available options.

Example Output

```
HostName> show snmp user SnmpUser
user-name:                      SnmpUser
auth-pass-type:                 SHA512
is-priv:                        false
privacy-pass-type:              AES

HostName>
```

show snmp users

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of all SNMP v3 users.

See:

- *"add snmp user" on page 492*
- *"set snmp user" on page 514*
- *"delete snmp user" on page 520*
- *"delete snmp users all" on page 521*

Syntax

```
show snmp users
```

Example Output

```
HostName> show snmp users
user-name    auth-pass-type    is-priv    privacy-pass-type
SnmpUser     SHA512            false      AES
HostName>
```

Configuring Smart Accel Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Smart Accel settings.

Note - These settings apply only to Locally Managed Appliances.

set fast-accel untrusted-wireless-networks

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

You can bypass the Security Gatewayinspection for these:

- Wireless guest networks (guest networks are defined as untrusted networks which cannot access the local network).
- Existing interfaces (for example, LAN1, LAN2, DMZ).
- IP Address ranges

The feature uses the fast acceleration mechanism to mark the traffic to bypass the security policy.

See also:

- *"set fast-accel add/remove object" on the next page*
- *"show fast-accel" on page 538*

Syntax

```
set fast-accel untrusted-wireless-networks <true | false>
```

Example Command

To bypass the security policy for traffic from and to untrusted wireless networks (this is the default).

```
set fast-accel untrusted-wireless-networks true
```

To apply the security policy to traffic from and to untrusted wireless networks (disable the bypass).

```
set fast-accel untrusted-wireless-networks false
```

set fast-accel add/remove object

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

The administrator can accelerate traffic for specific networks (for example, guest networks or gaming networks) where speed and connectivity are more important than security.

Use this command to enable or disable the security policy bypass for an existing interface (applies to traffic from and to the network behind the specified interface).

See also:

- *"set fast-accel untrusted-wireless-networks" on the previous page*
- *"show fast-accel" on the next page*

Syntax

```
set fast-accel { add | remove }object <Name of Interface / Network
Object>
```

Example Command

```
set fast-accel add object [Press the TAB key to see the available
options.]
DMZ
LAN2
LAN3
LAN4
LAN1
```

show fast-accel

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows the wireless guest networks, interfaces, and IP ranges that are configured to bypass the security policy.

See also:

- *"set fast-accel untrusted-wireless-networks" on page 536*
- *"set fast-accel add/remove object" on the previous page*

Syntax

```
show fast-accel
```

Example Output

```
show fast-accel
untrusted-wireless-networks:  true
fastAccelObjects:             LAN1
```

add smart-accel-services name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add service to the selected Smart Accel services.

See:

- *"delete smart-accel-services name" on page 547*
- *"show smart-accel-services" on page 543*
- *"show services-to-smart-accel" on page 545*

Syntax

```
add smart-accel-services name <service-name>
```

Parameters

Parameter	Description
name	Service name

Example Command

```
add smart-accel-services name YouTube\ -\ Smart\ Accel
```

add smart-accel-assets asset-type

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Add assets for Smart Accel for this device.

See:

- *"set smart-accel-assets assets-mode" on page 542*
- *"delete smart-accel-assets asset-type" on page 548*
- *"show smart-accel-assets" on page 545*

Syntax

```
add smart-accel-assets asset-type <Device>
```

Parameters

Parameter	Description
device	Press the TAB key to see the available options. You can only add one device at a time.

Example Command

```
add smart-accel-assets asset-type alarm
```

set accel-settings enabled

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Allows you to turn Smart Accel settings on or off.

See *"show accel-setting" on page 543*.

Syntax

```
set accel-settings enabled { true | false }
```

Parameters

Parameter	Description
accel-settings	■ `true` - Enables the feature. ■ `false` - Disables the feature.

Example Command

```
set accel-settings enabled true
```

set smart-accel-services mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Turn on the Smart Accel.

See also:

- *"add smart-accel-services name" on page 538*
- *"delete smart-accel-services name" on page 547*
- *"show smart-accel-services" on page 543*
- *"show services-to-smart-accel" on page 545*

Syntax

```
set smart-accel-services mode { on | off}
```

Parameters

Parameter	Description
mode	Valid values: ■ on ■ off (default)

Example Command

```
set smart-accel-services mode on
```

set smart-accel-assets assets-mode

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Allows you to turn Smart Accel assets on or off.

See:

- *"add smart-accel-assets asset-type" on page 539*
- *"delete smart-accel-assets asset-type" on page 548*
- *"show smart-accel-assets" on page 545*

Syntax

```
set smart-accel-assets assets-mode { true | false }
```

Parameters

Parameter	Description
assets-mode	■ `true` - Smart Accel turned on for assets. ■ `false` - Smart Accel turned off for assets.

Example Command

```
set smart-accel-assets assets-mode false
```

show accel-setting

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Show if the feature is enabled.

See *"set accel-settings enabled" on page 540*.

Syntax

```
show accel-setting
```

Example Command

```
HostName> show accel-setting
enabled:........false
```

show smart-accel-services

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the Smart Accel services settings.

See:

- *"add smart-accel-services name" on page 538*
- *"set smart-accel-services mode" on page 540*
- *"delete smart-accel-services name" on page 547*
- *"show services-to-smart-accel" on page 545*

Syntax

```
show smart-accel-services
```

Parameters

Parameter	Description
n/a	

Example Command

```
show smart-accel-services
```

Example Output

```
mode:                          true
selected-services:             5
```

show smart-accel-assets

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Shows if Smart Accel is turned on for assets and also displays the number of total assets.

See:

- *"add smart-accel-assets asset-type" on page 539*
- *"set smart-accel-assets assets-mode" on page 542*
- *"delete smart-accel-assets asset-type" on page 548*

Syntax

```
show smart-accel-assets
```

Example Command

```
HostName> show smart-accel-assets
assets-mode:.............false
selected-assets:........101
```

show services-to-smart-accel

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the selected Smart Accel services.

See:

- *"add smart-accel-services name" on page 538*
- *"set smart-accel-services mode" on page 540*
- *"delete smart-accel-services name" on page 547*
- *"show smart-accel-services" on page 543*

Syntax

```
show services-to-smart-accel
```

Parameters

Parameter	Description
n/a	

Example Command

```
show services-to-smart-accel
```

Example Output

```
is-accelerated:                 true
uid:                            CP_HIGHBW_Facebook_Smart_Accel
category:                       table: 0xf6ca8cb0
name:                           Facebook - Smart Accel
category-name:                  highbw
parent-uid:                     CP_HIGHBW_Social_Media_services_Smart_
Accel
is-accelerated:                 true
uid:                            CP_HIGHBW_TikTok_Smart_Accel
category:                       table: 0xf6cac760
name:                           TikTok - Smart Accel
category-name:                  highbw
parent-uid:                     CP_HIGHBW_Social_Media_services_Smart_
Accel
```

delete smart-accel-services name

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Delete a service from the selected Smart Accel services.

See:

- *"add smart-accel-services name" on page 538*
- *"set smart-accel-services mode" on page 540*
- *"show smart-accel-services" on page 543*
- *"show services-to-smart-accel" on page 545*

Syntax

```
delete smart-accel-services name <service-name>
```

Parameters

Parameter	Description
name	Service name

Example Command

```
delete smart-accel-services name YouTube\ -\ Smart\ Accel
```

delete smart-accel-assets asset-type

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Delete assets for Smart Accel from this device.

See:

- *"add smart-accel-assets asset-type" on page 539*
- *"set smart-accel-assets assets-mode" on page 542*
- *"show smart-accel-assets" on page 545*

Syntax

```
delete smart-accel-assets asset-type <device>
```

Parameters

Parameter	Description
device	Press the TAB key to see the available options. You can delete all devices at the same time, or select an individual device to delete.

Example Command

```
delete smart-accel-assets asset-type computer
```

Configuring Static Routes

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure static routes.

add static-route

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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> ] [ rank
<rank> ]
```

Parameters

Parameter	Description
destination	IP address and subnet mask length of the destination of the packet in the format IP Address/Subnet. For example: 192.168.0.0/16 Default: 0.0.0.0/0 **Note** - The value "`0.0.0.0/0`" is supported starting from the R81.10.05 version.
metric	Specifies the route metric (integer).
rank	Specifies the rank for a static route. Supported starting from R81.10.10. ■ Only allowed on destination-based routes. ■ Rank is per destination, which means that all routes with the same destination even though their next hop and metric are different. ■ Default = 60. To change the default route rank, go to the WebUI > **Advanced Settings**.
service	Specifies the service name.
source	IP address and subnet mask length of the source of the packet in the format IP Address/Subnet. For example: 192.168.1.0/24

Example Command

```
add static-route source 172.15.47.0/24 service http destination
172.15.47.0/24 nexthop gateway logical My_Network metric 10
```

```
add static-route destination 0.0.0.0/0 nexthop gateway ipv4-
address 172.28.4.4
```

```
add static-route destination 7.7.7.0/24 nexthop gateway ipv4-
address 192.168.200.200 rank 40
```

add static-route service HTTP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

When the cluster virtual IPv4 address is in a different subnet than the IPv4 address of a physical interface, enable scope local to allow the cluster member to accept static routes on the subnet of the cluster virtual IPv4 address.

Syntax

```
add static-route service HTTP nexthop gateway monitored-ip <IP-address> {on | off} monitored-ip-option {fail-all | fail | any | off } logical <Name-of-Internet-Connection>
```

Parameters

Parameter	Description
monitored-ip	An IP address for monitoring. Up to three unique addresses can be added here (in separate commands). The address is followed by "on" or "off": "on" means this address is being added, while "off" removes it.
monitored-ip-option	The failure condition and flavor for the configured monitored IP address (es). The accepted options are fail-all, fail_any and off.

Example Command

```
add static-route service HTTP nexthop gateway monitored-ip 1.2.3.4 on monitored-ip-option fail-all logical Internet1
```

add static-route ... nexthop gateway monitored-ip

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add static route monitoring.

Notes:

- You can only add or set a default static route if the Advanced Setting "`allow-default-static-route`" is turned on.
- Probing static route can only be done on the default route.

Syntax

```
add static-route [ source ] [ service ] [ destination ] [ nexthop
gateway monitored-ip <Monitored IP Address> {on | off}
monitored-ip-option {fail-all | fail-any | off} { logical | ipv4-
address } ] [ metric ]
```

Parameters

Parameter	Description
destination	IP address and subnet mask length of the destination of the packet in the format IP Address/Subnet. For example: 192.168.0.0/16 Default: 0.0.0.0/0 **Note** - The value "`0.0.0.0/0`" is supported starting from the R81.10.05 version.
metric	Specifies the route metric (integer).
service	Specifies the service name.
source	IP address and subnet mask length of the source of the packet in the format IP Address/Subnet. For example: 192.168.1.0/24

Parameter	Description
monitored-ip	Remote server to monitor for the next hop gateway. **Note** - This is deprecated starting from R81.10.07. You can a maximum of three unique servers (in separate commands). The IPv4 address is followed by "`on`" or "`off`": ■ `on` - Adds this address ■ `off` - Removes this address
monitored-ip-option	**Note** - This is deprecated starting from R81.10.07. Sets the failure condition for the configured monitored servers. Options: ■ `fail-all` - - If all the checked servers fail, the probing fails. Fails the next hop gateway when all monitored IP addresses become unreachable. Restores the next hop. ■ `fail_any` - If only one of the servers fails, the probing fails. Fails the next hop gateway when one of the monitored IP addresses becomes unreachable. ■ `off` - Turns off the route probing.
monitored-server	**Note** - In R81.10.07 and higher only. IP Address or Hostname - Remote server to monitor for the next hop gateway
monitoring-mode	**Note** - In R81.10.07 and higher only. Enables route monitoring. Options: ■ `on` ■ `off`

Example Commands

R81.10.07 and higher

```
add static-route destination 0.0.0.0/0 nexthop gateway ipv4-address 172.28.4.4 monitoring-mode on monitored-server 172.28.4.4 on metric
101
```

R81.10.05 and lower

```
add static-route service http nexthop gateway monitored-ip
172.15.47.0 on monitored-ip-option fail-all logical internet
```

```
add static-route destination 0.0.0.0/0 nexthop gateway ipv4-address 172.28.4.4
```

set static-route

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing manually configured route rule.

Note - Probing static route can only be done on the default route.

Syntax

```
set static-route <id> [ source <source> ] [ service <service> ] [
destination <destination> ] [ nexthop gateway { logical <logical>
| ipv4-address <ipv4-address> | gateway-vti <gateway-vti> |
gateway-interface <gateway-interface> } ] [ metric <metric> ] [
disabled <disabled> ]
```

Parameters

Parameter	Description
destination	IP address and subnet mask length of the destination of the packet in the format IP Address/Subnet. For example: 192.168.0.0/16 Default: 0.0.0.0/0 **Note** - The value "`0.0.0.0/0`" is supported starting from the R81.10.05 version.
disabled	Specifies whether this route is enabled (`disabled false`) or disabled (`disabled true`)
id	Specifies the route ID (an integer).
metric	Specifies the route metric (integer).
service	Specifies the service name.
source	IP address and subnet mask length of the source of the packet in the format IP Address/Subnet. For example: 192.168.1.0/24

Example Command

```
set static-route 15 source 172.15.47.0/24 service http destination
172.15.47.0/24 nexthop gateway logical My_Network metric 15
disabled true
```

```
add static-route destination 0.0.0.0/0 nexthop gateway ipv4-address 172.28.4.4 metric 102
```

delete static-route

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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" A number with no fractional part (integer)

Example Command

```
delete static-route 3
```

delete static-routes

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all manually defined static routing rules.

Syntax

```
delete static-routes
```

Parameters

Parameter	Description
n/a	

Example Command

```
delete static-routes
```

show static-routes

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows all static routes.

Syntax

```
show static-routes
```

Parameters

Parameter	Description
n/a	

Example Command

```
show static-routes
```

add static-route-ipv6

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add static route for an IPv6 connection.

Syntax

```
add static-route-ipv6 [ ipv6-destination <ipv6-destination> ] [
nexthop gateway { logical <logical> | ipv6-address <ipv6-address>
} ] [ priority <priority> ]
```

Parameters

Parameter	Description
ipv6-destination	IPv6 address of the destination network and IPv6 prefix length
priority	Priority Define which default gateway to select as the nexthop when multiple default gateways are configured. The lower the configured priority, the higher the preference. When multiple default gateways are configured with the same priority, the one with the lower IP address is selected (for example, 2001:db8:3333:4444:5555:6666:7777:0011 instead of 2001:db8:3333:4444:5555:6666:7777:0022).

Example Command

```
add static-route-ipv6 ipv6-destination
2001:0db8:3333:4444:5555:6666:0000:0000/96 nexthop gateway logical
My_Network priority 2001:db8:3333:4444:5555:6666:0000:0001
```

set static-route-ipv6

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure static route for an IPv6 connection.

Syntax

```
set static-route-ipv6 <ID> [ ipv6-destination <ipv6-destination> ]
[ nexthop gateway { logical <name-of-local-interface> | ipv6-
address <ipv6-address> } ] [ priority <priority> ] [ disabled
{true | false}
```

Parameters

Parameter	Description
disabled	Enables (`true`) or disables (`false`) the route
id	Route ID
ipv6-destination	IPv6 address of the destination network and IPv6 prefix length
priority	Priority Define which default gateway to select as the nexthop when multiple default gateways are configured. The lower the configured priority, the higher the preference. When multiple default gateways are configured with the same priority, the one with the lower IP address is selected (for example, 2001:db8:3333:4444:5555:6666:7777:0011 instead of 2001:db8:3333:4444:5555:6666:7777:0022).
logical	Name of the local interface with IPv6 address configured, through which the traffic must exit

Example Command

```
set static-route-ipv6 2001:0db8:3333:4444:5555:6666:0000:0000/96
ipv6-destination 2001:0db8:3333:4444:5555:6666:0000:0000/96
nexthop gateway logical My_Network priority
2001:0db8:3333:4444:5555:6666:0000:0001 disabled true
```

delete static-route-ipv6

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete static route for an IPv6 connection.

Syntax

```
delete static-route-ipv6 <id>
```

Parameters

Parameter	Description
id	Route ID Press the TAB key to see the available options.

Example Command

```
delete static-route-ipv6 2
```

show router-configuration

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows dynamic routing configuration.

Syntax

```
show router-configuration <category>
```

Press the TAB key to see the available options.

Category	Description
aggregate	Shows the Route Aggregation configuration.
as	Shows the Autonomous System configuration.
bgp	Shows the BGP configuration.
igmp	Shows the IGMP configuration.
kernel-routes	Shows the configuration for kernel routes.
max-path-splits	Shows the configuration for path splits.
ospf	Shows the OSPF configuration.
pim	Shows the PIM configuration.
protocol-rank	Shows the protocol rank configuration.
rip	Shows the RIP configuration.
route-redistribution	Shows the Route Redistribution configuration.
routemap	Shows the configuration for a specific Route Map.
routemaps	Shows the configuration for all Route Maps.
router-id	Shows the Router ID configuration.
router-options	Shows the configuration for Router Options.
static-mroute	Shows the configuration for static multicast route.
static-route	Shows the static routes (takes time to show the result).
trace	Shows the Trace configuration.
tracefile	Shows the Tracefile configuration.

Example 1

```
Gaia> show router-configuation bgp
set bgp internal on
set bgp internal local-address 192.168.200.1 on
set bgp internal protocol all on
set bgp internal interface all on
```

Example 2

```
Gaia> show router-configuration
# Aggregate
# As
set as 5
# BGP
set bgp internal on
set bgp internal local-address 192.168.200.1 on
set bgp internal protocol all on
set bgp internal interface all on
#IGMP
# Kernel Routes
# max-path-splits
set max-path-splits 8
# OSPF
set ospf instance default area backbone on
# PIM
# Protocol Rank
# RIP
set rip update-interval default gateway set rip expire-interval
default
... ... (truncated for brevity) ... ...
```

Configuring Static Route Probing

In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

The commands in this section enable you to set and probe a default static route that uses an internal LAN while there is also a default gateway on WAN.

If there is a route probing fail, there is a failover between LAN and WAN on certain conditions.

add static-route destination

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Configure and probe a default static route that uses an internal LAN while there is also a default gateway on WAN.

Note - Advanced Probing Settings exist only in the WebUI.

See *"set static route destination" on page 568*.

Syntax

```
add static-route destination 0.0.0.0/0 nexthop gateway ipv4-
address <IPv4 Address> monitored-ip-options { fail-any | fail-all
| off }
```

Parameters

Parameter	Description
ipv4-address	The IPv4 address of the internal LAN.
monitored-ip-options	**Note** - This is deprecated in R81.10.07 and higher. Specifies the monitoring options: ■ `fail-any` - If one host fails, the entire probing fails. ■ `fail-all` - All the hosts (maximum of 3) must fail for the probing to fail. ■ `off` - Stops the route probing completely.
monitored-server	**Note** - In R81.10.07 and higher only. IP Address or Hostname - Remote server to monitor for the next hop gateway
monitoring-mode	**Note** - In R81.10.07 and higher only. Enables route monitoring. Options: ■ `on` ■ `off`

Example Command

In R81.10.05 and lower

```
add static-route destination 0.0.0.0/0 nexthop gateway ipv4-
address 192.168.22.33 monitored-ip-options fail-all
```

In R81.10.07 and higher

```
add static-route destination 0.0.0.0/0 nexthop gateway ipv4-address 172.28.4.4 monitoring-mode on monitored-server 8.8.8.8 on metric 101
```

set static route destination

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Configure the hosts you want to probe to the route.

You can add up to 3 hosts with this command.

See *"add static-route destination" on page 566*

Syntax

```
set static route <Route ID> destination 0.0.0.0/0 nexthop gateway
ipv4-address <IPv4 Address> monitored-ip <IPv4 Address> {on | off}
```

Parameters

Parameter	Description
route	The ID of the configured default static route.
ipv4-address	The IPv4 address of the configured LAN.
monitored-ip	The IPv4 address of the site you probe to check if you can reach it through the configured route. ■ `on` - Enables the configuration ■ `off` - Disables the configuration

Example Command

```
set static route 1234 destination 0.0.0.0/0 nexthop gateway ipv4-
address 1.1.1.1 monitored-ip 2.2.2.2 on
```

show route-probe-stats

In the R81.10.X releases, this command is available starting from the R81.10.07 version.

Description

Display all the statistics for each of the configured static route and for each of the servers of the route from the past 24 hours.

Syntax

```
show route-probe-stats
```

Example Output

```
Route 1 to any from any via 192.168.1.226:
Server: dns.google.com:
time    avg[ms] min[ms] max[ms] packet loss[%]
13:00      4.05       3      23    0.00
14:00      4.22       3      73    0.00
15:00      4.60       3      82    0.00
Server: dns.cloudflare.com:
time    avg[ms] min[ms] max[ms] packet loss[%]
13:00      4.03       2      70    0.00
14:00      3.85       3      76    0.00
15:00      3.84       2      61    0.00
Server: dns.opendns.com:
time    avg[ms] min[ms] max[ms] packet loss[%]
13:00     54.35      53      91    0.08
14:00     54.44      53     102    0.00
15:00     54.44      53      98    0.00
```

Configuring MAC Filtering Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the MAC filtering settings.

set mac-filtering-settings state

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the settings for MAC filtering.

Syntax

```
set mac-filtering-settings state {on | off}
```

Example Command

```
set mac-filtering-settings state on
```

set mac-filtering settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the settings for MAC filtering.

Syntax

```
set mac-filtering-settings advanced-settings log-activation <log-activation>
```

Parameters

Parameter	Description
n/a	

Example Command

```
set mac-filtering-settings advanced-settings log-activation on
```

set mac-filtering settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the settings for MAC filtering.

Syntax

```
set mac-filtering-settings advanced-settings log-interval 0-90
```

Parameters

Parameter	Description
log-interval	Indicates the suspension time (from 0 to 90 seconds) between logs for blocked MAC addresses

Example Command

```
set mac-filtering-settings advanced-settings log-interval 60
```

set mac-filtering-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Turn on/off blocklist mode for MAC filtering

Syntax

```
set mac-filtering-settings state <state> [ blocklist [on|off ]
```

Parameters

Parameter	Description
blocklist	Blocklist mode Options: on, off

Parameter	Description
state	MAC Filtering state Options: on, off

Example Command

```
set mac-filtering-settings state on blocklist on
```

show mac-filtering-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the settings for MAC filtering.

Syntax

```
show mac-filtering-settings
```

Parameters

Parameter	Description
n/a	

Example Command

```
show mac-filtering-settings
```

show mac-filtering-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the advanced settings for MAC filtering.

Syntax

```
show mac-filtering-settings advanced-settings
```

Parameters

Parameter	Description
n/a	

Example Command

```
show mac-filtering-settings advanced-settings
```

add mac-filtering-list

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
add mac-filtering-list mac 00:1C:7F:21:05:BE
```

delete mac-filtering-list

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
delete mac-filtering-list mac 00:1C:7F:21:05:BE
```

show mac-filtering-list

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the MAC addresses that are allowed to access LAN/DMZ networks.

Syntax

```
show mac-filtering-list
```

Parameters

Parameter	Description
n/a	

Example Command

```
show mac-filtering-list
```

Configuring Notification Policy

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the notification policy.

set notifications-policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the policy for sending notifications to the user.

Syntax

```
set notifications-policy [ send-push-notifications {true | false}
] [ send-detailed-push-notifications {true | false} ] [ send-
cloud-notifications {true | false} ]
```

Parameters

Parameter	Description
send-detailed-push-notifications	Sending of detailed notifications to the mobile application. Notification previews may contain information about your network. Turning off this feature means that the security gateway removes this information from the push notification.
send-push-notifications	Sending of notifications to the mobile application.
send-cloud-notifications	Sending of notifications to the cloud.

Example Command

```
set notifications-policy send-push-notifications true send-
detailed-push-notifications true set notifications-policy send-
cloud-notifications true
```

set notifications-policy advanced-settings limit-notifications

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the policy for sending notifications to the user.

Syntax

```
set notifications-policy advanced-settings limit-notifications 0-
3600
```

Parameters

Parameter	Description
limit-notifications	The maximal number of notifications to send (between 0 and 3600)

Example Command

```
set notifications-policy advanced-settings limit-notifications 10
```

set notifications-policy advanced-settings send-push-notifications

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the policy for sending notifications to the user.

Syntax

```
set notifications-policy advanced-settings send-push-notifications
{true | false}
```

Example Command

```
set notifications-policy advanced-settings send-push-notifications
true
```

show notifications-policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the policy for sending notifications to the user.

Syntax

```
show notifications-policy
```

Example Command

```
show notifications-policy
```

show notifications-policy advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the policy for sending notifications to the user.

Syntax

```
show notifications-policy advanced-settings
```

Example Command

```
show notifications-policy advanced settings
```

show notifications-log

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the notification logs.

Syntax

```
show notifications-log
```

Example Command

```
show notifications-log
```

Configuring Privacy Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure privacy settings.

set privacy-settings advanced-settings customer-consent

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

In Advanced Settings, select if the customer consents to sending diagnostic data to Check Point.

Syntax

```
set privacy-settings advanced-settings customer-consent {true |
false}
```

Example Command

```
set privacy-settings advanced-settings customer-consent true
```

set privacy-settings advanced-settings proactive-device-details

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enable or disable proactive querying (in the Locally Managed mode) sent to devices that are connected to the local network to collect device details to show on the **Active Devices** page in WebUI.

Syntax

```
set privacy-settings advanced-settings proactive-device-details
{true | false}
```

Parameters

Parameter	Description
n/a	

Example Command

```
set privacy-settings advanced-settings proactive-device-details
false
```

show privacy-settings advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

In Advanced Settings, show if the customer consents to sending diagnostic data.

Syntax

```
show privacy-settings advanced-settings
```

Example Command

```
show privacy-settings advanced-settings
```

Sample Output

```
customer-consent: true
```

Configuring Report Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the local report settings.

set report-settings advanced-settings centrally-max-period

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure advanced local report settings when the appliance works in the Centrally Managed mode.

Syntax

```
set report-settings advanced-settings centrally-max-period
<centrally-max-period>
```

Example Command

```
set report-settings advanced-settings centrally-max-period 1h
```

set report-settings advanced-settings locally-max-period

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure advanced local report settings when the appliance works in the Locally Managed mode.

Syntax

```
set report-settings advanced-settings locally-max-period <locally-max-period>
```

Example Command

```
set report-settings advanced-settings locally-max-period 1h
```

show report-settings advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configured settings for report scheduling and creation.

Syntax

```
show report-settings advanced-settings
```

Example Command

```
show report-settings advanced-settings
```

Configuring NAT Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure NAT settings.

add nat-rule

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new manual NAT rule to hide a source or destination behind NAT.

Note - Updatable objects and FQDN can be used only as the original source/destination and cannot be translated.
Limitations: When an updatable object is used as the original source or destination, it cannot be translated. "Translated source/destination" = "Original| only.

There are no new parameters for FQDN as it is used as any other object.

Syntax

```
add nat-rule
      [ name <name> ]
      [ comment "<comment>" ]
      [ { position <position> | position-above <position-above> |
position-below <position-below> } ]
      [ original-source <original-source> ]
      [ original-destination <original-destination> ]
      [ original-service <original-service> ]
      [ translated-source <translated-source> ]
      [ translated-destination <translated-destination> ]
      [ translated-service <translated-service> ]
      [ enable-arp-proxy {true | false} ]
      [ hide-sources {true | false} ]
```

Parameters

Parameter	Description
comment	Configures the comment text. A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '`(`' (opening round bracket) ■ '`)`' (closing round bracket) ■ ':' (colon) ■ '`@`' (at)
enable-arp-proxy	Controls whether to enable (`true`) or disable (`false`) the ARP proxy. When enabled, the gateway replies to ARP Requests that are sent to the original destination's IP address. This does not apply to IP Range objects or Network objects.
hide-sources	Controls whether to hides (`true`) or not (`false`) multiple sources behind the translated source addresses.
name	Name of the rule. A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
original-destination	Specifies the original destination object. Press the TAB key to see the available options. To configure all addresses, select the value "`any`".

original-destination-updatable-object	Valid values: (see *"show updatable-objects" on page 915*)
	`name`
	`uuid`

original-service	Specifies the original service. Press the TAB key to see the available options. To configure all services, select the value "`any`".

Parameter	Description
original-source	Specifies the original source object. Press the TAB key to see the available options. To configure all addresses, select the value "`any`".

original-source-updatable object	Valid values: (see *"show updatable-objects" on page 915*)
	`name`
	`uuid`

position	Specifies the order of the rule (a decimal number) in comparison to other manual rules.
position-above	Specifies the relative order of the rule (a decimal number) in comparison to other manual rules.
position-below	Specifies the relative order of the rule (a decimal number) in comparison to other manual rules.
translated-destination	Specifies the translated destination object. Press the TAB key to see the available options. To use the original address, select the value "`original`".
translated-service	Specifies the translated service. Press the TAB key to see the available options. To use the original service, select the value "`original`".
translated-source	Specifies the translated source object. Press the TAB key to see the available options. To use the original address, select the value "`original`".

Example Command

The NAT rule as it appears in WebUI:

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Comment
Manual NAT Rules							
1	MyInternalNetwork	MyExternalNetwork	HTTP	MyHideNAT	* Original	* Original	Hide HTTP traffic from Internal to External

The required command:

```
add nat-rule name MyNatRule comment "Hide HTTP traffic from
Internal to External" original-source MyInternalNetwork original-
destination MyExternalNetwork original-service HTTP translated-
source MyHideNAT translated-destination original translated-
service original hide-sources true enable-arp-proxy true position
2
```

Example with updatable object:

```
add nat-rule original-destination-updatable-object name Tuvalu
original-service HTTP translated-service HTTPS translated-
destination original original-source any
```

set nat advanced-settings address-trans

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings address-trans {true | false}
```

Parameters

Parameter	Description
n/a	

Example Command

```
set nat advanced-settings address-trans true
```

set nat advanced-settings arp-proxy-merge

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings arp-proxy-merge {true | false}
```

Parameters

Parameter	Description
n/a	

Example Command

```
set nat advanced-settings arp-proxy-merge true
```

set nat advanced-settings increase-hide-capacity

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings increase-hide-capacity <increase-hide-capacity>
```

Parameters

Parameter	Description
n/a	

Example Command

```
set nat advanced-settings increase-hide-capacity true
```

set nat advanced-settings ip-pool-nat

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
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
```

set nat advanced-settings nat-automatic-arp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings nat-automatic-arp {true | false}
```

Parameters

Parameter	Description
n/a	

Example Command

```
set nat advanced-settings nat-automatic-arp true
```

set nat advanced-settings nat-cache-expiration

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings nat-cache-expiration <nat-cache-expiration>
```

Parameters

Parameter	Description
n/a	

Example Command

```
set nat advanced-settings nat-cache-expiration 100
```

set nat advanced-settings nat-cache-num-entries

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set nat advanced-settings nat-cache-num-entries 100
```

set nat advanced-settings nat-destination-client-side

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings nat-destination-client-side {true |
false}
```

Parameters

Parameter	Description
n/a	

Example Command

```
set nat advanced-settings nat-destination-client-side true
```

set nat advanced-settings nat-destination-client-side-manual

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings nat-destination-client-side-manual {true
| false}
```

<nat-destination-client-side-manual>

Parameters

Parameter	Description
n/a	

Example Command

```
set nat advanced-settings nat-destination-client-side-manual true
```

set nat advanced-settings nat-hash-size

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings nat-hash-size <nat-hash-size>
```

Parameters

Parameter	Description
n/a	

Example Command

```
set nat advanced-settings nat-hash-size 1024
```

set nat advanced-settings nat-limit

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings nat-limit <nat-limit>
```

Parameters

Parameter	Description
n/a	

Example Command

```
set nat advanced-settings nat-limit 100
```

set nat advanced-settings perform-cluster-hide-fold

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced NAT policy settings.

Syntax

```
set nat advanced-settings perform-cluster-hide-fold {true | false}
```

Parameters

Parameter	Description
n/a	

Example Command

```
set nat advanced-settings perform-cluster-hide-fold true
```

set nat hide-internal-networks

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures if local networks will be hidden by default behind the external IP addresses of the gateway.

Syntax

```
set nat [ hide-internal-networks {true | false} ]
```

Parameters

Parameter	Description
hide-internal-networks	Hide internal networks behind the Gateway's external IP address

Example Command

```
set nat hide-internal-networks true
```

set nat-rule

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Configures the comment text for the manual NAT rule. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
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)

Parameter	Description
hide-sources	Hide multiple sources behind the translated source addresses Type: Boolean (true/false)
name	name A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
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
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 Command

```
set nat-rule name MyNatRule 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
disabled true
```

set nat-rule position

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Configures the comment text for the manual NAT rule. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
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)

Parameter	Description
hide-sources	Hide multiple sources behind the translated source addresses Type: Boolean (true/false)
name	name A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
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
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 Command

```
set nat-rule position 2 original-source TEXT original-destination
TEXT original-service TEXT translated-source TEXT translated-
destination TEXT translated-service TEXT name MyNatRule comment
"This is a comment" hide-sources true enable-arp-proxy true
position 2 disabled true
```

delete nat-rule

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes a manually configured NAT rule by name.

Syntax

```
delete nat-rule name <name>
```

Parameters

Parameter	Description
name	name A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)

Example Command

```
delete nat-rule name MyNatRule
```

delete nat-rule position

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
delete nat-rule position 2
```

show nat

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows NAT policy.

Syntax

```
show nat
```

Example Command

```
show nat
```

show nat-rule

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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>
```

Example Command

```
show nat-rule name MyNatRule
```

show nat-rules

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration of all manually and auto-generated NAT rules.

Syntax

```
show nat-rules
```

Parameters

Parameter	Description
n/a	

Example Command

```
show nat-rules position 2
```

show nat-manual-rules

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show nat-rule name MyNatRule
```

show nat advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced settings for NAT policy.

Syntax

```
show nat advanced-settings
```

Configuring IP Fragment Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure how the appliances handles IP fragment packets.

set ip-fragments-params advanced-settings config

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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> ]
```

Example Command

```
set ip-fragments-params advanced-settings config track none limit
150 advanced-state forbid timeout 15 pkt-cap true
```

set ip-fragments-params advanced-settings minsize

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures how the appliance handles IP fragments.

Syntax

```
set ip-fragments-params advanced-settings minsize <minsize>
```

Example Command

```
set ip-fragments-params advanced-settings minsize 150
```

show ip-fragments-params

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration of IP fragments handling.

Syntax

```
show ip-fragments-params advanced-settings
```

Parameters

Parameter	Description
n/a	

Example Command

```
show ip-fragments-params advanced-settings
```

Configuring IPv6 Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure IPv6 settings.

add internet-connection-ipv6 enable-nd-proxy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add a new IPv6 connection and enable the Neighbor Discovery proxy.

On some IPv6 networks, where prefix delegation is not supported, it is possible to use an alternative method for assigning globally-routable IPv6 addresses to internal (LAN) interfaces and hosts.

Prerequisites:

- Configure IPv6 on WAN or DMZ interface, with connection type: "**Obtain automatically (DHCPv6/SLAAC)**" (in Gaia Clish, "`auto-obtain`").
- Disable NAT and prefix delegation in case they are enabled.

Syntax

```
add internet-connection-ipv6 name <connection-name> interface-ipv6
{WAN | DMZ} type-ipv6 auto-obtain disable-nat {on | off} enable-
nd-proxy {on | off} nd-proxy-local-network <LAN-name>
```

Parameters

Parameter	Description
name	Configures the IPv6 connection name. A string that contains up to 64 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '@' (at)
disable-nat	Disables (`on`) or enables (`off`) NAT (Network Address Translation) for traffic going through this Internet connection. When you add a new connection, you must enter the value "`on`".
enable-nd-proxy	Enables (`on`) or disables (`off`) the neighbor discovery proxy for this Internet connection. When you add a new connection, you must enter the value "`on`".
interface-ipv6	Specifies the interface. You must select WAN or DMZ.
nd-proxy-local-network	Specifies the local IPv6 network name. You must select one of LAN interfaces.

Example Command

```
add internet-connection-ipv6 name myNet1 interface-ipv6 WAN type-
ipv6 auto-obtain disable-nat on enable-nd-proxy on nd-proxy-local-
network LAN3
```

set internet-connection-ipv6 enable-nd-proxy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the Neighbor Discover proxy settings for an existing IPv6 connection.

On some IPv6 networks, where prefix delegation is not supported, it is possible to use an alternative method for assigning globally-routable IPv6 addresses to internal (LAN) interfaces and hosts.

Syntax

```
set internet-connection-ipv6 <connection-name> interface-ipv6 {WAN
| DMZ} type-ipv6 auto-obtain disable-nat {on | off} enable-nd-
proxy {on | off} nd-proxy-local-network <LAN-name>
```

Parameters

Parameter	Description
disable-nat	Disables (`on`) or enables (`off`) NAT (Network Address Translation) for traffic going through this Internet connection. When you add a new connection, you must enter the value "`on`".
enable-nd-proxy	Enables (`on`) or disables (`off`) the neighbor discovery proxy for this Internet connection.
interface-ipv6	Specifies the interface. You must select WAN or DMZ.
internet-connection-ipv6	Specifies the connection name. Press the TAB key to see the available options.
nd-proxy-local-network	Specifies the local IPv6 network name. You must select one of LAN interfaces.

Example Command

```
set internet-connection-ipv6 myNet1 type-ipv6 auto-obtain enable-
nd-proxy on nd-proxy-local-network LAN3
```

set internet-connection probe-icmp6-servers

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the probing IPv6 addresses (or hostnames) to monitor an existing internet connection.

If there is no connectivity to these servers, the connection reports its status as failed.

In Web UI, this corresponds to:

1. Click the **Device** view > **Network** section > **Internet** page.
2. Click the **Configure monitoring** link.
3. Click **Save**.

See:

- *"show internet-connection icmp-servers" on page 635*
- *"set internet-connection probe-icmp6-servers" on the previous page*
- *"set internet-connection probe-servers" on page 357*
- *"set internet-connection probe-icmp-servers" on page 359*
- *"set internet-connection probing-method" on page 361*

Syntax

```
set internet-connection <Name>
      probe-icmp6-servers
            first-ipv6 <IPv6-Address>
            [ second-ipv6 <IPv6-Address> ]
            [ third-ipv6 <IPv6-Address> ]
```

Parameters

Parameter	Description
name	Name of the Internet connection. Press the TAB key to see the available options.
first-ipv6	First IPv6 address (or hostname) for the probing method (when using connection monitoring).
second-ipv6	Second IPv6 address (or hostname) for the probing method (when using connection monitoring).
third-ipv6	Third IPv6 address (or hostname) for the probing method (when using connection monitoring).

Example Command

```
set internet-connection "My connection" probe-icmp6-servers first-
ipv6 2001:4860:4860::8888 second-ipv6 dns.cloudflare.com third-
ipv6 dns.opendns.com
```

set ipv6-state

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enable the IPv6 mode of the appliance.

You must enable the IPv6 mode before you can configure IPv6 address, IPv6 routes, and IPv6 objects.

Warning - This command immediately reboots the appliance to apply the change.

See:

- *"set ipv6-state-networking-enabled" below*
- *"set ipv6-state-security-enabled" on the next page*
- *"show ipv6-state" on page 634*
- *"show ipv6-state-networking-enabled" on page 634*
- *"show ipv6-state-security-enabled" on page 635*

Syntax

```
set ipv6-state on
```

set ipv6-state-networking-enabled

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables and disable IPv6 enforcement for networking.

Warning - This command immediately reboots the appliance to apply the change.

See:

- *"set ipv6-state" above*
- *"set ipv6-state-security-enabled" on the next page*
- *"show ipv6-state" on page 634*

- *"show ipv6-state-networking-enabled" on page 634*
- *"show ipv6-state-security-enabled" on page 635*

Syntax

```
set ipv6-state-networking-enabled {on | off}
```

Example Command

```
set ipv6-state-networking-enabled on
```

set ipv6-state-security-enabled

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure IPv6 enforcement for security policy.

Warning - This command immediately reboots the appliance to apply the change.

See:

- *"set ipv6-state" on the previous page*
- *"set ipv6-state-networking-enabled" on the previous page*
- *"show ipv6-state" on page 634*
- *"show ipv6-state-networking-enabled" on page 634*
- *"show ipv6-state-security-enabled" on page 635*

Syntax

```
set ipv6-state-security-enabled { on | off
}
```

Example Command

```
set ipv6-state-security-enabled on
```

show ipv6-state

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the state of the IPv6 mode on the appliance.

See:

- *"set ipv6-state" on page 632*
- *"set ipv6-state-networking-enabled" on page 632*
- *"set ipv6-state-security-enabled" on page 633*
- *"show ipv6-state-networking-enabled" below*
- *"show ipv6-state-security-enabled" on the next page*

Syntax

```
show ipv6-state
```

Example Output

```
HostName> show ipv6-state
IPv6 is enabled
```

show ipv6-state-networking-enabled

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the state of the IPv6 enforcement for networking on the appliance.

See:

- *"set ipv6-state" on page 632*
- *"set ipv6-state-networking-enabled" on page 632*
- *"set ipv6-state-security-enabled" on page 633*
- *"show ipv6-state" above*
- *"show ipv6-state-security-enabled" on the next page*

Syntax

```
show ipv6-state-networking-enabled
```

Example Output

```
HostName> show ipv6-state-networking-enabled
IPv6 networking is enabled
```

show ipv6-state-security-enabled

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the state of the IPv6 enforcement for security policy on the appliance.

See:

- *"set ipv6-state" on page 632*
- *"set ipv6-state-networking-enabled" on page 632*
- *"set ipv6-state-security-enabled" on page 633*
- *"show ipv6-state" on the previous page*
- *"show ipv6-state-networking-enabled" on the previous page*

Syntax

```
show ipv6-state-security-enabled
```

Example Output

```
HostName> show ipv6-state-security-enabled
IPv6 security policy is enforced
```

show internet-connection icmp-servers

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configured IPv4 and IPv6 probing servers for health monitoring of defined internet connection.

If there is no connectivity to these servers, the connection reports its status as failed.

In Web UI, this corresponds to:

1. Click the **Device** view > **Network** section > **Internet** page.
2. Click the **Configure monitoring** link.
3. Click **Cancel**.

See:

- *"set internet-connection probe-icmp-servers" on page 359*
- *"set internet-connection probe-icmp6-servers" on page 629*

Syntax

```
show internet-connection <name> icmp-servers
```

Parameters

Parameter	Description
name	Specifies the connection name. Press the TAB key to see the available options.

Example Output

```
HostName> show internet-connection Internet2 icmp-servers
first: cloudflare.com
second: dns.opendns.com
third: dns.opendns.com
first-ipv6: 2001:4860:4860::8888
second-ipv6: dns.cloudflare.com
third-ipv6: dns.opendns.com
```

Configuring NetFlow Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

Introduction

NetFlow is an industry standard for traffic monitoring. Cisco developed this network protocol to collect network traffic patterns and volume.

One host (the *NetFlow Exporter*) sends information about its network flows to a different host (the *NetFlow Collector*).

A network flow is a unidirectional stream of packets that contain the same set of characteristics.

You can configure a Quantum Spark Appliance as an Exporter of NetFlow records for all the traffic that passes through it.

The NetFlow Collector is a different external server, and you configure it separately.

NetFlow Export configuration is a list of collectors, to which the service sends records:

- To enable NetFlow, configure at minimum one NetFlow Collector.
- To disable NetFlow, remove all NetFlow Collectors from the Gaia Embedded configuration.

You can configure a maximum of three NetFlow Collectors. Gaia Embedded sends the NetFlow records go to all configured NetFlow Collectors. If you configure three NetFlow Collectors, Gaia Embedded sends each NetFlow record three times.

Regardless of which NetFlow export format you configure, Gaia Embedded exports values as set of fields.

The fields

- Source IP address.
- Destination IP address.
- Source port.
- Destination port.
- Ingress physical interface index (defined by SNMP).
- Egress physical interface index (defined by SNMP).
- Packet count for this flow.
- Byte count for this flow.

- Start of flow timestamp (FIRST_SWITCHED).
- End of flow timestamp (LAST_SWITCHED).
- IP protocol number.
- TCP flags from the flow (TCP only).

Notes:

- The IP addresses and TCP/UDP ports the NetFlow reports are the ones, on which the NetFlow expects to receive traffic.
  Therefore, for NAT connections, the NetFlow reports one of the two directions of the flow with the NATed address.
- NetFlow sends the connection records after the connections terminated.
  If the connections are open for a long time, it can take time for the NetFlow to sends the records.

Configuration Procedure for Centrally Managed

1. **Configure the NetFlow Export settings in Gaia Clish**

   a. Add the NetFlow Collector.

   See *"add netflow collector" on page 640*.

   b. If needed, change the NetFlow Collector configuration.

   See *"set netflow collector" on page 643*.

2. **In SmartConsole, configure the explicit Access Control rule**

   a. From the left navigation panel, click **Security Policies**.

   b. Open the applicable policy.

   c. In the top left corner, click **Access Control > Policy**.

   d. Add an explicit rule for the traffic that you wish to export with NetFlow:

Source	Destination	VPN	Services & Applications	Content	Action	Track
Source Host or Network objects	Destination Host or Network objects	`*Any`	Applicable service objects	`*Any`	`Accept`	`Log Accounting`

   e. Publish the SmartConsole session.

   f. Install the Access Control policy on the Quantum Spark Appliance object.

add netflow collector

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new NetFlow Collector object (you can configure up to three). The NetFlow records are exported to each defined collector.

In addition, see *"Configuring NetFlow Settings" on page 637*.

Syntax

```
add netflow collector ip <IPv4 Address of Collector> port
<Destination Port on Collector> [srcaddr <Source IPv4 Address>]
export-format {Netflow_V5 | Netflow_V9} is-enabled {true | false}
```

Parameters

Parameter	Description
ip <*IPv4 Address of Collector*>	Specifies the destination IPv4 address of the NetFlow Collector, to which Gaia Embedded sends the NetFlow packets.
port <*Destination Port on Collector*>	Specifies the destination UDP port number on the NetFlow Collector, on which the collector listens. Type: Port number
srcaddr <*Source IPv4 Address*>	**Optional:** Specifies the source IPv4 address of the NetFlow packets. This must be an IPv4 address of the local host. The default is an IPv4 address of the network interface, from which Gaia Embedded sends the NetFlow packets. We recommend the default.
export-format {Netflow_V5 | Netflow_V9}	The NetFlow protocol version to use: ▪ `Netflow_V5` - Protocol NetFlow v5 ▪ `Netflow_V9` - Protocol NetFlow v9 (default) Each NetFlow protocol version has a different packet format.
is-enabled {true | false}	Enables (`true`) and disables (`false`) the NetFlow Collector. Type: Boolean (true/false)

Example Command

```
add netflow collector ip 192.168.22.33 port 8080 export-format
Netflow_V9 srcaddr 192.168.1.1 is-enabled true
```

delete netflow collector

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing NetFlow Collector.

In addition, see *"Configuring NetFlow Settings" on page 637*.

Syntax

```
delete netflow collector ip [Press TAB to select the configured
IPv4 Address of Collector] port [Press TAB to select the
configured Destination Port on Collector]
```

Parameters

Parameter	Description
ip <*IPv4 Address of Collector*>	Selects the configured NetFlow Collector by its destination IPv4 address.
port <*Destination Port on Collector*>	Selects the configured NetFlow Collector by its destination UDP port number. Type: Port number

Example Command

```
delete netflow collector ip 192.168.22.33 port 8080
```

set netflow collector

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing NetFlow Collector that you added with the *"add netflow collector" on page 640* command.

In addition, see *"Configuring NetFlow Settings" on page 637*.

Syntax

```
set netflow collector
   for-ip [Press TAB to select the configured IPv4 Address of
Collector]
      for-port [Press TAB to select the configured Destination
Port on Collector]
         ip <IPv4 Address of Collector> port <Destination Port on
Collector> export-format {Netflow_V5 | Netflow_V9} [srcaddr
<Source IPv4 Address>] is-enabled {true | false}
```

Parameters

Parameter	Description
for-ip <*IPv4 Address of Collector*>	Selects the configured NetFlow Collector by its destination IPv4 address. **Notes:** ■ If you configured only one NetFlow Collector, it is not necessary to use the "`for-ip`" and the "`for-port`" parameters. ■ If you configured two or three NetFlow Collectors with different IP addresses, use the "`for-ip`" parameter. ■ If you configured two or three collectors with the same IPv4 address and different UDP ports, you must use the "`for-ip`" and the "`for-port`" parameters to identify the collectors.
for-port <*Destination Port on Collector*>	Selects the configured NetFlow Collector by its destination UDP port number. Type: Port number

Parameter	Description
ip <*IPv4 Address of Collector*>	Specifies the destination IPv4 address of the NetFlow Collector, to which Gaia Embedded sends the NetFlow packets.
port <*Destination Port on Collector*>	Specifies the destination UDP port number on the NetFlow Collector, on which the collector listens. Type: Port number
export-format {Netflow_V5 | Netflow_V9}	The NetFlow protocol version to use: ■ `Netflow_V5` - Protocol NetFlow v5 ■ `Netflow_V9` - Protocol NetFlow v9 (default) Each NetFlow protocol version has a different packet format.
srcaddr <*Source IPv4 Address*>	**Optional:** Specifies the source IPv4 address of the NetFlow packets. This must be an IPv4 address of the local host. The default is an IPv4 address of the network interface, from which Gaia Embedded sends the NetFlow packets. We recommend the default.
is-enabled {true | false}	Enables (`true`) and disables (`false`) the NetFlow Collector. Type: Boolean (true/false)

Example Command

```
set netflow collector for-ip 192.168.22.33 for-port 8080 ip
192.168.22.33 port 8080 export-format Netflow_V9 srcaddr
192.168.1.1 is-enabled true
```

show netflow collector

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration of a specific NetFlow collector.

In addition, see:

- *"show netflow collectors" on page 646*
- *"Configuring NetFlow Settings" on page 637*

Syntax

```
show netflow collector ip [Press TAB to select the configured IPv4
Address of Collector] port [Press TAB to select the configured
Destination Port on Collector]
```

Parameters

Parameter	Description
ip <*IPv4 Address of Collector*>	Selects the configured NetFlow Collector by its destination IPv4 address.
port <*Destination Port on Collector*>	Selects the configured NetFlow Collector by its destination UDP port number. Type: Port number

Example Command

```
show netflow collector ip 192.168.22.33 port 8080
```

show netflow collectors

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration of all NetFlow collectors.

In addition, see:

- *"show netflow collector" on page 645*
- *"Configuring NetFlow Settings" on page 637*

Syntax

```
show netflow collectors
```

Example Command

```
show netflow collectors
```

Configuring Host Objects

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure a Host object specified by its IP address.

add host

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new host object specified by its IP address.

See:

- *"set host" on page 650*
- *"show host" on page 653*
- *"show hosts" on page 654*
- *"show hosts-details" on page 654*
- *"delete host" on page 652*

Syntax

```
add host name <name>
      [ ipv4-address <ipv4-address> ]
      [ ipv6-address <ipv6-address> ]
      [ dns-resolving {true | false} ]
      [ dhcp-exclude-ip-addr off ]
      [ dhcp-exclude-ip-addr on ]
            [ dhcp-reserve-ip-addr-to-mac { off | on [ mac-addr
<mac-addr> ] ]
            [ mac-reserved-in-dhcp { off | on [ mac-addr <mac-
addr> ] ]
```

Parameters

Parameter	Description
name	Configures the Network Object name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)
ipv4-address	Configures the IPv4 address.
ipv6-address	Configures the IPv6 address.
dns-resolving	Controls whether to add (`true`) or not (`false`) the name of this network object to the database of the internal DNS service
dhcp-exclude-ip-addr	Controls whether to exclude (`on`) or not (`off`) the object's IP address(es) from the internal DHCP service.
dhcp-reserve-ip-addr- to-mac	Controls whether to reserve (`on`) or not (`off`) the association of the object's IP address and its MAC address in the internal DHCP service.
mac-addr	Configures the MAC address.
mac-reserved-in-dhcp	This parameter is deprecated. Use the parameter "`dhcp-reserve-ip-addr-to-mac`".
reserve-mac-address	This parameter is deprecated. Use the parameter "`mac-addr`".

Example Command

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

set host

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing host object configured with an IP address.

See:

- *"add host" on page 648*
- *"show host" on page 653*
- *"show hosts" on page 654*
- *"show hosts-details" on page 654*
- *"delete host" on page 652*

Syntax

```
set host <name>
      [ name <new-name> ]
      [ ipv4-address <ipv4-address> ]
      [ ipv6-address <ipv6-address> ]
      [ dns-resolving {true | false} ]
      [ dhcp-exclude-ip-addr off ]
      [ dhcp-exclude-ip-addr on ]
            [ dhcp-reserve-ip-addr-to-mac { off | on [ mac-addr
<mac-addr> ] ]
            [ mac-reserved-in-dhcp { off | on [ mac-addr <mac-
addr> ] ]
```

Parameters

Parameter	Description
host	Specifies the host object name. Press the TAB key to see the available options.

Parameter	Description
name	Configures the new object name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)
dhcp-exclude-ip-addr	Controls whether to exclude (`on`) or not (`off`) the object's IP address(es) from the internal DHCP service.
dhcp-reserve-ip-addr- to-mac	Controls whether to reserve (`on`) or not (`off`) the association of the object's IP address and its MAC address in the internal DHCP service.
dns-resolving	Controls whether to add (`true`) or not (`false`) the name of this network object to the database of the internal DNS service
ipv4-address	Configures the IPv4 address.
ipv6-address	Configures the IPv6 address.
mac-addr	Configures the MAC address.
mac-reserved-in-dhcp	This parameter is deprecated. Use the parameter "`dhcp-reserve-ip-addr-to-mac`".
reserve-mac-address	This parameter is deprecated. Use the parameter "`mac-addr`".

Example Command

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

delete host

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing host object configured with an IP address.

See:

- *"add host" on page 648*
- *"set host" on page 650*
- *"show host" on page 653*
- *"show hosts" on page 654*
- *"show hosts-details" on page 654*

Syntax

```
delete host <name>
```

Parameters

Parameter	Description
host	Specifies the host object name. Press the TAB key to see the available options.

Example Command

```
delete host MyHost
```

show host

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of an existing host object configured with an IP address.

See:

- *"add host" on page 648*
- *"set host" on page 650*
- *"show hosts" on page 654*
- *"show hosts-details" on page 654*
- *"delete host" on page 652*

Syntax

```
show host <name>
```

Parameters

Parameter	Description
host	Specifies the host object name. Press the TAB key to see the available options.

Example Output

```
HostName> show host MyHost
name:                           MyHost
ipv4-address:                   192.168.1.20
ipv6-address:
dns-resolving:                  true
dhcp-exclude-ip-addr:           on
dhcp-reserve-ip-addr-to-mac:    off
mac-addr:

HostName>
```

show hosts

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows all existing host objects configured with an IP address

The output shows a row for each host object that contains an object's name, its IPv4 address, and its IPv6 address.

See:

- *"add host" on page 648*
- *"set host" on page 650*
- *"show host" on page 653*
- *"show hosts-details" below*
- *"delete host" on page 652*

Syntax

```
show hosts
```

Example Output

```
HostName> show hosts
name                                ipv4-address
 ipv6-address
MyHost_1                            192.168.1.20

MyHost_2                            192.168.1.30

HostName>
```

show hosts-details

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows all existing host objects configured with an IP address

The output shows a section for each host object that contains an object's name, its IPv4 address, and its IPv6 address.

See:

- *"add host" on page 648*
- *"set host" on page 650*
- *"show host" on page 653*
- *"show hosts" on the previous page*
- *"delete host" on page 652*

Syntax

```
show hosts-details
```

Example Output

```
HostName> show hosts-details
name:                          MyHost_1
ipv4-address:                  192.168.10.20
ipv6-address:

name:                          MyHost_2
ipv4-address:                  192.168.10.30
ipv6-address:

HostName>
```

Configuring Device Objects

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure a Device object specified by its MAC address.

add host-by-mac

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new device (host) object configured with a static MAC address.

See:

- *"set host-by-mac" on the next page*
- *"delete host-by-mac" on page 658*
- *"show host-by-mac" on page 659*
- *"show hosts-by-mac" on page 660*

Syntax

```
add host-by-mac name <name> mac-address <mac-address>
```

Parameters

Parameter	Description
name	Configures the object name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)
mac-address	Configures the host MAC address in the format XX:XX:XX:XX:XX:XX.

Example Command

```
add host-by-mac name MyDevice mac-address 00:11:22:33:44:55
```

set host-by-mac

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing device (host) object configured with a static MAC address.

- *"add host-by-mac" on the previous page*
- *"delete host-by-mac" on the next page*
- *"show host-by-mac" on page 659*
- *"show hosts-by-mac" on page 660*

Syntax

```
set host-by-mac
      [ name <new-name> ]
      [ bypass-host-by-ssl-inspection {true | false} ]
      [ mac-address <mac-address> ]
```

Parameters

Parameter	Description
host-by-mac	Specifies the object name. Press the TAB key to see the available options.
name	Configures the new object name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)
bypass-host-by-ssl-inspection	Controls whether this device bypasses (`true`) or not (`false`) the SSL Inspection.
mac-address	Configures the device MAC address in the format XX:XX:XX:XX:XX:XX.

Example Command

```
set host-by-mac name MyDevice name MyNewDevice mac-address
00:11:22:33:44:55
```

delete host-by-mac

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing device (host) object configured with a static MAC address.

See:

- *"add host-by-mac" on page 656*
- *"set host-by-mac" on the previous page*
- *"show host-by-mac" on the next page*
- *"show hosts-by-mac" on page 660*

Syntax

```
delete host-by-mac
      [ mac-address <mac-address> ]
      [ name <name> ]
```

Parameters

Parameter	Description
name	Specifies the object name. Press the TAB key to see the available options.
mac-address	Specifies the device MAC address. Press the TAB key to see the available options.

Example Command

```
delete host-by-mac name MyDevice
```

show host-by-mac

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows an existing device (host) object configured with a static MAC address.

See:

- *"add host-by-mac" on page 656*
- *"set host-by-mac" on page 657*
- *"delete host-by-mac" on the previous page*
- *"show hosts-by-mac" on the next page*

Syntax

```
show host-by-mac name <name> mac-address <mac-address>
```

Parameters

Both parameters are mandatory.

Parameter	Description
name	Specifies the object name. Press the TAB key to see the available options.
mac-address	Specifies the device MAC address. Press the TAB key to see the available options.

Example Output

```
HostName> show host-by-mac name MyDevice mac-address
00:11:22:33:44:55
name:                          MyDevice
mac-address:                   00:11:22:33:44:55
bypass-host-by-ssl-inspection:true

HostName>
```

show hosts-by-mac

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows all existing device (host) objects configured with a static MAC address.

See:

- *"add host-by-mac" on page 656*
- *"set host-by-mac" on page 657*
- *"delete host-by-mac" on page 658*
- *"show hosts-by-mac" above*

Syntax

```
show hosts-by-mac
```

Example Command

```
HostName> show hosts-by-mac
name:                           MyDevice_1
mac-address:                    00:11:22:33:44:55
bypass-host-by-ssl-inspection:true

name:                           MyDevice_2
mac-address:                    00:99:88:77:66:55
bypass-host-by-ssl-inspection:true

HostName>
```

Configuring Group Objects

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Group objects.

add group

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new group object that contains other network objects.

Syntax

```
add group name <name> [ comments "<comment>" ] [ member <name-of-object> ]
```

Parameters

Parameter	Description
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
member	Specifies the network object. Press the TAB key to see the available options.
name	Specifies the group object name. Press the TAB key to see the available options.

Example Command

```
add group name MyGroupObject comments "This is a comment" member MyHostObject
```

set group new-name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing network objects group.

Syntax

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

Parameters

Parameter	Description
name	Specifies the Network Object group name. Press the TAB key to see the available options.
new-name	Configures the new Network Object group name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)

Example Command

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

set group add member

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds an existing Network Object to an existing Group Object.

Syntax

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

Parameters

Parameter	Description
member	Specifies the Network Object name. Press the TAB key to see the available options.
name	Specifies the Group object name. Press the TAB key to see the available options.

Example Command

```
set group MyGroup add member MyHost
```

set group remove member

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Removes an existing Network Object from an existing Network Group object.

Syntax

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

Parameters

Parameter	Description
member	Specifies the Network Object name. Press the TAB key to see the available options.
name	Specifies the Group object name. Press the TAB key to see the available options.

Example Command

```
set group MyGroup remove member MyHost
```

set group remove-all members

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Removes all members from an existing network objects group.

Syntax

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

Parameters

Parameter	Description
name	Specifies the Group object name. Press the TAB key to see the available options.

Example Command

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

delete group

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing group object of network objects.

Syntax

```
delete group <name>
```

Parameters

Parameter	Description
name	Specifies the Group object name. Press the TAB key to see the available options.

Example Command

```
delete group myObject_17
```

show group

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the contents of a network object group.

Syntax

```
show group <name>
```

Parameters

Parameter	Description
name	Specifies the Group object name. Press the TAB key to see the available options.

Example Command

```
show group myObject_17
```

show groups

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the contents of all network object groups.

Syntax

```
show groups
```

Parameters

Parameter	Description
n/a	

Example Command

```
show groups
```

Configuring Groups for User Objects

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure groups for user objects.

add local-group

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new group for user objects.

See *"set local-group" on page 675*.

Syntax

```
add local-group name <name> [ comments "<comments>" ] [ remote-
access-on {true | false} ]
```

Parameters

Parameter	Description
name	Configures the group object name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '`(`' (opening round bracket) ■ '`)`' (closing round bracket) ■ ':' (colon) ■ '`@`' (at)
remote-access-on	Enables (`true`) or disables (`false`) the remote access permissions for this the users group.

Example Command

```
add local-group name MyGroup1 comments "This is Group 1" remote-
access-on true
```

set local-group

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing user group object.

See:

- *"add local-group" on page 673*
- *"set local-group users add user-name" on page 677*
- *"set local-group users remove user-name" on page 678*

Syntax

```
set local-group name <name> [ new-name <new-name> ] [ comments
"<comments>" ] [ remote-access-on {true | false} ]
```

Parameters

Parameter	Description
name	Specifies the name of the existing local group name. Press the TAB key to see the available options.
new-name	Configures the new name for the local group. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
remote-access-on	Specifies if the users group have remote access permissions.

Example Command

```
set local-group name myObject_17 new-name myObject_17 comments
"This is a comment" remote-access-on true
```

set local-group users add user-name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options.
user-name	User's name in the local database

Example Command

```
set local-group users name myObject_17 add user-name user1
```

set local-group users remove user-name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options.
user-name	User's name in the local database Press the TAB key to see the available options.

Example Command

```
set local-group users name myObject_17 remove user-name user1
```

delete local-group

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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

Example Command

```
delete local-group name myObject_17
```

delete local-group all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all existing group objects for user objects.

Syntax

```
delete local-group all
```

Example Command

```
delete local-group all
```

show local-group

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the content of an existing user group object.

Syntax

```
show local-group name <name>
```

Parameters

Parameter	Description
name	Local group name

Example Command

```
show local-group name myObject_17
```

show local-groups

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the content of all existing user group objects.

Syntax

```
show local-groups
```

Example Command

```
show local-groups
```

Configuring Service Objects

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Service objects.

Configuring the Built-In Service Objects

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the built-in Service objects.

set service-system-default Any_TCP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 {true | false} ] [ sync-connections-on-cluster
{true | false} ] [ sync-delay-enable {true | false} ] [ delay-
sync-interval <delay-sync-interval> ] [ aggressive-aging-enable
{true | false} ] [ aggressive-aging-timeout <aggressive-aging-
timeout>]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port. See *IANA Service Name and Port Number Registry*.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	In a cluster, controls whether to delay synchronization of connections with this service.
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in Any_TCP service object.

Syntax

```
show service-system-default Any_TCP
```

Example Output

```
HostName> show service-system-default Any_TCP
port:                          1-65535
type:                          tcp
proto-type:                    none
comments:                      Any TCP service
session-timeout:               3600
use-source-port:
source-port:
keep-connections-open-after-policy-installation:false
sync-connections-on-cluster:   true
sync-delay-enable:             false
delay-sync-interval:           30
aggressive-aging-enable:       true
aggressive-aging-timeout:      600

HostName>
```

set service-system-default Any_UDP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 {true | false} ] [ sync-connections-on-cluster
{true | false} ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ] [ accept-
replies {true | false} ]
```

Parameters

Parameter	Description
accept-replies	Specifies whether to accept reply traffic for this service.
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
use-source-port	Use source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in Any_UDP service object.

Syntax

```
show service-system-default Any_UDP
```

Example Output

```
HostName> show service-system-default Any_UDP
port:                          1-65535
type:                          udp
proto-type:                    none
comments:                      Any UDP service
session-timeout:               40
use-source-port:
source-port:
keep-connections-open-after-policy-installation:false
sync-connections-on-cluster:   true
aggressive-aging-enable:       true
aggressive-aging-timeout:      15
accept-replies:                true

HostName>
```

set service-system-default CIFS

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	In a cluster, controls whether to delay synchronization of connections with this service.
use-source-port	Use source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in CIFS service object.

Syntax

```
show service-system-default CIFS
```

Example Output

```
HostName> show service-system-default CIFS
type:                          tcp
comments:                      Microsoft CIFS over TCP
port:                          445
disable-inspection:            true
proto-type:                    CIFS_PROTOCOL
session-timeout:               3600
use-source-port:
source-port:
keep-connections-open-after-policy-installation:false
sync-connections-on-cluster:   true
sync-delay-enable:             false
delay-sync-interval:           30
aggressive-aging-enable:       true
aggressive-aging-timeout:      600

HostName>
```

set service-system-default Citrix

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false}] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	In a cluster, controls whether to delay synchronization of connections with this service.
use-source-port	Use source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in Citrix service object.

Syntax

```
show service-system-default Citrix
```

Example Output

```
HostName> show service-system-default Citrix
type:                          tcp
comments:                      Allows servers to provide
applications and data for attached computer workstations for
Windows
port:                          1494
disable-inspection:            false
proto-type:                    none
session-timeout:               3600
use-source-port:
source-port:
keep-connections-open-after-policy-installation:false
sync-connections-on-cluster:   true
sync-delay-enable:             false
delay-sync-interval:           30
aggressive-aging-enable:       true
aggressive-aging-timeout:      600

HostName>
```

set service-system-default Citrix firewall-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set service-system-default Citrix firewall-settings protocol-
support PROTO_TYPE.WIN_FRAME
```

show service-system-default Citrix firewall-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the inspection settings of the built-in Citrix service object.

Syntax

```
show service-system-default Citrix firewall-settings
```

set service-system-default DHCP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures settings of the built-in DHCP service object.

Syntax

```
set service-system-default DHCP [ port <port> ] [ disable-
inspection {true | false} ] [ session-timeout <session-timeout> ]
[ use-source-port { false | true [ source-port <source-port> ] } ]
[ accept-replies {true | false} ]
```

Parameters

Parameter	Description
accept-replies	Specifies whether to accept reply traffic for this service.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port. See *IANA Service Name and Port Number Registry*.
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in DHCP service object.

Syntax

```
show service-system-default DHCP
```

Example Output

```
HostName> show service-system-default DHCP
type:                          udp
comments:                      DHCP request from enforcement module
only
port:                          67-68
disable-inspection:            false
proto-type:                    none
session-timeout:               40
use-source-port:
source-port:
accept-replies:                true

HostName>
```

set service-system-default DNS_TCP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	In a cluster, controls whether to delay synchronization of connections with this service.
use-source-port	Use source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in DNS_TCP service object.

Syntax

```
show service-system-default DNS_TCP
```

Example Output

```
HostName> show service-system-default DNS_TCP
type:                          tcp
comments:                      Domain Name System Download
port:                          53
disable-inspection:            false
proto-type:                    DNS_TCP
session-timeout:               3600
use-source-port:
source-port:
keep-connections-open-after-policy-installation:false
sync-connections-on-cluster:   true
sync-delay-enable:             false
delay-sync-interval:           30
aggressive-aging-enable:       true
aggressive-aging-timeout:      600

HostName>
```

set service-system-default DNS_UDP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures settings of the built-in DNS_UDP service object.

Syntax

```
set service-system-default DNS_UDP [ port <port> ] [ disable-
inspection {true | false} ] [ session-timeout <session-timeout> ]
[ use-source-port { false | true [ source-port <source-port> ] } ]
[ accept-replies {true | false} ]
```

Parameters

Parameter	Description
accept-replies	Specifies whether to accept reply traffic for this service.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
port	Destination ports (a comma separated list of ports/ranges).
session-timeout	Configures the time (in seconds) before the session times out..
source-port	Source port.
use-source-port	Use source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in DNS_UDP service object.

Syntax

```
show service-system-default DNS_UDP
```

Example Output

```
HostName> show service-system-default DNS_UDP
type:                          udp
comments:                      Domain Name System Queries
port:                          53
disable-inspection:            false
proto-type:                    DNS_UDP
session-timeout:               40
use-source-port:
source-port:
accept-replies:                true

HostName>
```

set service-system-default FTP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false}] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
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	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy..
port	Destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out..
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	In a cluster, controls whether to delay synchronization of connections with this service.
use-source-port	Use source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in FTP service object.

Syntax

```
show service-system-default FTP
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default FTP
```

set service-system-default FTP firewall-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set service-system-default FTP firewall-settings mode any
```

show service-system-default FTP firewall-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show service-system-default FTP firewall-settings
```

set service-system-default GRE

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 {true | false} ] [ match
"<match>" ] [ keep-connections-open-after-policy-installation
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
aggressive-aging-enable {true | false} ] [ aggressive-aging-
timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
accept-replies	Specifies whether to accept reply traffic for this service.
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. A number with no fractional part (integer)
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy..
match	INSPECT expression that searches for a pattern in a packet, only relevant for services of type 'other'.
session-timeout	Configures the time (in seconds) before the session times out.
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in GRE service object.

Syntax

```
show service-system-default GRE
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default GRE
```

set service-system-default H323

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ]
```

Parameters

Parameter	Description
delay-sync-interval	Time (in seconds) after connection initiation to start synchronizing connections.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy..
port	Destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out..
source-port	Source port.
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	In a cluster, controls whether to delay synchronization of connections with this service.
use-source-port	Use source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in H323 service object.

Syntax

```
show service-system-default H323
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default H323
```

set service-system-default H323_RAS

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures settings of the built-in H323_RAS service object.

Syntax

```
set service-system-default H323_RAS [ port <port> ] [ disable-
inspection {true | false} ] [ session-timeout <session-timeout> ]
[ use-source-port { false | true [ source-port <source-port> ] } ]
[ accept-replies {true | false} ]
```

Parameters

Parameter	Description
accept-replies	Specifies whether to accept reply traffic for this service.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
port	Destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out..
source-port	Source port.
use-source-port	Use source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show service-system-default H323_RAS
```

set service-system-default HTTP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster <sync-connections-
on-cluster> ] [ sync-delay-enable {true | false}] [ delay-sync-
interval <delay-sync-interval> ] [ aggressive-aging-enable {true |
false} ] [ 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	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy..
port	Destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out..
source-port	Source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	In a cluster, controls whether to delay synchronization of connections with this service.
use-source-port	Use source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in HTTP service object.

Syntax

```
show service-system-default HTTP
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default HTTP
```

set service-system-default HTTPS

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
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	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy..
port	Destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out..
source-port	Source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	In a cluster, controls whether to delay synchronization of connections with this service.
use-source-port	Use source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in HTTPS service object.

Syntax

```
show service-system-default HTTPS
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default HTTPS
```

set service-system-default HTTP ips-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show service-system-default HTTP ips-settings
```

set service-system-default HTTPS url-filtering-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set service-system-default HTTPS url-filtering-settings
categorize-https-sites true
```

show service-system-default HTTPS url-filtering-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show service-system-default HTTPS url-filtering-settings
```

set service-system-default IIOP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false}] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
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	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy..
port	Destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out..
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	In a cluster, controls whether to delay synchronization of connections with this service.
use-source-port	Use source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in IIOP service object.

Syntax

```
show service-system-default IIOP
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default IIOP
```

set service-system-default IMAP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
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	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy..
port	Destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in IMAP service object.

Syntax

```
show service-system-default IMAP
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default IMAP
```

set service-system-default LDAP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in LDAP service object.

Syntax

```
show service-system-default LDAP
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default LDAP
```

set service-system-default MGCP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures settings of the built-in MGCP service object.

Syntax

```
set service-system-default MGCP [ port <port> ] [ disable-
inspection {true | false} ] [ session-timeout <session-timeout> ]
[ use-source-port { false | true [ source-port <source-port>] } ]
[ accept-replies {true | false} ]
```

Parameters

Parameter	Description
accept-replies	Specifies whether to accept reply traffic for this service.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in MGCP service object.

Syntax

```
show service-system-default MGCP
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default MGCP
```

set service-system-default NetBIOSDatagram

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures settings of the built-in NetBiosDatagram service object.

Syntax

```
set service-system-default NetBIOSDatagram [ port <port> ] [
disable-inspection {true | false} ] [ session-timeout <session-
timeout> ] [ use-source-port { false | true [ source-port <source-
port> ] } ] [ accept-replies {true | false} ]
```

Parameters

Parameter	Description
accept-replies	Specifies whether to accept reply traffic for this service.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in NetBiosDatagram service object.

Syntax

```
show service-system-default NetBIOSDatagram
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default NetBIOSDatagram
```

set service-system-default NetBIOSName

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures settings of the built-in NetBiosName service object.

Syntax

```
set service-system-default NetBIOSName [ port <port> ] [ disable-
inspection {true | false} ] [ session-timeout <session-timeout> ]
[ use-source-port { false | true [ source-port <source-port> ] } ]
[ accept-replies {true | false} ]
```

Parameters

Parameter	Description
accept-replies	Specifies whether to accept reply traffic for this service.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in NetBiosName service object.

Syntax

```
show service-system-default NetBIOSName
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default NetBIOSName
```

set service-system-default NetShow

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in NetShow service object.

Syntax

```
show service-system-default NetShow
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default NetShow
```

set service-system-default NNTP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in NNTP service object.

Syntax

```
show service-system-default NNTP
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default NNTP
```

set service-system-default POP3

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in POP3 service object.

Syntax

```
show service-system-default POP3
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default POP3
```

set service-system-default PPTP_TCP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false}] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show service-system-default PPTP_TCP
```

set service-system-default PPTP_TCP ips-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set service-system-default PPTP_TCP ips-settings action block
track none strict true
```

show service-system-default PPTP_TCP ips-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show service-system-default PPTP_TCP ips-settings
```

set service-system-default RealAudio

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in RealAudio service object.

Syntax

```
show service-system-default RealAudio
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default RealAudio
```

set service-system-default RSH

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in RSH service object.

Syntax

```
show service-system-default RSH
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default RSH
```

set service-system-default RTSP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in RTSP service object.

Syntax

```
show service-system-default RTSP
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default RTSP
```

set service-system-default SCCP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in SCCP service object.

Syntax

```
show service-system-default SCCP
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default SCCP
```

set service-system-default SCCPS

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in SCCPS service object.

Syntax

```
show service-system-default SCCPS
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default SCCPS
```

set service-system-default SIP_TCP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show service-system-default SIP_TCP
```

set service-system-default SIP_UDP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures settings of the built-in SIP_UDP service object.

Syntax

```
set service-system-default SIP_UDP [ port <port> ] [ disable-
inspection {true | false} ] [ session-timeout <session-timeout> ]
[ use-source-port { false | true [ source-port <source-port> ] } ]
[ accept-replies {true | false} ]
```

Parameters

Parameter	Description
accept-replies	Specifies whether to accept reply traffic for this service.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show service-system-default SIP_UDP
```

set service-system-default SMTP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in SMTP service object.

Syntax

```
show service-system-default SMTP
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default SMTP
```

set service-system-default SNMP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures settings of the built-in SNMP service object.

Syntax

```
set service-system-default SNMP [ port <port> ] [ disable-
inspection {true | false} ] [ session-timeout <session-timeout> ]
[ use-source-port { false | true [ source-port <source-port> ] } ]
[ accept-replies {true | false} ]
```

Parameters

Parameter	Description
accept-replies	Specifies whether to accept reply traffic for this service.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in SNMP service object.

Syntax

```
show service-system-default SNMP
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default SNMP
```

set service-system-default SNMP firewall-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set service-system-default SNMP firewall-settings read-only true
```

show service-system-default SNMP firewall-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show service-system-default SNMP firewall-settings
```

set service-system-default SQLNet

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in SQLNet service object.

Syntax

```
show service-system-default SQLNet
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default SQLNet
```

set service-system-default SSH

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false} ] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in SSH service object.

Syntax

```
show service-system-default SSH
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default SSH
```

set service-system-default SSH ips-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set service-system-default SSH ips-settings block-version true
```

show service-system-default SSH ips-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show service-system-default SSH ips-settings
```

set service-system-default TELNET

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
{true | false} ] [ sync-connections-on-cluster {true | false} ] [
sync-delay-enable {true | false}] [ delay-sync-interval <delay-
sync-interval> ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.

Parameter	Description
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	True to delay connections synchronization
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in TELNET service object.

Syntax

```
show service-system-default TELNET
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default TELNET
```

set service-system-default TFTP

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures settings of the built-in TFTP service object.

Syntax

```
set service-system-default TFTP [ port <port> ] [ disable-
inspection {true | false} ] [ accept-replies {true | false} ] [
session-timeout <session-timeout> ] [ use-source-port { false |
true [ source-port <source-port> ] } ] [ keep-connections-open-
after-policy-installation {true | false} ] [ sync-connections-on-
cluster {true | false} ]
```

Parameters

Parameter	Description
accept-replies	Specifies whether to accept reply traffic for this service.
disable-inspection	Controls whether to disable deep inspection of traffic that matches this service.
keep-connections-open-after-policy-installation	Controls whether to keep the current connections after policy installation, even if these connections are not allowed by the new policy.
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port.
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
use-source-port	Controls whether to use the source port.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the settings of the built-in TFTP service object.

Syntax

```
show service-system-default TFTP
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-system-default TFTP
```

service-group

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

add service-group

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new group for service objects.

Syntax

```
add service-group name <name> [ comments "<comment>" ] [ member
<member> ]
```

Parameters

Parameter	Description
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
member	Specifies the Network Object. Press the TAB key to see the available options.
name	Configires the Service Group name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)

Example Command

```
add service-group name MyServiceGroup comments "My Web Services"
member HTTP
```

set service-group

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing service objects group.

Syntax

```
set service-group <name> [ new-name <new-name> ] [ comments
"<comment>" ]
```

Parameters

Parameter	Description
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
name	Specifies the Service Group name. Press the TAB key to see the available options.
new-name	Configures the new Service Group name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)

Example Command

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

set service-group remove-all members

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Removes all service objects from an existing service objects group.

Syntax

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

Parameters

Parameter	Description
name	Specifies the Service Group name. Press the TAB key to see the available options.

Example Command

```
set service-group MyServiceGroup remove-all members
```

set service-group add member

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
member	Specifies the Service object. Press the TAB key to see the available options.
name	Specifies the Service Group object. Press the TAB key to see the available options.

Example Command

```
set service-group MyServiceGroup add member HTTP
```

set service-group remove member

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Parameters

Parameter	Description
member	Specifies the Service object. Press the TAB key to see the available options.
name	Specifies the Service Group object. Press the TAB key to see the available options.

Example Command

```
set service-group MyServiceGroup remove member HTTP
```

delete service-group

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing group object for service objects by object name.

Syntax

```
delete service-group <name>
```

Parameters

Parameter	Description
name	Specifies the Service Group object name. Press the TAB key to see the available options.

Example Command

```
delete service-group myObject_17
```

show service-group

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the content of a service object group.

Syntax

```
show service-group <name>
```

Parameters

Parameter	Description
name	Specifies the Service Group object name. Press the TAB key to see the available options.

Example Command

```
show service-group myObject_17
```

show service-groups

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the content of all service object groups.

Syntax

```
show service-groups
```

Parameters

Parameter	Description
n/a	

Example Command

```
show service-groups
```

service-tcp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

add service-tcp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new TCP service object with configurable ports.

Syntax

```
add service-tcp name <name> port <port> [ comments "<comment>" ]
```

Parameters

Parameter	Description
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
name	Configures the Service name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.

Example Command

```
add service-tcp name MyService port 8080-8090 comments "This is a
comment"
```

set service-tcp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing TCP service object.

Syntax

```
set service-tcp <existing-name> [ name <name> ] [ port <port> ] [
comments "<comment>" ] [ session-timeout <session-timeout>] [
sync-connections-on-cluster {true | false} ] [ sync-delay-enable
{true | false} ] [ delay-sync-interval <delay-sync-interval> ] [
aggressive-aging-enable {true | false} ] [ 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 Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
delay-sync-interval	In a cluster, configures the delay time (in seconds), after which the connection synchronization starts.

Parameter	Description
name	Configures the Service name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
service-tcp	Specifies the existing Service name. Press the TAB key to see the available options.
session-timeout	Configures the time (in seconds) before the session times out.
source-port	Configures the source port. See *IANA Service Name and Port Number Registry*.
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.
sync-delay-enable	In a cluster, controls whether to delay synchronization of connections with this service.
use-source-port	Controls whether to use the source port.

Example Command

```
set service-tcp MyService name MyService2 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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing TCP service object by name.

Syntax

```
delete service-tcp <name>
```

Parameters

Parameter	Description
name	Specifies the Service name. Press the TAB key to see the available options.

Example Command

```
delete service-tcp MyService
```

show service-tcp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of a specific TCP service object.

Syntax

```
show service-tcp <name>
```

Parameters

Parameter	Description
name	Service name Type: String

Example Command

```
show service-tcp TEXT
```

show services-tcp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of all TCP service objects.

Syntax

```
show services-tcp
```

Parameters

Parameter	Description
n/a	

Example Command

```
show services-tcp
```

service-udp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

add service-udp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new UDP service object with configurable ports.

Syntax

```
add service-udp name <name> port <port> [ comments "<comment>" ]
```

Parameters

Parameter	Description
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
name	Configures the Service name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.

Example Command

```
add service-udp name MyService port 8080-8090 comments "This is a
comment"
```

set service-udp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing UDP service object.

Syntax

```
set service-udp <existing-name> [ name <new-name> ] [ port <port>
] [ comments "<comment>" ] [ session-timeout <session-timeout> ] [
accept-replies {true | false} ] [ sync-connections-on-cluster
{true | false} ] [ aggressive-aging-enable {true | false} ] [
aggressive-aging-timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
accept-replies	Specifies whether to accept reply traffic for this service.
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)

Parameter	Description
name	Configures the Service name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)
port	Configures the destination ports (a comma separated list of ports/ranges). See *IANA Service Name and Port Number Registry*.
service-udp	Specifies the existing Service name. Press the TAB key to see the available options.
session-timeout	Configures the time (in seconds) before the session times out.
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.

Example Command

```
set service-udp MyService name MyService2 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
```

delete service-udp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes aexisting UDP service object by name.

Syntax

```
delete service-udp <name>
```

Parameters

Parameter	Description
name	Specifies the Service name. Press the TAB key to see the available options.

Example Command

```
delete service-udp MyService
```

show service-udp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of a specific UDP service object

Syntax

```
show service-udp <name>
```

Parameters

Parameter	Description
name	Service name Type: String

Example Command

```
show service-udp TEXT
```

show services-udp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of all UDP service objects.

Syntax

```
show services-udp
```

Parameters

Parameter	Description
n/a	

Example Command

```
show services-udp
```

service-icmp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

add service-icmp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new ICMP-type service object.

Syntax

```
add service-icmp name <name> icmp-code <icmp-code> icmp-type
<icmp-type> [ comments "<comment>" ]
```

Parameters

Parameter	Description
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
icmp-code	Configures the ICMP code. See RFC 792.
icmp-type	Configures the ICMP type. See RFC 792.
name	Configures the Service name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)

Example Command

```
add service-icmp name MyService icmp-code 2 icmp-type 5 comments
"This is a comment"
```

set service-icmp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing ICMP-type service object.

Syntax

```
set service-icmp <existing-name>[ name <new-name> ] [ icmp-code
<icmp-code> ] [ icmp-type <icmp-type> ] [ comments "<comment>" ]
```

Parameters

Parameter	Description
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
icmp-code	Configures the ICMP code. See RFC 792.
icmp-type	Configures the ICMP type. See RFC 792.
name	Configures the new Service name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)

Parameter	Description
service-icmp	Specifies the existing Service name. Press the TAB key to see the available options.

Example Command

```
set service-icmp MyService name TEXT icmp-code 2 icmp-type 5
comments "This is a comment"
```

delete service-icmp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing ICMP-type service object by name.

Syntax

```
delete service-icmp <name>
```

Parameters

Parameter	Description
name	Specifies the Service name. Press the TAB key to see the available options.

Example Command

```
delete service-icmp MyService
```

show service-icmp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show service-icmp TEXT
```

show services-icmp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of all ICMP-type service objects.

Syntax

```
show services-icmp
```

Example Command

```
show services-icmp
```

service-protocol

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

add service-protocol

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new non-TCP/UDP service object that uses a protocol other than TCP (6) or UDP (17).

Syntax

```
add service-protocol name <name> ip-protocol <ip-protocol> [
comments "<comment>" ]
```

Parameters

Parameter	Description
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
ip-protocol	Configures the IP protocol number. See *IANA Protocol Numbers*.
name	Configures the Service name.

Example Command

```
add service-protocol name TEXT ip-protocol 50 comments "This is a
comment"
```

set service-protocol

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing non-TCP/UDP service object.

Syntax

```
set service-protocol <service-protocol-name> [ name <name> ] [ ip-
protocol <ip-protocol> ] [ comments "<comment>" ] [ session-
timeout <session-timeout> ] [ accept-replies {true | false} ] [
sync-connections-on-cluster {true | false} ] [ match "<match>" ] [
aggressive-aging-enable {true | false} ] [ aggressive-aging-
timeout <aggressive-aging-timeout> ]
```

Parameters

Parameter	Description
accept-replies	Specifies whether to accept reply traffic for this service.
aggressive-aging-enable	Enable to manage the connections table capacity and memory consumption of the Security Gateway.
aggressive-aging-timeout	Configures the time (in seconds) before the aggressive aging times out.
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '`(`' (opening round bracket) ■ '`)`' (closing round bracket) ■ ':' (colon) ■ '`@`' (at)
ip-protocol	Configures the IP protocol number. See *IANA Protocol Numbers*.

Parameter	Description
match	Configures the INSPECT expression that searches for a pattern in a packet. Applies only to services of type '`other`'. For more information, see capture examples in sk30583.
name	Configures the Service name.
session-timeout	Configures the time (in seconds) before the session times out.
service-protocol	Specifies the predefined service protocol. Press the TAB key to see the available options.
sync-connections-on-cluster	In a cluster, controls whether to synchronize connections with this service.

Example Command

```
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 "port(80)" aggressive-aging-
enable true aggressive-aging-timeout 15
```

delete service-protocol

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes aexisting non-TCP/UDP service object by name.

Syntax

```
delete service-protocol <name>
```

Parameters

Parameter	Description
name	Specifies the Service name. Press the TAB key to see the available options.

Example Command

```
delete service-protocol MyService
```

show service-protocol

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show service-protocol TEXT
```

show services-protocol

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of all non-TCP/UDP service objects.

Syntax

```
show services-protocol
```

Parameters

Parameter	Description
n/a	

Example Command

```
show services-protocol
```

Configuring IPv4 Network Address Objects

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure IPv4 Network Address objects.

add network

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new Network object (with a network IP address 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
name	Configures the object name
network-ipv4-address	Configures the IPv4 address
mask-length	Configures the IPv4 subnet mask length
subnet-mask	Configures the IPv4 subnet mask

Example Command

```
add network name MyInternalNetwork network-ipv4-address
172.16.10.0 subnet-mask 255.255.255.0
```

set network

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set network TEXT name TEXT network-ipv4-address 172.16.10.0
subnet-mask 255.255.255.0
```

delete network

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
delete network TEXT
```

show network

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration of a specific IP address network object.

Syntax

```
show network <name>
```

Parameters

Parameter	Description
name	Network Object name Type: String

Example Command

```
show network TEXT
```

show networks

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration of all IP address network objects.

Syntax

```
show networks
```

Parameters

Parameter	Description
n/a	

Example Command

```
show networks
```

Configuring IPv6 Network Address Objects

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure IPv6 Network Address objects.

add ipv6-network

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add an IPv6 network object.

Syntax

```
add ipv6-network name "<name>" network-ipv6-address <network-ipv6-address> ipv6-prefix <ipv6-prefix>
```

Parameters

Parameter	Description
name	Network Object name
network-ipv6-address	Network IPv6 address
ipv6-prefix	IPv6 address prefix

Example Command

```
add ipv6-network name MyIPv6_Net network-ipv6-address 2001:db8:abcd:0012::0 ipv6-prefix 64
```

delete ipv6-network

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete an IPv6 network.

Syntax

```
delete ipv6-network name <name>
```

Parameters

Parameter	Description
name	Network Object name Type: String

Example Command

```
delete ipv6-network name TEXT
```

set ipv6-network

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure settings for IPv6 network.

Syntax

```
set ipv6-network <name> [ network-ipv6-address <network-ipv6-
address> ] ipv6-prefix <ipv6-prefix> ]
```

Parameters

Parameter	Description
ipv6-prefix	The prefix length for IPv6 address
name	Network Object name Type: String
network-ipv6-address	IPv6 address

Example Command

```
set ipv6-network TEXT network-ipv6-address v6network ] ipv6-prefix
ipv6prefixLength
```

show ipv6-network

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the IPv6 network.

Syntax

```
show ipv6-network name <name>
```

Parameters

Parameter	Description
name	Network Object name Type: String

Example Command

```
show ipv6-network name netObj2
```

Example Output

```
name:                           netObj2
network-ipv6-address:           2620:0:2a03:81::
ipv6-prefix:                    64
```

show ipv6-networks

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the IPv6 networks.

Syntax

```
show ipv6-networks
```

Example Command

```
show ipv6-networks
```

Example Output

```
name                                network-ipv6-address   ipv6-
prefix
netObj2                             2620:0:2a03:81::       64
```

show ipv6-networks-details

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show details of the IPv6 networks.

Syntax

```
show ipv6-networks-details
```

Example Command

```
show ipv6-networks-details
```

Example Output

```
name:                           netObj2
network-ipv6-address:           2620:0:2a03:81::
ipv6-prefix:                    64
```

Configuring IPv4 Address Range Objects

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure IPv4 Address Range objects.

add address-range

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 {on | off} ]
```

Parameters

Parameter	Description
dhcp-exclude-ip-addr	Indicates if the IP range addresses are excluded from the internal DHCP daemon
end-ipv4	The last IP address in the IP range
name	Network Object name
start-ipv4	The first IP address in the IP range

Example Command

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

set address-range

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

delete address-range

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing address range object.

Syntax

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

Parameters

Parameter	Description
name	Network Object name Type: String

Example Command

```
delete address-range TEXT
```

show address-range

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show address-range TEXT
```

show address-ranges

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows settings of all configured IP address range objects.

Syntax

```
show address-ranges
```

Parameters

Parameter	Description
n/a	

Example Command

```
show address-ranges
```

Configuring IPv6 Address Range Objects

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure IPv6 Address Range objects.

add address-ipv6-range

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add an IP address in the IPv6 range.

Syntax

```
add address-ipv6-range name <name> { start-ipv6 <start-ipv6> |
ipv6-address <ipv6-address> } end-ipv6 <end-ipv6>
```

Parameters

Parameter	Description
end-ipv6	The end of the IPv6 range
ipv6-address	This field is deprecated. Use the field `start-ipv6`
name	Network Object name
start ipv6	The beginning of the IPv6 range

Example Command

```
add address-ipv6-range name TEXT start-ipv6 ipv6addr end-ipv6
ipv6addr
```

set address-ipv6-range

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure an IP address in the IPv6 range.

Syntax

```
set address-ipv6-range <name> [ name <name> ] { [ start-ipv6
<start-ipv6> | [ ipv6-address <ipv6-address> ] } [ end-ipv6 <end-
ipv6> ]
```

Parameters

Parameter	Description
end-ipv6	The end of the IPv6 range
ipv6-address	This field is deprecated. Please use field `start-ipv6`
name	Network Object name Type: String
start-ipv6	The beginning of the IPv6 range

Example Command

```
set address-ipv6-range TEXT name TEXT start-ipv6 ipv6addr end-ipv6
ipv6addr
```

delete address-ipv6-range

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete an IP address in the IPv6 range.

Syntax

```
delete address-ipv6-range <name>
```

Parameters

Parameter	Description
name	Network Object name Type: String

Example Command

```
delete address-ipv6-range TEXT
```

show address-ipv6-range

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show an IP address in the IPv6 range.

Syntax

```
show address-ipv6-range <name>
```

Parameters

Parameter	Description
name	Network Object name Type: String

Example Command

```
show address-ipv6-range netObj1
```

Example Output

```
name:                           netObj1
start-ipv6:                     2620:0:2a03:86::
end-ipv6:                       2620:0:2a03:87::
```

show address-ipv6-ranges

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show IP address in the IPv6 ranges.

Syntax

```
show address-ipv6-ranges
```

Parameters

Parameter	Description
n/a	

Example Command

```
show address-ipv6-ranges
```

Example Output

```
name                                    start-ipv6   end-ipv6
netObj1                                 2620:0:2...  2620:0...
```

show address-ipv6-ranges-details

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show details of the IPv6 ranges.

Syntax

```
show address-ipv6-ranges-details
```

Example Command

```
show address-ipv6-ranges-details
```

Example Output

```
name:                           netObj1
start-ipv6:                     2620:0:2a03:86::
end-ipv6:                       2620:0:2a03:87::
```

Configuring Server Objects

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Server objects.

add server

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new server object.

Server objects 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 {true | false} ] type { web-server | ftp-server | citrix-server | pptp-server | mail-server | dns-server | custom-server [ tcpProtocol {true | false} [ tcp-ports <tcp-ports> ] udpProtocol {true | false} [ udp-ports <udp-ports> ] ] }
```

Parameters

Parameter	Description
name	Server object name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)

Parameter	Description
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
dhcp-exclude-ip-addr	Indicates if the internal DHCP service will not distribute the configured IP address of this server/network object to anyone 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 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
ipv4-address	The beginning of the IP range
mac-addr	MAC address of the server
tcp-ports	Range of TCP ports for the server of type 'other'
tcpProtocol	This is a TCP-based protocol
udp-ports	Range of UDP ports for the server of type 'other'
udpProtocol	This is a UDP-based protocol

Example Command

```
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
```

set server server-access

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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. 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

Parameter	Description
name	Specifies the Server object name. Press the TAB key to see the available options.
trusted-zone-dmz	Indicates if traffic from the DMZ network to the server is allowed or blocked by default Options: blocked, allowed
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 Command

```
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-ports

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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)

Parameter	Description
name	Specifies the Server object name. Press the TAB key to see the available options.
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)
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)

Parameter	Description
tcp-ports	TCP ports for server of type 'other' See *IANA Service Name and Port Number Registry*.
tcpProtocol	tcpProtocol Type: Boolean (true/false)
udp-ports	UDP ports for server of type 'other' See *IANA Service Name and Port Number Registry*.
udpProtocol	udpProtocol Type: Boolean (true/false)
web-server	Indicates a web server (for each type we provide default but configurable ports)

Example Command

```
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
```

set server server-network-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures network settings in an existing Server object.

Syntax

```
set server server-network-settings <name> [ name <name> ] [ dhcp-
exclude-ip-addr { off | on [ dhcp-reserve-ip-addr-to-mac { off |
on mac-addr <mac-addr> } ] } ] [ comments "<comment>" ] [ dns-
resolving {true | false} ] [ ipv4-address <ipv4-address> ]
```

Parameters

Parameter	Description
comments	Configures the comment text. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
dhcp-exclude-ip-addr	Specifies if the internal DHCP service will not distribute the configured IP address of this server/network object to anyone.
dhcp-reserve-ip-addr- to-mac	Specifies if the internal DHCP service will distribute the configured IP address only to this server/network object according to its MAC address.
dns-resolving	Specifies if the name of the server/network object to be used as a hostname for internal DNS service.
ipv4-address	Configures the beginning of the IP range.

Parameter	Description
mac-addr	Configures the MAC address of the server.
name	Specifies the Server object name. Press the TAB key to see the available options.

Example Command

```
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-nat-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Specifies the Server object name. Press the TAB key to see the available options.
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) 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

Parameter	Description
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

Example Command

```
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
```

delete server

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing server object.

Syntax

```
delete server <name>
```

Parameters

Parameter	Description
name	Server object name

Example Command

```
delete server myObject_17
```

show server

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration of an existing server object.

Syntax

```
show server <name>
```

Parameters

Parameter	Description
name	Server object name

Example Command

```
show server myObject_17
```

show servers

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of all server objects.

Syntax

```
show servers
```

Example Command

```
show servers
```

Configuring RADIUS Servers

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure RADIUS servers.

set radius-server

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures RADIUS servers.

Allows locally managed Remote Access users (on the RADIUS server) to have longer passwords for increased security.

See:

- *"show radius-server priority" on the next page*
- *"show radius-server priority" on the next page*
- *"delete radius-server" on page 883*

Syntax

```
set radius-server priority {1 | 2} ipv4-address <ipv4-address> [
ipv6-address <ipv6-address> ] shared-secret <shared-secret> [ udp-
port <udp-port> ] [ timeout <timeout> ] [ version {1 | 2} ]
```

Parameters

Parameter	Description
ipv4-address	The IPv4 address of the RADIUS server.
ipv6-address	The IPv6 address of the RADIUS server.
priority	Priority of the RADIUS server: ■ 1 (primary) ■ 2 (secondary) Default: 1.
shared-secret	Pre-shared secret between the RADIUS server and the appliance. A string that contains alphanumeric and special characters.
timeout	A timeout value in seconds for communication with the RADIUS server. Default: 3. Range: 0 - 5000.

Parameter	Description
version	Version of the RADIUS server: ■ 1 ■ 2 Default: 1.
udp-port	The port number through which the RADIUS server communicates with clients. Default: 1812.

Example Command

```
set radius-server priority 2 ipv4-address 192.168.1.1 shared-
secret a(&7Ba timeout 15 version 2
```

show radius-server priority

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show RADIUS servers with the specified priority.

See:

- *"set radius-server" on the previous page*
- *"show radius-servers" on page 882*

Syntax

```
show radius-server priority {1 | 2}
```

Parameters

Parameter	Description
priority	Specifies the priority of the RADIUS servers to show.

Example Command

```
HostName> show tacacs-server priority 1

priority:                       1
ipv4-address:                   192.168.3.200
ipv6-address:
udp-port:                       1812
shared-secret:                  78343c263a57
timeout:                        3
version:                        1
```

show radius-servers

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of all RADIUS servers.

See:

- *"show radius-server priority" on page 880*
- *"set radius-server" on page 879*

Syntax

```
show radius-servers
```

delete radius-server

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing configured RADIUS server.

See:

- *"set radius-server" on page 879*
- *"show radius-server priority" on page 880*
- *"show radius-servers" on page 882*

Syntax

```
delete radius-server priority <priority>
```

Parameters

Parameter	Description
priority	Priority of the RADIUS server.

Example Command

```
delete radius-server priority 1
```

Configuring TACACS+ Servers

In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

This section provides commands to work with TACACS+ servers.

set tacacs-server

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Configure the settings for the TACACS+ server.

See:

- *"show tacacs-servers" on page 886*
- *"show tacacs-servers priority" on page 887*
- *"delete tacacs-server" on page 888*

Syntax

```
set tacacs-server priority {1 | 2} ipv4-address <ipv4-address>
shared-secret <shared-secret> [ tcp-port <tcp-port> ] [ timeout
<timeout> ]
```

Parameters

Parameter	Description
priority	Priority of the TACACS+ server: ■ 1 (primary) ■ 2 (secondary) Default: 1.
ipv4-address	The IP address of the TACACS+ server
shared-secret	Pre-shared secret between the TACACS+ server and the appliance. A string that contains alphanumeric and special characters.
tcp-port	The port number through which the TACACS+ server communicates with clients. Default: 49.
timeout	A timeout value in seconds for communication with the TACACS+ server. Range: 0 - 5000. Default: 3.

Example Command

```
set tacacs-server priority 1 ipv4-address 1.1.1.1 shared-secret
aaaaaaa timeout 50
```

show tacacs-servers

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Display all configured TACACS+ servers.

Syntax

```
show tacacs-servers
```

Parameters

Parameter	Description
priority	Priority of the server (integer): ■ 1 (primary) ■ 2 (secondary)
ipv4-address	The IP address of the TACACS+ server
tcp-port	The port number(integer) through which the TACACS+ server communicates with clients. Default: 49.
shared-secret	Pre-shared secret between the TACACS+ server and the appliance. A string that contains alphanumeric and special characters.
timeout	A timeout value in seconds (integer) for communication with the TACACS+ server. Default: 3 seconds

Example Command

```
HostName> show tacacs-servers
priority      ipv4-address    tcp-port    shared-secret    timeout
1             2.2.2.2         49          24312e33513......5
2             1.2.3.4         50          021d5c3b273      50
```

show tacacs-servers priority

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Show the details for a TACACS+ server with a specific priority.

See:

- *"show tacacs-servers" on page 886*
- *"set tacacs-server" on page 884*
- *"delete tacacs-server" on page 888*

Syntax

```
show tacacs-server priority {1 | 2}
```

Example Command

```
HostName> show tacacs-server priority 1

priority:                       1
ivp4-address:                   192.168.3.200
tcp-port:                       49
shared-secret                   78343c263a57
timeout:                        3
```

delete tacacs-server

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Delete a specific TACACS+ server with a specific priority.

See:

- *"set tacacs-server" on page 884*
- *"show tacacs-servers" on page 886*
- *"show tacacs-servers priority" on page 887*

Syntax

```
delete tacacs-server priority <priority>
```

Parameters

Parameter	Description
priority	Priority of the server (integer): ■ 1 (primary) ■ 2 (secondary)

Example Command

```
delete tacacs-server priority 1
```

Configuring NAS IP Address for RADIUS server

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure NAS IPv4 / IPv6 address for a RADIUS server authentication.

set global-radius-conf

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the NAS IPv4 / IPv6 address for RADIUS server authentication.

NAS IPv4 / 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-ipv4-address> ] [
nasIPV6 <nas-ipv6-address> ]
```

Parameters

Parameter	Description
nas-ipv4-address	NAS IPv4 address Type: IPv4 address
nas-ipv4-address	NAS IPv4 address Type: IPv6 address

Example Command

```
set global-radius-conf nas-ip-address 192.168.1.1 nasIPV6
0:0:0:0:0:ffff:c0a8:0101
```

show global-radius-conf

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the NAS IPv4 / IPv6 address for RADIUS server authentication.

Syntax

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

Example Command

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

Example Output

```
nas-ip-address:                 1.1.1.1
nasIPV6:                        2620:0:2a03:81::
```

Configuring Active Directory Server Objects

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Active Directory Server objects.

add ad-server

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new Active Directory server object.

Syntax

```
add ad-server domain <domain> ipv4-address <ipv4-address> ipv6-
address <ipv6-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
ipv6-address	Domain controller IPv6 address
password	The user's password A string that contains alphanumeric and special characters.

Parameter	Description
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 A string that contains up to 64 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '@' (at)

Example Command

```
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
```

set ad-server

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing Active Directory server object.

Syntax

```
set ad-server <domain> [ ipv4-address <ipv4-address> ] [ ipv6-
address <ipv6-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
ipv6-address	Domain controller IPv6 address
password	The user's password 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

Parameter	Description
username	A user name with administrator privileges to communicate with the AD server A string that contains up to 64 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '@' (at)

Example Command

```
set ad-server myHost.com ipv4-address 192.168.1.1 ipv6-address
ipv6addr 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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing Active Directory server object.

Syntax

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

Parameters

Parameter	Description
domain	Domain name Type: Host name

Example Command

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

show ad-server

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

show ad-servers

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows settings of all configured AD server objects.

Syntax

```
show ad-servers
```

Example Command

```
show ad-servers
```

Configuring Syslog Server

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Syslog server settings.

add syslog-server

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
name	System Log Server name A string of alphanumeric characters **with** a space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
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 Command

```
add syslog-server ipv4-address 192.168.1.1 port 8080 enabled true
name MySysLogServer sent-logs system-logs
```

add-syslog-server protocol tls

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new external syslog server for the TLS protocol.

Syntax

```
add syslog-server protocol tls
```

Example Command

```
add syslog-server protocol tls
```

set syslog-server name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
name	System Log Server name A string of alphanumeric characters **with** a space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
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 Command

```
set syslog-server name MySyslogServer ipv4-address 192.168.1.1
enabled true port 8080 sent-logs system-logs
```

set syslog-server ipv4-address

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
name	System Log Server name A string of alphanumeric characters **with** a space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
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 Command

```
set syslog-server ipv4-address 192.168.1.1 ipv4-address
192.168.1.1 enabled true name MySyslogServer port 8080 sent-logs
system-logs
```

delete syslog-server ipv4-address

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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

Example Command

```
delete syslog-server ipv4-address 192.168.1.1
```

delete syslog-server name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes a configured external syslog server by name.

Syntax

```
delete syslog-server name <name>
```

Parameters

Parameter	Description
name	Specifies the syslog server name. Press the TAB key to see the available options.

Example Command

```
delete syslog-server name MySyslogServer
```

show syslog-server name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration of an external syslog server by name.

Syntax

```
show syslog-server name <name>
```

Parameters

Parameter	Description
name	Specifies the syslog server name. Press the TAB key to see the available options.

Example Command

```
show syslog-server name MySyslogServer
```

show syslog-server ipv4-address

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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

Example Command

```
show syslog-server ipv4-address 192.168.1.1
```

show syslog-server all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration of all external syslog servers.

Syntax

```
show syslog-server all
```

Parameters

Parameter	Description
n/a	

Example Command

```
show syslog-server all
```

Configuring Dynamic Objects

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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.

Parameter	Description
<toIP>	Ending IPv4 address.

Example Command

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

Configuring Updatable Objects

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Updatable objects.

add updatable-object name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add an object to the table of imported updatable objects by name.

Syntax

```
add updatable-object name <name>
```

Parameters

Parameter	Description
name	The name of the updatable object. Type: String

Example Command

```
add updatable-object name Country
```

add access-rule outgoing source-updatable-object name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add access rule for updatable source and updatable destination by name, using only imported updatable objects.

Syntax

```
add access-rule type outgoing source-updatable-object name
<source-updatable-object-name> destination-updatable-object name
<destination-updatable-object-name> action accept
```

Parameters

Parameter	Description
source-updatable-object-name	Name of the imported updatable object used as source
destination-updatable-object-name	Name of the imported updatable object used as destination

Example Command

```
add access-rule type outgoing source-updatable-object name China
destination-updatable-object name Japan action accept
```

add access-rule outgoing source-updatable-object uid

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add access rule for updatable source and updatable destination by ID, using only imported updatable objects.

Syntax

```
add access-rule type outgoing source-updatable-object uid <source-
updatable-object-ID> destination-updatable-object uid
<destination-updatable-object-ID> action accept
```

Parameters

Parameter	Description
source-updatable-object-ID	ID of the imported updatable object used as source
destination-updatable-object-ID	ID of the imported updatable object used as destination

Example Command

```
add access-rule type outgoing source-updatable-object uid CP_GEO_
CN destination-updatable-object uid CP_GEO_JP action accept
```

delete updatable-object name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete an object from the table of imported updatable objects by name.

Syntax

```
delete updatable-object name <name>
```

Parameters

Parameter	Description
name	The name of the updatable object. Type: String

Example Command

```
delete updatable-object name Country
```

show updatable-object name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show details of the updatable object by name.

Syntax

```
show updatable-object name <object-name>
```

Parameters

Parameter	Description
<object-name>	The name of the updatable object.

Example Command

```
show updatable-object name Country
```

Example Output

```
uid: CP_GEO_IL
name: Israel
parent-uid: CP_GEO_ASIA
is-imported: true
```

show updatable-object uid

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show a single updatable object by ID.

Syntax

```
show updatable-object uid <uid>
```

Parameters

Parameter	Description
uid	The code name of the updatable object, as used in the Management Server.

Example Command

```
show updatable-object uid CP_GEO_IL
```

Example Output

```
uid:                                CP_GEO_IL
name:                               Israel
parent-uid:                         CP_GEO_ASIA
is-imported:                        true
```

show updatable-objects

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the list of all available updatable objects.

Syntax

```
show updatable-objects
```

Example Command

```
show updatable-objects
```

Example Output

```
name:                           Africa
uuid:                           d00802e8-0570-4851-8900-0a7c2ca80a9a
is-imported:                    false
uid:                            CP_GEO_AFRICA
parent-uid:
name:                           Burkina Faso
uuid:                           91dac46d-1d35-4f8c-b4a4-ac588325c9b7
is-imported:                    false
uid:                            CP_GEO_BF
parent-uid:                     CP_GEO_AFRICA
name:                           Burundi
uuid:                           e80e48ad-022b-4fec-88df-91164346513e
is-imported:                    false
uid:                            CP_GEO_BI
parent-uid:                     CP_GEO_AFRICA
```

show updatable-objects-imported

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows a list of all the imported updatable objects.

Syntax

```
show updatable-objects-imported
```

Example Command

```
show updatable-objects-imported
```

Example Output

```
name:                           Benin
uuid:                           96d9b816-3216-45c8-9446-c73380244bbd
is-imported:                    true
uid:                            CP_GEO_BJ
parent-uid:                     CP_GEO_AFRICA
name:                           Chad
uuid:                           11be095e-9343-47dc-aaed-2e2cb4ad2862
is-imported:                    true
uid:                            CP_GEO_TD
parent-uid:                     CP_GEO_AFRICA
name:                           Japan
uuid:                           3f615c4d-3d99-4b08-b4e1-cf6b3b2e73e1
is-imported:                    true
uid:                            CP_GEO_JP
parent-uid:                     CP_GEO_ASIA
```

Configuring IP Resolving

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure IP Resolving settings.

set ip-resolving

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure IP Resolving settings.

Syntax

```
set ip-resolving [ mode {on | off} ] [ ttl <ttl> ]
```

Parameters

Parameter	Description
mode	Enable / Disable IP Resolving logs enrichment.
ttl	The time (in seconds) for which the hostname resolution will be used. Limited to a range of 30-86400. A number with no fractional part (integer)

Example Command

```
set ip-resolving mode on ttl -3600
```

show ip-resolving

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show IP Resolving.

Syntax

```
show ip-resolving
```

Example Command

```
show ip-resolving
```

Example Output

```
HostName> show ip-resolving
mode: on
ttl: 1800
```

Configuring the Schedule for Software Blade Updates

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the schedule for Software Blade updates.

set blade-update-schedule

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 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 A number with no fractional part (integer)
recurrence	The recurrence of the updates - hourly, daily, weekly or monthly 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)

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

Example Command

```
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 advanced-settings max-num-of-retries

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for Software Blade updates.

Syntax

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

Example Command

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

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for Software Blade updates.

Syntax

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

Example Command

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

show blade-update-schedule

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of Software Blade updates schedule

Syntax

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

Example Command

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

show blade-update-schedule advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced settings of Software Blade updates schedule.

Syntax

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

Example Command

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

Configuring the Firewall Software Blade

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the Firewall Software Blade settings.

set fw policy mode / track

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

set fw policy advanced-settings blocked-packets-action

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Example Command

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

set fw policy advanced-settings log-implied-rules

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Example Command

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

set fw policy user-check accept

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 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 A string that contains only printable characters.
title	The title of an APPI 'Accept' user message A string that contains only printable characters.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that contains only printable characters.
confirm-text	This text appears next to the 'ignore warning' checkbox of an APPI 'Ask' user message 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 A string that contains only printable characters.
title	The title of an APPI 'Ask' user message A string that contains only printable characters.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 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 A string that contains only printable characters.
title	The title of an APPI 'Block' user message A string that contains only printable characters.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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. A string that contains only printable characters.
subject	The subject of the 'Block Device' user message A string that contains only printable characters.
title	The title of the 'Block Device' user message A string that contains only printable characters.

Example Command

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

set fw policy user-check block-infected-device

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that contains only printable characters.
subject	The subject of the 'Block Infected Device' user message A string that contains only printable characters.
title	The title of the 'Block Infected Device' user message A string that contains only printable characters.

Example Command

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

show fw policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configured policy for the Firewall blade.

Syntax

```
show fw policy
```

Parameters

Parameter	Description
n/a	

Example Command

```
show fw policy
```

show fw policy advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced settings for the Firewall blade.

Syntax

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

Example Command

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

show fw policy user-check

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press TAB to see available options

Example Command

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

Configuring Threat Prevention Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Threat Prevention settings.

threat-prevention-advanced

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

set threat-prevention-advanced

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set threat-prevention-advanced advanced-settings file-inspection-
size-kb 15000
```

show threat-prevention-advanced

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced settings for the Threat Prevention blades.

Syntax

```
show threat-prevention-advanced advanced-settings
```

Parameters

Parameter	Description
n/a	

Example Command

```
show threat-prevention-advanced advanced-settings
```

threat-prevention anti-bot

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

set threat-prevention anti-bot engine

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the engine settings of the Anti-Bot Software 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 Command

```
set threat-prevention anti-bot engine malicious-activity ask
reputation-domains ask reputation-ips ask reputation-urls ask
unusual-activity ask
```

set threat-prevention anti-bot policy mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the policy of the Anti-Bot blade.

Syntax

```
set threat-prevention anti-bot policy [ mode {true | false} ] [
detect-mode {true | false} ]
```

Parameters

Parameter	Description
detect-mode	Indicates if the Anti-Bot blade is set to 'Detect Only' mode
mode	Indicates if the Anti-Bot blade is active

Example Command

```
set threat-prevention anti-bot policy mode true detect-mode true
```

set threat-prevention anti-bot policy advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
res-class-mode	

Example Command

```
set threat-prevention anti-bot policy advanced-settings res-class-
mode rs-hold
```

set threat-prevention anti-bot user-check ask

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 {accept |
block} ] [ frequency {day | week | month} ] [ subject "<subject>"
] [ title "<title>" ] [ reason-displayed {true | false} ]
```

Parameters

Parameter	Description
activity-text	This text appears next to the 'ignore warning' checkbox of an Anti-Bot 'Ask' user message. A string that contains only printable characters.
body	The informative text that appears in the Anti-Bot 'Ask' user message. 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.
subject	The subject of an Anti-Bot 'Ask' user message. A string that contains only printable characters.
title	The title of an Anti-Bot 'Ask' user message. A string that contains only printable characters.

Example Command

```
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
```

set threat-prevention anti-bot user-check block

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 {true | false} ]
```

Parameters

Parameter	Description
body	The informative text that appears in the Anti-Bot 'Block' user message. 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.
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.
subject	The subject of an Anti-Bot 'Block' user message. A string that contains only printable characters.
title	The title of an Anti-Bot 'Block' user message. A string that contains only printable characters.

Example Command

```
set threat-prevention anti-bot user-check block body My Network
redirect-url "http://example.com" subject "My Network" title "My
Network" redirect-to-url true
```

show threat-prevention anti-bot engine

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the engine settings of the Anti-Bot blade.

Syntax

```
show threat-prevention anti-bot engine
```

Parameters

Parameter	Description
n/a	

Example Command

```
show threat-prevention anti-bot engine
```

show threat-prevention anti-bot policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the policy of the Anti-Bot blade.

Syntax

```
show threat-prevention anti-bot policy
```

Example Command

```
show threat-prevention anti-bot policy
```

show threat-prevention anti-bot policy advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the advanced settings of the Anti-Bot blade.

Syntax

```
show threat-prevention anti-bot policy advanced-settings
```

Example Command

```
show threat-prevention anti-bot policy advanced-settings
```

show threat-prevention anti-bot user-check ask

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show threat-prevention anti-bot user-check ask
```

show threat-prevention anti-bot user-check block

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
```

Example Command

```
show threat-prevention anti-bot user-check block
```

threat-prevention anti-virus

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

add threat-prevention anti-virus file-type

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)

Parameter	Description
extension	File extension that represents this file type A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)

Example Command

```
add threat-prevention anti-virus file-type extension "This is a
comment" action block description This is a comment
```

set threat-prevention anti-virus file-type

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)

Parameter	Description
extension	File extension that represents this file type A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '`(`' (opening round bracket) ■ '`)`' (closing round bracket) ■ ':' (colon) ■ '`@`' (at)

Example Command

```
set threat-prevention anti-virus file-type extension pdf action
block description "This is a comment"
```

set threat-prevention anti-virus engine

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set threat-prevention anti-virus engine urls-with-malware ask viruses ask
```

set threat-prevention anti-virus user-check block

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 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 A string that contains only printable characters.
title	The title of an Anti-Virus 'Block' user message A string that contains only printable characters.

Example Command

```
set threat-prevention anti-virus user-check block body My Network
redirect-url urlWithHttp subject My Network title My Network
redirect-to-url true
```

set threat-prevention anti-virus user-check ask

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that contains only printable characters.
body	The informative text that appears in the Anti-Virus 'Ask' user message 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 A string that contains only printable characters.
title	The title of an Anti-Virus 'Ask' user message A string that contains only printable characters.

Example Command

```
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
```

set threat-prevention anti-virus policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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)

Parameter	Description
scope	Indicates the source of scanned filed: Scan incoming files, or scan both incoming and outgoing files Options: incoming, incoming-and-outgoing

Example Command

```
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 advanced-settings action-when-nesting-level-exceeded

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set threat-prevention anti-virus policy advanced-settings action-
when-nesting-level-exceeded allow
```

set threat-prevention anti-virus policy advanced-settings file-scan-size-kb

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set threat-prevention anti-virus policy advanced-settings file-
scan-size-kb 15000
```

set threat-prevention anti-virus policy advanced-settings max-nesting-level

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set threat-prevention anti-virus policy advanced-settings max-
nesting-level 2
```

set threat-prevention anti-virus policy advanced-settings priority-scanning

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings of the Anti-Virus blade.

Syntax

```
set threat-prevention anti-virus policy advanced-settings
priority-scanning {true | false}
```

Parameters

Parameter	Description
n/a	

Example Command

```
set threat-prevention anti-virus policy advanced-settings
priority-scanning true
```

set threat-prevention anti-virus policy advanced-settings res-class-mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
res-class-mode	

Example Command

```
set threat-prevention anti-virus policy advanced-settings res-
class-mode rs-hold
```

delete threat-prevention anti-virus file-type

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)

Example Command

```
delete threat-prevention anti-virus file-type extension pdf
```

delete threat-prevention anti-virus file-type custom

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all manually configured custom file types.

Syntax

```
delete threat-prevention anti-virus file-type custom all
```

Parameters

Parameter	Description
n/a	

Example Command

```
delete threat-prevention anti-virus file-type custom all
```

show threat-prevention anti-virus engine

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the engine settings of the Anti-Virus blade.

Syntax

```
show threat-prevention anti-virus engine
```

Parameters

Parameter	Description
n/a	

Example Command

```
show threat-prevention anti-virus engine
```

show threat-prevention anti-virus file-type

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '`,`' (comma) ■ '`.`' (period) ■ '`-`' (minus) ■ '`(`' (opening round bracket) ■ '`)`' (closing round bracket) ■ '`:`' (colon) ■ '`@`' (at)

Example Command

```
show threat-prevention anti-virus file-type extension pdf
```

show threat-prevention anti-virus file-types

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show threat-prevention anti-virus file-types
```

show threat-prevention anti-virus policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the policy for the Anti-Virus blade.

Syntax

```
show threat-prevention anti-virus policy
```

Parameters

Parameter	Description
n/a	

Example Command

```
show threat-prevention anti-virus policy
```

show threat-prevention anti-virus policy advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced settings for the Anti-Virus blade.

Syntax

```
show threat-prevention anti-virus policy advanced-settings
```

Parameters

Parameter	Description
n/a	

Example Command

```
show threat-prevention anti-virus policy advanced-settings
```

show threat-prevention anti-virus user-check ask

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show threat-prevention anti-virus user-check ask
```

show threat-prevention anti-virus user-check block

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show threat-prevention anti-virus user-check block
```

threat-prevention exception

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

add threat-prevention exception

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new exception rule for Threat Prevention malware protection.

Note - The source and destination can be a network objects view or an updatable object, but not both.

Syntax

```
add threat-prevention exception [ destination <destination> |
<destination-updatable-object name>] | <destination-updatable-
object uid> ] [ destination-negate {true | false} ] [ service
<service> ] [ service-negate {true | false} ] [ source <source> |
<source-updatable-object name> | <source-updatable-object uid> ] [
source-negate {true | false} ] [ { protection-name <protection-
name> | [ protection-code <protection-code> ] | [ blade <blade> ]
} ] [ action <action> ] [ log <logging> ] [ 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

Parameter	Description
comment	Additional description for the exception A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
destination	Network object that is the target of the connection
destination-updatable-object name	A valid name of an updatable object, to be used as the destination
destination-updatable-object uid	A valid UID of an updatable object, to be used as the destination
destination-negate	If true, the destination is all traffic except what is defined in the destination field
log	The logging method used when there is a match on the rule: ■ `none` - Do not generate a log ■ `log` - Generate a log ■ `alert` - Generate a log with 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
source	IP address, network object or user group that the exception applies to

Parameter	Description
source-updatable-object name	A valid name of an updatable object, to be used as the source
source-updatable-object uid	A valid UID of an updatable object, to be used as the source
source negate	If true, the source is all traffic except what is defined in the source field

Example Command

```
add threat-prevention exception destination TEXT destination-
negate true service TEXT service-negate true source TEXT source-
negate true protection-name MyProtection action ask log none
comment "This is a comment"

add threat-prevention exception destination-updatable-object name
Greece source-updatable-object name Poland
```

set threat-prevention exception

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing exception rule for the Threat Prevention malware exceptions.

Note - The source and destination can be a network objects view or an updatable object, but not both.

Syntax

```
set threat-prevention exception <position> [ destination
<destination> | <destination-updatable-object name>] |
<destination-updatable-object uid> ] [ destination-negate {true |
false} ] [ service <service> ] [ service-negate {true | false} ] [
source <source> | <source-updatable-object name> | <source-
updatable-object uid> ] [ source-negate {true | false} ] [ {
protection-name <protection-name> | [ protection-code <protection-
code> ] | [ blade <blade> ] } ] [ action <action> ] [ log
<logging> ] [ 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

Parameter	Description
comment	Additional description for the exception A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ `','` (comma) ■ `'.'` (period) ■ `'-'` (minus) ■ `'(` (opening round bracket) ■ `')'` (closing round bracket) ■ `':'` (colon) ■ `'@'` (at)
destination	Network object that is the target of the connection
destination-updatable-object name	A valid name of an updatable object, to be used as the destination
destination-updatable-object uid	A valid UID of an updatable object, to be used as the destination
destination-negate	If true, the destination is all traffic except what is defined in the destination field
log	The logging method used when there is a match on the rule: ■ `none` - Do not generate a log ■ `log` - Generate a log ■ `alert` - Generate a log with 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
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

Parameter	Description
source	IP address, network object or user group that the exception applies to
source-updatable-object name	A valid name of an updatable object, to be used as the source
source-updatable-object uid	A valid UID of an updatable object, to be used as the source
source-negate	If true, the source is all traffic except what is defined in the source field

Example Command

```
set threat-prevention exception 2 destination TEXT destination-
negate true service http service-negate true source TEXT source-
negate true protection-name MyProtection action ask log none
comment "This is a comment"

set threat-prevention exception 3 destination-updatable-object
name Greece source-updatable-object name Poland
```

delete threat-prevention exception

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)

Example Command

```
delete threat-prevention exception name MyException
```

delete threat-prevention exceptions

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all existing malware exception rules for Anti-Virus, Anti-Bot and Threat Emulation (where applicable).

Syntax

```
delete threat-prevention exceptions all
```

Example Command

```
delete threat-prevention exceptions all
```

show threat-prevention exception

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
position	The order of the rule in comparison to other rules Type: Decimal number

Example Command

```
show threat-prevention exception position 3
```

Example Output

```
index: 3
source: Poland
source-negate: false
destination: Greece
destination-negate: false
service:
service-negate: false
protection: any
action: detect
disabled: false
log: log
comment:
```

threat-prevention ips

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

find threat-prevention ips protection

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)

Example Command

```
find threat-prevention ips protection CIFS
```

add threat-prevention ips network-exception

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Configures the comment text for the IPS Network exception. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
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

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 service is everything except what is defined in the service field Type: Boolean (true/false)

Example Command

```
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"
```

add threat-prevention ips network-exception protection-name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Configures the comment text for the IPS Network exception. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
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

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 service is everything except what is defined in the service field Type: Boolean (true/false)

Example Command

```
add threat-prevention ips network-exception protection-name
MyProtection destination TEXT destination-negate true service TEXT
service-negate true source TEXT source-negate true comment "This
is a comment"
```

set threat-prevention ips custom-default-policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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

Parameter	Description
disable-protocol-anomalies	Do not activate protocol anomaly detection signatures Type: Boolean (true/false)
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 Command

```
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
```

set threat-prevention ips network-exception position protection-name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 {true | false} ] [ service <service>] [
service-negate {true | false} ] [ source <source> ] [ source-
negate {true | false} ] [ comment "<comment>" ]
```

Parameters

Parameter	Description
comment	Configures the comment text for the IPS Network exception. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
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 fiel
position	The order of the rule in the Rule Base (a decimal number)
protection-name	Indicates if the exception rule will be matched on all IPS protections or a specific one

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
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

Example Command

```
set threat-prevention ips network-exception position 2 protection-
name MyProtection 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 position

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 {true | false} ] [ service <service> ]
[service-negate {true | false} ] [ source <source> ] [ source-
negate {true | false} ] [ comment "<comment>" ]
```

Parameters

Parameter	Description
comment	Configures the comment text for the IPS Network exception. A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
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
position	The order of the rule in the Rule Base (a 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

Parameter	Description
service-negate	If true, the service is everything except what is defined in the service field
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

Example Command

```
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 policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set threat-prevention ips policy mode true log none default-policy
MyTPpolicy detect-mode true
```

set threat-prevention ips protection-action-override protection-code

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set threat-prevention ips protection-action-override protection-
code 12345678 action prevent track none
```

set threat-prevention ips protection-action-override protection-code override-policy-action

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 {true | false}
```

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
protection-code	The IPS topic the override belongs to. Every override belongs to a single topic. Value between 4,503,599,627,370,495 and 4,503,599,627,370,495.

Example Command

```
set threat-prevention ips protection-action-override protection-
code 12345678 override-policy-action true
```

set threat-prevention ips protection-action-override protection-name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
track	Indicates the manually configured tracking option for this protection

Example Command

```
set threat-prevention ips protection-action-override protection-
name MyProtection action prevent track none
```

set threat-prevention ips protection-action-override protection-name override-policy-action

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 {true | false}
```

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
protection-name	Specifies the name of the IPS topic. Press the TAB key to see the available options.

Example Command

```
set threat-prevention ips protection-action-override protection-
name MyProtection override-policy-action true
```

delete threat-prevention ips network-exception position

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
delete threat-prevention ips network-exception position 2
```

delete threat-prevention ips network-exception all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all existing exception rules for the IPS blade.

Syntax

```
delete threat-prevention ips network-exception all
```

Parameters

Parameter	Description
n/a	

Example Command

```
delete threat-prevention ips network-exception all
```

show threat-prevention ips custom-default-policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of a custom IPS policy.

Syntax

```
show threat-prevention ips custom-default-policy
```

Parameters

Parameter	Description
n/a	

Example Command

```
show threat-prevention ips custom-default-policy
```

show threat-prevention ips network-exception

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show threat-prevention ips network-exception position 2
```

show threat-prevention ips policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the policy of the IPS blade.

Syntax

```
show threat-prevention ips policy
```

Example Command

```
show threat-prevention ips policy
```

show threat-prevention ips protection-action-override protection-code

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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. Value between 4,503,599,627,370,495 and 4,503,599,627,370,495.

Example Command

```
show threat-prevention ips protection-action-override protection-
code 12345678
```

show threat-prevention ips protection-action-override protection-name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Specifies the name of the IPS topic. Press the TAB key to see the available options.

Example Command

```
show threat-prevention ips protection-action-override protection-
name MyProtection
```

threat-prevention policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Shows commands relevant to Threat Prevention policy.

set threat-prevention policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the policy for the Threat Prevention blades Anti-Virus, Anti-Bot and Threat Emulation (where applicable).

Syntax

```
set threat-prevention policy [ track {alert | log | none} ] [
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 {true | false}
```

Parameters

Parameter	Description
profile	Unified policy profile
fail-mode	
track	Tracking options for Threat Prevention protections: ■ `alert` - Generate an alert ■ `log` - Generate a regular log ■ `none` - Do not track

Example Command

```
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
```

set threat-prevention policy advanced-settings allow-attack-stats

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Allow user to view attack statistics in the User Center account.

Syntax

```
set threat-prevention policy advanced-settings allow-attack-stats
{ true | false }
```

Prerequisite

This command requires the administrator to first run this command:

```
set privacy-settings advanced-settings customer-consent true
```

Note - There is an optional command to enable the real IP address information in the attack reports:

```
set threat-prevention policy advanced-settings allow-ipaddr-in-
stats true
```

Example Command

```
set threat-prevention policy advanced-settings allow-attack-stats
true
```

set threat-prevention policy advanced-settings allow-ipaddr-in-stats

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enable the real IP address information in the attack reports.

Syntax

```
set threat-prevention policy advanced-settings allow-ipaddr-in-
stats { true | false }
```

Prerequisite

Note - This command requires the administrator to first run these 2 commands:

```
set privacy-settings advanced-settings customer-consent true
```

```
set threat-prevention policy advanced-settings allow-attack-stats
true
```

Example Command

```
set threat-prevention policy advanced-settings allow-ipaddr-in-
stats true
```

show threat-prevention policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
```

Example Command

```
show threat-prevention policy
```

```
show threat-prevention policy advanced-settings
```

threat-prevention threat-emulation additional-remote-emulator

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

add threat-prevention threat-emulation additional-remote-emulator

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
name	Remote emulation gateway name A string of alphanumeric characters **with** a space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)

Example Command

```
add threat-prevention threat-emulation additional-remote-emulator
ip-address 192.168.1.1 name MyProtection
```

set threat-prevention threat-emulation additional-remote-emulator

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
name	Remote emulation gateway name A string of alphanumeric characters **with** a space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)

Example Command

```
set threat-prevention threat-emulation additional-remote-emulator
name "My Remote Emulator" ip-address 192.168.1.1
```

delete threat-prevention threat-emulation additional-remote-emulator ip-address

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Specifies the IP address of the remote emulation gateway

Example Command

```
delete threat-prevention threat-emulation additional-remote-
emulator ip-address 192.168.1.1
```

delete threat-prevention threat-emulation additional-remote-emulator name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Specifies the name of the remote emulation gateway. Press the TAB key to see the available options.

Example Command

```
delete threat-prevention threat-emulation additional-remote-
emulator name "My Remote Emulator"
```

show threat-prevention threat-emulation additional-remote-emulator

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show all gateways that are configured as additional (private) emulation gateways.

Syntax

```
show threat-prevention threat-emulation additional-remote-emulator
```

Example Command

```
show threat-prevention threat-emulation additional-remote-emulator
```

show threat-prevention threat-emulation additional-remote-emulator name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Specifies the name of the remote emulation gateway. Press the TAB key to see the available options.

Example Command

```
show threat-prevention threat-emulation additional-remote-emulator
name "My Remote Emulator"
```

threat-prevention threat-emulation

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

set threat-prevention threat-emulation file-type

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
extension	File extension that represents this file type A string of alphanumeric characters **without** space between them: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits)
file-type	The file type Press the TAB key to see the available options.

Example Command

```
set threat-prevention threat-emulation file-type pdf action bypass
description "This is a comment"
```

set threat-prevention threat-emulation policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures policy settings for the Threat Emulation blade (where applicable).

Syntax

```
set threat-prevention threat-emulation policy [ mode {true |
false} ] [ detect-mode {true | false} ] [ scope <scope> ] [
interfaces <interfaces> ] [ protocol-http {true | false} ] [
protocol-mail {true | false} ] [ 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
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
protocol-http	Indicates if file emulation will be performed on all configured ports of HTTP traffic
protocol-mail	Indicates if file emulation will be performed on mail traffic (SMTP)

Parameter	Description
scope	Indicates the source of scanned file: scan incoming files, or scan both incoming and outgoing files Options: incoming, incoming-and-outgoing

Example Command

```
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 advanced-settings connection-handling-mode-smtp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
connection-handling-mode-smtp	

Example Command

```
set threat-prevention threat-emulation policy advanced-settings
connection-handling-mode-smtp background
```

set threat-prevention threat-emulation policy protocol

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Disable or enable the ability to configure FTP protocol via Threat Emulation.

See *"show threat-prevention threat-emulation policy protocol-ftp" on page 1039*.

Syntax

```
set threat-prevention threat-emulation policy protocol-ftp { true
| false }
```

Parameters

Parameter	Description
protocol-ftp	■ To enable configuring FTP through Threat Emulation, set to `true`. ■ To disable configuring FTP through Threat Emulation, set to `false`.

Example Command

```
set threat-prevention threat-emulation policy protocol-ftp true
```

show threat-prevention threat-emulation file-type

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options.

Example Command

```
show threat-prevention threat-emulation file-type pdf
```

show threat-prevention threat-emulation file-types

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show threat-prevention threat-emulation file-types
```

show threat-prevention threat-emulation policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the policy of the Threat Emulation policy.

Syntax

```
show threat-prevention threat-emulation policy
```

Example Command

```
show threat-prevention threat-emulation policy
```

show threat-prevention threat-emulation policy advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced settings of the Threat Emulation policy.

Syntax

```
show threat-prevention threat-emulation policy advanced-settings
```

Example Command

```
show threat-prevention threat-emulation policy advanced-settings
```

show threat-prevention threat-emulation policy protocol-ftp

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Shows if FTP is configured via Threat Emulation.

See *"set threat-prevention threat-emulation policy protocol" on page 1034*.

Syntax

```
show threat-prevention threat-emulation policy protocol-ftp
```

Returned Values

Parameter	Description
`true`	FTP is configured through Threat Emulation.
`false`	FTP is not configured through Threat Emulation.

Example Command

```
HostName> show threat-prevention threat-emulation policy protocol-
ftp
protocol-ftp:                    true
```

threat-prevention whitelist

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

add threat-prevention whitelist mail

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
add threat-prevention whitelist mail email-address
MyEmail@mail.com type recipient
```

add threat-prevention whitelist type-file

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
add threat-prevention whitelist type-file md5
d41d8cd98f00b204e9800998ecf8427e
```

add threat-prevention whitelist type-url

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
add threat-prevention whitelist type-url url
http://somehost.example.com
```

set threat-prevention whitelist mail

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set threat-prevention whitelist mail MyEmail@mail.com type
recipient
```

delete threat-prevention whitelist mails

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
delete threat-prevention whitelist mails all
```

delete threat-prevention whitelist type-file md5

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
delete threat-prevention whitelist type-file md5
d41d8cd98f00b204e9800998ecf8427e
```

delete threat-prevention whitelist type-file all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Removes all excluded files for Threat Prevention blades.

Syntax

```
delete threat-prevention whitelist type-file all
```

Parameters

Parameter	Description
n/a	

Example Command

```
delete threat-prevention whitelist type-file all
```

delete threat-prevention whitelist type-url url

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
delete threat-prevention whitelist type-url url
http://somehost.example.com
```

delete threat-prevention whitelist type-url all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Removes all excluded URLs for Threat Prevention blades.

Syntax

```
delete threat-prevention whitelist type-url all
```

Example Command

```
delete threat-prevention whitelist type-url all
```

delete threat-prevention whitelist mail

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
delete threat-prevention whitelist mail MyEmail@mail.com
```

show threat-prevention whitelist mail

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show threat-prevention whitelist mail MyEmail@mail.com
```

show threat-prevention whitelist mails

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the whitelist email addresses set for the Threat Prevention blades.

Syntax

```
show threat-prevention whitelist mails
```

Parameters

Parameter	Description
n/a	

Example Command

```
show threat-prevention whitelist mails
```

show threat-prevention whitelist files

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show threat-prevention whitelist files
```

show threat-prevention whitelist urls

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the whitelist URLs set for the Threat Prevention blades.

Syntax

```
show threat-prevention whitelist urls
```

Parameters

Parameter	Description
n/a	

Example Command

```
show threat-prevention whitelist urls
```

set threat-prevention threat-emulation file-types-revert-actions-to-default

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set threat-prevention threat-emulation file-types-revert-actions-
to-default
```

show threat-prevention infected-hosts

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows a list of infected hosts detected by Threat Prevention blades.

Syntax

```
show threat-prevention infected-hosts
```

Parameters

Parameter	Description
n/a	

Example Command

```
show threat-prevention infected-hosts
```

cpssh

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

SSH deep packet inspection was integrated as part of the Quantum Spark code alignment to R81.10.

The cpssh_config command is used to configure the feature and enable SSH deep packet inspection.

When cpssh_config is used it sends signal USR1 to cpsshd and cpsshd is responsible to update settings in the kernel.

After the kernel is updated, whenever there is an incoming connection, it checks if cpsshd inspection is enabled and if it is, it starts inspecting traffic.

Note - SSH DPI is disabled by default.

Syntax

In Expert mode:

```
cppsh_config
```

Example Command

```
[Expert@gateway1234-53]# cpssh_config
CPSSH key-conf utility. This application assings ssh public
keyfiles (myname.pub) to origins.
Use: "cpssh_config -ORIGIN_TYPE -CMD ORIGIN public_key"
ORIGIN_TYPE should be server (s) or client (c)
In case you want to add a server key, the ORIGIN should be the
name of the server (example my_ssh_server.com or my_ssh_
server.com).
In case you want to add a client key, the ORIGIN should be the
[client name]@[client host] (example admin@my_ssh_server.com).
Example usage:
"cpssh_config -s -g my_ssh_server.com -e /home/admin/serv_key.pub
":
       Assigning servers public key serv_key.pub to server host: my_ssh_
server.com, the application will generate pair of RSA keys.
       (If the server host (my_ssh_server.com) already exists, the
application will fail)
"cpssh_config -c -f -g admin@my_ssh_server.com -e
/home/admin/client_key.pub -l /home/admin/serv_key.pub":
       Assigning client public key client_key.pub to client: admin@my_
ssh_server.com, and link it to server with public key: serv_
key.pub.
       The application will generate pair of RSA keys.
       (If the client (admin@my_ssh_server.com) already exists, the
application will overwrite it)
"cpssh_config -s -a my_ssh_server.com -e /home/admin/serv_key.pub
-i /home/admin/gwkey":
       Assigning servers public key serv_key.pub to server host: my_ssh_
server.com using gateway private key gwkey.
       (If the server host (my_ssh_server.com) already exists, the
application will fail)
"cpssh_config -c -f -a admin@my_ssh_server.com  -e
/home/admin/client_key.pub -l /home/admin/serv_key.pub -i
/home/admin/gwkey":
       Assigning client public key client_key.pub to client: admin@my_
ssh_server.com, and link it to server with public key: serv_
key.pub, using gateway keys gwkey.pub and gwkey.
       (If the client (admin@my_ssh_server.com) already exists, the
application will overwrite it)
"cpssh_config -s -r my_ssh_server.com": Remove server with IP my_
ssh_server.com
"cpssh_config -s -v my_ssh_server.com": view one server with IP:
my_ssh_server.com

Config options:
"cpssh_config -q": Show available config IDs, read current
```

```
configuration
"cpssh_config -w KeyExchange": Show configuration for KeyExchange
"cpssh_config -w Cipher -y aes128-cbc -u 0": Set Cipher aes128-cbc
to 0 (off)
"cpssh_config -h": Show help

Short Options:
"cpssh_config ion": Enable SSH Inspection
"cpssh_config ioff": Disable SSH Inspection
"cpssh_config istatus": Show status of SSH Inspection
[Expert@gateway1234]#
```

Configuring the Streaming Engine Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the streaming engine settings.

set streaming-engine-settings advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the streaming engine advanced 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>]
```

Example Command

```
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
```

set streaming-engine-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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

Parameter	Description
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
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 Command

```
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
```

show streaming-engine-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows streaming engine settings.

Syntax

```
show streaming-engine-settings
```

Example Command

```
show streaming-engine-settings
```

show streaming-engine-settings advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows streaming engine advanced settings.

Syntax

```
show streaming-engine-settings advanced-settings
```

Example Command

```
show streaming-engine-settings advanced-settings
```

Configuring User Awareness Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure User Awareness settings.

set user-awareness mode ad-queries-mode browser-based-authentication-mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the activation mode and user identification methods for the User Awareness Software Blade.

Syntax

```
set user-awareness [ mode {true | false} ] [ ad-queries-mode {true
| false} ] [ browser-based-authentication-mode {true | false} ]
```

Parameters

Parameter	Description
mode	Enables (true) or disables (false) the User Awareness mode
ad-queries-mode	Indicates if User Awareness seamlessly uses the AD Query to query the Active Directory servers to get user information
browser-based-authentication-mode	Indicates if User Awareness uses a Browser-Based Authentication portal to identify locally defined users or as a backup to other identification methods

Example Command

```
set user-awareness mode true ad-queries-mode true browser-based-
authentication-mode true
```

set user-awareness advanced-settings association-timeout

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the association timeout for the User Awareness Software Blade.

Syntax

```
set user-awareness advanced-settings association-timeout
<association-timeout>
```

Example Command

```
set user-awareness advanced-settings association-timeout 10
```

set user-awareness advanced-settings assume-single-user

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the single-user mode for the User Awareness Software Blade.

Syntax

```
set user-awareness advanced-settings assume-single-user {true |
false}
```

Example Command

```
set user-awareness advanced-settings assume-single-user true
```

set user-awareness browser-based-authentication

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 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

Parameter	Description
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 Press TAB to see available options
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 Command

```
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 add net-obj

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures a network object to be used in the User Awareness Software Blade.

See:

- *"set user-awareness browser-based-authentication remove net-obj" on page 1074*
- *"set user-awareness browser-based-authentication remove-all net-objs" on page 1075*

Syntax

```
set user-awareness browser-based-authentication add net-obj <net-obj>
```

Parameters

Parameter	Description
net-obj	Specifies the network object name. Press the TAB key to see the available options.

Example Command

```
set user-awareness browser-based-authentication add net-obj MyHost
```

set user-awareness browser-based-authentication remove net-obj

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Removes a network object from the User Awareness Software Blade configuration.

See:

- *"set user-awareness browser-based-authentication add net-obj" on page 1073*
- *"set user-awareness browser-based-authentication remove-all net-objs" on page 1075*

Syntax

```
set user-awareness browser-based-authentication remove net-obj
<net-obj>
```

Parameters

Parameter	Description
net-obj	Specifies the network object name. Press the TAB key to see the available options.

Example Command

```
set user-awareness browser-based-authentication remove net-obj
MyHost
```

set user-awareness browser-based-authentication remove-all net-objs

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Removes all network objects from the User Awareness Software Blade configuration.

See:

- *"set user-awareness browser-based-authentication add net-obj" on page 1073*
- *"set user-awareness browser-based-authentication remove net-obj" on page 1074*

Syntax

```
set user-awareness browser-based-authentication remove-all net-
objs
```

set user-awareness browser-based-authentication add excluded-sources-net-obj

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures a network object to be excluded from the User Awareness Software Blade.

See *"set user-awareness browser-based-authentication remove excluded-sources-net-obj" on the next page*.

Syntax

```
set user-awareness browser-based-authentication add excluded-
sources-net-obj <net-obj>
```

Parameters

Parameter	Description
net-obj	Specifies the network object name. Press the TAB key to see the available options.

Example Command

```
set user-awareness browser-based-authentication add excluded-
sources-net-obj MyHost
```

set user-awareness browser-based-authentication remove excluded-sources-net-obj

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Removes an excluded network object from the User Awareness Software Blade.

See *"set user-awareness browser-based-authentication add excluded-sources-net-obj" on the previous page*.

Syntax

```
set user-awareness browser-based-authentication remove excluded-
sources-net-obj <net-obj>
```

Parameters

Parameter	Description
net-obj	Specifies the network object name. Press the TAB key to see the available options.

Example Command

```
set user-awareness browser-based-authentication remove excluded-
sources-net-obj MyHost
```

set user-awareness identity-collector ipv4-address secret

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Configure the Identity Collector with the authorized client IPv4 address and secret.

See:

- *"set user-awareness identity-collector-mode" on page 1079*
- *"show user-awareness" on page 1080*
- *"show user-awareness identity-collector" on page 1083*

Syntax

```
set user-awareness identity-collector ipv4-address <ipv4-address>
secret <password>
```

Parameters

Parameter	Description
ipv4-address	The authorized Identity Collector client IPv4 address.
secret	The authorized Identity Collector client password.

Example Command

```
set user-awareness identity-collector ipv4-address 2.2.2.2 secret
1111111111
```

set user-awareness identity-collector-mode

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Enables turning on or off the Identity Collector tool for authentication.

See:

- *"set user-awareness identity-collector ipv4-address secret" on page 1078*
- *"show user-awareness" on page 1080*
- *"show user-awareness identity-collector" on page 1083*

Syntax

```
set user-awareness identity-collector-mode { on | off }
```

Parameters

Parameter	Description
identity-collector-mode	Turn the Identity Collector tool for authentication on or off

Example Command

```
set user-awareness identity-collector on
```

show user-awareness

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of the User Awareness Software Blade.

See *"show user-awareness identity-collector" on page 1083*.

Syntax

```
show user-awareness
```

Note - The line "`identity-collector-mode`" in the output appears starting from the R81.10.05 version.

Example Command

```
HostName> show user-awareness
mode:                                 false
ad-queries-mode:                      false
browser-based-authentication-mode:true
identity-collector-mode:              false
```

show user-awareness advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced settings of the User Awareness Software Blade.

Syntax

```
show user-awareness advanced-settings
```

Example Command

```
show user-awareness advanced-settings
```

show user-awareness browser-based-authentication

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the Browser-Based Authentication configuration of the User Awareness Software Blade.

Syntax

```
show user-awareness browser-based-authentication
```

Example Output

```
HostName> show user-awareness browser-based-authentication
destination-net-obj:          Montova-1
mode:                         false
redirect-upon-destinations:   manually-defined
redirect-upon-destination-internet:true
redirect-upon-destinations-net-objs:false
block-unauthenticated-non-web-traffic:false
portal-address:               <dynamic-ip>
session-timeout:              720
log-out-on-portal-close:      false
require-user-agreement:       false
agreement-text:
excluded-net-obj:             Montova-1
                              Montova-2
                              My-PC
```

show user-awareness identity-collector

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Show the authorized Identity Collector client with IPv4 address and secret.

See *"show user-awareness" on page 1080*.

Syntax

```
show user-awareness identity-collector
```

Example Command

```
show user-awareness identity-collector
client-name:                        1.2.3.4
secret:                             1111111111
```

Configuring Anti-Spoofing Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Anti-Spoofing settings.

set antispoofing advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

```
set antispoofing advanced-settings global-activation {true |
false}
```

Example Command

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

show antispoofing advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the Anti-Spoofing configuration.

Syntax

```
show antispoofing advanced-settings
```

Example Command

```
show antispoofing advanced-settings
```

Configuring Application Control Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

set application-control

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the default policy for the Application Control and URL Filtering Software 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)

Parameter	Description
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)
mode	Applications & URLs mode - true for on, false for off Type: Boolean (true/false)
set-limit	The limit, in kbps, for downloading 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 Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configured policy for the Application Control Software Blade.

Syntax

```
show application-control
```

Example Command

```
show application-control
```

show application-control other-undesired-applications

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
```

Example Command

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

Configuring Applications for Application Control

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure applications for Application Control.

add application application-name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

add application-url

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

set application application-name add url

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

set application application-name remove url

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

set application application-name add category

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

set application application-name remove category

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

set application application-name category regex-url

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

set application application-id add url

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A number with no fractional part (integer)
url	Application URL

Example Command

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

set application application-id remove url

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A number with no fractional part (integer)
url	Application URL

Example Command

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

set application application-id add category

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A number with no fractional part (integer)
category	Category name

Example Command

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

set application application-id remove category

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A number with no fractional part (integer)
category	Category name

Example Command

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

set application application-id category regex-url

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 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 Command

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

find application

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
find application TEXT
```

delete application application-name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

delete application application-id

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A number with no fractional part (integer)

Example Command

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

show application application-name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

show application application-id

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A number with no fractional part (integer)

Example Command

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

show applications

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows details of all applications.

Syntax

```
show applications
```

Parameters

Parameter	Description
n/a	

Example Command

```
show applications
```

Configuring Application Groups for Application Control

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure application groups for Application Control.

add application-group name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new group object for applications.

Syntax

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

Parameters

Parameter	Description
name	Application group name A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '`.`' (period) ■ '`-`' (minus) ■ '`&`' (ampersand)

Example Command

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

set application-group name add application-name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '&' (ampersand)

Example Command

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

set application-group name remove application-name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '&' (ampersand)

Example Command

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

set application-group name add application-id

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '&' (ampersand)

Example Command

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

set application-group name remove application-id

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '–' (minus) ■ '&' (ampersand)

Example Command

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

set application-group application-group-id add application-name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A number with no fractional part (integer)
application-name	Application or group name

Example Command

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

set application-group application-group-id remove application-name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A number with no fractional part (integer)
application-name	Application or group name

Example Command

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

set application-group application-group-id add application-id

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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

Example Command

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

set application-group application-group-id remove application-id

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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

Example Command

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

delete application-group name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '`.`' (period) ■ '`-`' (minus) ■ '`&`' (ampersand)

Example Command

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

delete application-group application-group-id

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A number with no fractional part (integer)

Example Command

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

show application-group application-group-id

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A number with no fractional part (integer)

Example Command

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

show application-group name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '`.`' (period) ■ '`-`' (minus) ■ '`&`' (ampersand)

Example Command

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

show application-groups

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of all specific application group objects.

Syntax

```
show application-groups
```

Parameters

Parameter	Description
n/a	

Example Command

```
show application-groups
```

Configuring Application Control Advanced Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the Application Control Software Blade's advanced engine settings.

set application-control-engine-settings advanced-settings fail-mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the Fail mode.

Syntax

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

Parameters

Parameter	Description
fail-mode	Fail-mode: ■ `allow-all-requests` - Allow all requests ■ `block-all-requests` - Blocks all requests

Example Command

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

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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>
```

Example Command

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

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures Application Control blade's advanced engine settings.

Syntax

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

Example Command

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

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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>
```

Example Command

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

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures Application Control blade's advanced engine settings.

Syntax

```
set application-control-engine-settings advanced-settings track-
browse-time {true | false}
```

<*track-browse-time*>

Example Command

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

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures Application Control blade's advanced engine settings.

Syntax

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

Example Command

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

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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>
```

Example Command

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

show application-control-engine-settings advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced settings of the Application Control Software Blade.

Syntax

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

Example Command

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

Configuring Anti-Spam Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Anti-Spam Software Blade and settings.

set antispam

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Configures policy and advanced settings for the Anti-Spam Software Blade.

set antispam

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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) A string of alphanumeric characters **with** a space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)

Parameter	Description
flag-suspected-spam-subject-stamp	Text to add to suspected spam emails subject (depends on action chosen for detected spam) A string of alphanumeric characters **with** a space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
log	Tracking options for spam emails: log, alert or none Options: none, log, alert
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 Command

```
set antispam mode on detection-method email-content log none
action-spam-email-content block flag-subject-stamp "This is spam"
detect-mode true specify-suspected-spam-settings true suspected-
spam-log none action-suspected-spam-email-content block flag-
suspected-spam-subject-stamp "This is suspected as spam"
```

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

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

Example Command

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

set antispam advanced-settings email-size-scan

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

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

Example Command

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

set antispam advanced-settings scan-outgoing

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

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

Example Command

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

set antispam advanced-settings spam-engine-timeout

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

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

Example Command

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

set antispam advanced-settings allow-mail-track

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

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

Example Command

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

set antispam advanced-settings transparent-proxy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

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

Example Command

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

set antispam advanced-settings ip-rep-timeout

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

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

Example Command

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

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced setting for the Anti-Spam blade.

Syntax

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

<*spam-engine-all-mail-track*>

Example Command

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

show antispam

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Shows the configured policy for the Anti-Spam Software Blade.

show antispam

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configured policy for the Anti-Spam blade.

Syntax

```
show antispam
```

Example Command

```
show antispam
```

show antispam advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

```
show antispam advanced-settings
```

Example Command

```
show antispam advanced-settings
```

antispam allowed-sender

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

add antispam allowed-sender ipv4-addr

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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

Example Command

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

add antispam allowed-sender sender-or-domain

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

delete antispam allowed-sender sender-or-domain

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

delete antispam allowed-sender ipv4-addr

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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

Example Command

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

delete antispam allowed-sender all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all existing Anti-Spam "allow" exceptions.

Syntax

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

Example Command

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

show antispam allowed-senders

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

```
show antispam allowed-senders
```

Example Command

```
show antispam allowed-senders
```

antispam blocked-sender

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

add antispam blocked-sender ipv4-addr

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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

Example Command

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

add antispam blocked-sender sender-or-domain

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

delete antispam blocked-sender sender-or-domain

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

delete antispam blocked-sender ipv4-addr

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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

Example Command

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

delete antispam blocked-sender all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all existing Anti-Spam "block" exceptions.

Syntax

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

Example Command

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

show antispam blocked-senders

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

```
show antispam blocked-senders
```

Example Command

```
show antispam blocked-senders
```

Configuring IPS Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the IPS Software Blade settings.

set ips engine-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
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 advanced-settings AboutConfigIPSErrorPageConfig

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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> ]
```

Example Command

```
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 advanced-settings AboutConfigIPSErrorPage

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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> ]
```

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows engine settings for the IPS blade.

Syntax

```
show ips engine-settings
```

Example Command

```
show ips engine-settings
```

show ips engine-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced engine settings for the IPS blade.

Syntax

```
show ips engine-settings advanced-settings
```

Parameters

Parameter	Description
n/a	

Example Command

```
show ips engine-settings advanced-settings
```

ips_filter

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Important:

- This command is intended only for Centrally Managed 1500 appliances.
- On Locally Managed 1500 appliances, you configure this feature in WebUI > **Device** > **Advanced Settings** > in the parameter "**IPS engine settings - Apply filter**".

Description

This command limits the number of IPS protections that can run on the appliance.

When this feature is enabled (this is the default), IPS protections consume less memory on the appliance.

Syntax

```
ips_filter { on | off }
```

Procedures

Enabling the IPS Filter

1. Connect to the command line on the appliance.
2. If your default shell is the Expert mode, go to Gaia Clish:

   ```
   clish
   ```

3. Enable the IPS Filter:

   ```
   ips_filter on
   ```

4. Go to the Expert mode:
   - If your default shell is the Expert mode, run:

     ```
     exit
     ```

   - If your default shell is Gaia Clish, run:

     ```
     expert
     ```

5. Examine the current state of the IPS Filter:

   ```
   pt ipsEngineSettings | grep applyIpsFilter
   ```

   The output must show:

   ```
   applyIpsFilter = true
   ```

Disabling the IPS Filter

1. Connect to the command line on the appliance.
2. If your default shell is the Expert mode, go to Gaia Clish:

   ```
   clish
   ```

3. Disable the IPS Filter:

   ```
   ips_filter off
   ```

4. Go to the Expert mode:
   - If your default shell is the Expert mode, run:

     ```
     exit
     ```

   - If your default shell is Gaia Clish, run:

     ```
     expert
     ```

5. Examine the current state of the IPS Filter:

   ```
   pt ipsEngineSettings | grep applyIpsFilter
   ```

   The output must show:

   ```
   applyIpsFilter = false
   ```

Configuring HTTPS Categorization Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure HTTPS categorization settings (categorization does not require a full SSL inspection mechanism).

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables and disables the validation of certificate expiration.

Syntax

```
set https-categorization advanced-settings validate-cert-
expiration {true | false}
```

Example Command

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

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables and disables the validation of unreachable CRLs.

Syntax

```
set https-categorization advanced-settings validate-unreachable-
crl {true | false}
```

Example Command

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

set https-categorization advanced-settings validate-crl

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables and disables the CRL validation.

Syntax

```
set https-categorization advanced-settings validate-crl {true |
false}
```

Example Command

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

show https-categorization

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration for HTTPS categorization feature.

Syntax

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

Example Command

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

set bypass-crl

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Bypass the CRL validation if the CRL contains more entries than the defined limit.

See *"show bypass-crl" on page 1214*.

Syntax

```
set bypass-crl bypassLargeCRL <VALUE>
```

Parameters

Parameter	Description
bypassLargeCRL	Configures the bypass limit. Default = 10000. To disable the bypass limit, configure the value 0.

Example Command

```
set bypass-crl bypassLargeCRL 999
```

show bypass-crl

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configured limit of entries in the CRL to bypass the CRL validation.

See *"set bypass-crl" on page 1213*.

Syntax

```
show bypass-crl
```

Configuring SSL Inspection Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure SSL Inspection settings.

ssl-inspection exception

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

add ssl-inspection exception

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add a new exception to bypass SSL Inspection policy for specific traffic.

Note - The source and destination can be a network objects view or an updatable object, but not both.

Syntax

```
add ssl-inspection exception [ source <source> | <source-
updatable-object name> | <source-updatable-object uid> ] [ source-
negate <source-negate> ] [ destination <destination> |
<destination-updatable-object name> | <destination-updatable-
object uid>] [ 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)

Parameter	Description
comment	Description of the rule A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
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)
destination-updatable-object name	A valid name of an updatable object, to be used as the destination.
destination-updatable-object uid	A valid UID of an updatable object, to be used as the destination.
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)
source-updatable-object name	A valid name of an updatable object, to be used as the source.

Parameter	Description
source-updatable-object uid	A valid UID of an updatable object, to be used as the source.
track	The action taken when there is a match on the rule. Values: `none`, `log`, `alert`

Example Command

```
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

add ssl-inspection exception destination-updatable-object name
Greece source-updatable-object name Poland
```

set ssl-inspection exception

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure an existing SSL Inspection policy exception.

See:

- *"add ssl-inspection exception" on page 1182*
- *"show ssl-inspection exception" on page 1190*

Note - The source and destination can be a network objects view or an updatable object, but not both.

Syntax

```
set ssl-inspection exception position  <position> [ source
<source>| <source-updatable-object name> | <source-updatable-
object uid> ]
] [ source-negate <source-negate> ] [ destination <destination> |
<destination-updatable-object name> | <destination-updatable-
object uid>] [
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)

Parameter	Description
comment	Description of the rule A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
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)
destination-updatable-object name	A valid name of an updatable object, to be used as the destination
destination-updatable-object uid	A valid UID of an updatable object, to be used as the destination
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
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-updatable-object name	A valid name of an updatable object, to be used as the source
source-updatable-object uid	A valid UID of an updatable object, to be used as the source

Parameter	Description
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 Values: `none`, `log`, `alert`

Example Command

```
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

set ssl-inspection exception position 5 destination-updatable-
object name Greece source-updatable-object name Poland
```

delete ssl-inspection exception position

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
delete ssl-inspection exception position 2
```

delete ssl-inspection exception all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete all existing SSL Inspection policy exceptions.

Syntax

```
delete ssl-inspection exception all
```

Example Command

```
delete ssl-inspection exception all
```

show ssl-inspection exception

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the configuration of a specific SSL Inspection policy exception.

See:

- *"add ssl-inspection exception" on page 1182*
- *"set ssl-inspection exception" on page 1185*

Syntax

```
show ssl-inspection exception position <position> position
<position>
```

Parameters

Parameter	Description
position	The index of exception Type: Decimal number

Example Command

```
show ssl-inspection exception position 5
```

Example Output

```
index: 5
source: Poland
source-negate: false
destination: Greece
destination-negate: false
service:
service-negate: false
category:
category-negate: false
disabled: false
track: log
comment:
```

show ssl-inspection exceptions

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show ssl-inspection exceptions position 2
```

ssl-inspection policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

add ssl-inspection policy inspect-asset type

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Allows you to add assets to the list of other assets.

See also: *"delete ssl-inspection policy inspect-asset type" on page 1206*

Syntax

```
add ssl-inspection policy inspect-asset-type <assets_name>
```

Parameters

Parameter	Description
assets_name	Name of the asset to add to the list of assets. Press the TAB key to see the available options.

Example Command

```
add ssl-inspection policy inspect-asset-type cloud
```

Press the TAB key to see the available options.

Examples of these include:

- Sensor
- Health Monitor Mode Sprinkler
- Scanner
- Smart device

set ssl-inspection policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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)

Parameter	Description
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)
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 Command

```
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 bypass-mac-os

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Lets the user change the MacOS checkbox status and its action.

Syntax

```
set ssl-inspection policy bypass-mac-os { true | false }
```

Parameters

Parameter	Description
bypass-mac-os	Enables (true) or disables (false)

Example Command

```
set ssl-inspection policy bypass-mac-os false
```

set ssl-inspection policy https-categorization-only-mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set ssl-inspection policy https-categorization-only-mode true
```

set ssl-inspection policy inspect-all-assets

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Lets the user change the relevant checkbox status and its action regarding SSL Policy inspection according to device type. In this case: device type is type 'all assets'.

Syntax

```
set ssl-inspection policy inspect-all-assets
```

Parameters

Parameter	Description
inspect-all-assets	Enables (true) or disables (false)

Example Command

```
set ssl-inspection policy inspect-all-assets false
```

set ssl-inspection policy inspect-computer-assets

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Change the relevant checkbox status and its action regarding SSL Policy inspection according to device type.

In this case, the device type is type 'computer assets'.

Syntax

```
set ssl-inspection policy inspect-computer-assets { true | false }
```

Parameters

Parameter	Description
inspect-computer-assets	Enables (true) or disables (false)

Example Command

```
set ssl-inspection policy inspect-computer-assets true
```

set ssl-inspection policy inspect-desktop-assets

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Lets the user change the relevant checkbox status and its action regarding SSL Policy inspection according to device type. In this case: device type is type 'desktop assets'.

Syntax

```
set ssl-inspection policy inspect-desktop-assets
```

Parameters

Parameter	Description
inspect -desktop-assets	Enables (true) or disables (false)

Example Command

```
set ssl-inspection policy inspect-desktop-assets true
```

set ssl-inspection policy inspect-https-protocol

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set ssl-inspection policy inspect-https-protocol true
```

set ssl-inspection policy inspect-imaps-protocol

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set ssl-inspection policy inspect-imaps-protocol true
```

set ssl-inspection policy inspect-laptop-assets

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Lets the user change the relevant checkbox status and its action regarding SSL Policy inspection according to device type. In this case: device type is type 'laptop assets'.

Syntax

```
set ssl-inspection policy inspect-laptop-assets
```

Parameters

Parameter	Description
inspect-laptop-assets	enables (true) or disables (false)

Example Command

```
set ssl-inspection policy inspect-laptop-assets false
```

set ssl-inspection policy inspect-other-assets

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Lets the user change the relevant checkbox status and its action regarding SSL Policy inspection according to device type. In this case: device type is type 'other assets'.

Syntax

```
set ssl-inspection policy inspect-other-assets
```

Parameters

Parameter	Description
inspect-other-assets	enables (true) or disables (false)

Example Command

```
set ssl-inspection policy inspect-other-assets true
```

show ssl-inspection policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show command allows the user to check the status of the SSL Inspection policy.

The parameter is true or false which represents the relevant checkbox.

See:

Syntax

```
show ssl-inspection policy
```

Parameters

Parameter	Description
n/a	

Example Command

```
show ssl-inspection policy
```

Example Output

```
mode:                          on
https-categorization-only-mode:off
inspect-https-protocol:        true
inspect-imaps-protocol:        false
inspect-pop3s-protocol:        false
inspect-desktop-assets:        true
inspect-laptop-assets:         true
inspect-other-assets:          true
bypass-mac-os:                 false
log-policy-bypass-traffic:     false
log-inspected-traffic:         false
```

```
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:false
bypass-untrusted-wireless-ssl-inspection:true
bypass-well-known-update-services:true
enable-wireless-bypass-logs:  false
```

delete ssl-inspection policy inspect-asset type

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Allows you to delete assets from the list of other assets.

See also: *"add ssl-inspection policy inspect-asset type" on page 1192*

Syntax

```
delete ssl-inspection policy inspect-asset-type <asset_name>
```

Parameters

Parameter	Description
asset_name	Name of the asset to delete

Example Command

```
delete ssl-inspection policy inspect-asset-type cloud
```

Press Enter to show all properties.

Examples of these include:

- Sensor
- Health monitor
- Sprinkler
- Scanner
- Smart device

ssl-inspection-trusted-ca-certificate

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Configure the settings for the SSL Inspection Trusted CA certificate.

add ssl-inspection trusted-ca-certificate

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add an SSL Inspection Trusted CA certificate.

Syntax

```
add ssl-inspection trusted-ca-certificate cert-base64-encoding
<cert-base64-encoding>
```

Parameters

Parameter	Description
<cert-base64-encoding>	The Base64 string of the certificate file in the CRT format (after it was converted to the Base64 format). Use any Base64 encoding tool (for example, the `base64` command on Linux OS) to convert your certificate file in the CRT format to the Base64 string.

Example Command

1. Convert the CRT file to the Base64 string using the Linux `base64` command (output is truncated):

   ```
   > base64 example_cert.crt | tr -d "\n\r"
   HNaeENSdHpYRGU1REI0N204...0tCg==
   ```

2. Add the SSL Inspection Trusted CA certificate (truncated):

   ```
   add ssl-inspection trusted-ca-certificate cert-base64-encoding
   HNaeENSdHpYRGU1REI0N204...0tCg==
   ```

set ssl-inspection trusted-ca-certificate

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Set an SSL Inspection Trusted CA certificate.

Syntax

```
set ssl-inspection trusted-ca-certificate uid <uid> enabled
<enabled>
```

Parameters

Parameter	Description
enabled	Enabled Type: Boolean (true/false)
uid	Unique Identifer Type: String

Example Command

```
set ssl-inspection trusted-ca-certificate uid TEXT enabled true
```

delete ssl-inspection trusted-ca-certificate

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete an SSL Inspection Trusted CA certificate.

Syntax

```
delete ssl-inspection trusted-ca-certificate uid <uid>
```

Parameters

Parameter	Description
uid	Unique Identifier Type: String

Example Command

```
delete ssl-inspection trusted-ca-certificate uid TEXT
```

show ssl-inspection trusted-ca-certificate

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the SSL Inspection Trusted CA certificates.

Syntax

```
show ssl-inspection trusted-ca-certificates
```

Example Command

```
show ssl-inspection trusted-ca-certificates
```

Example Output

```
HostName> show ssl-inspection trusted-ca-certificates
uid                                     issuer
                 issued-to
expiration-date                         enabled
5066AECC-3ADA-4702-AA3F-EE2FB495E25E    Hotspot 2.0 Trust Root
CA - 03            Hotspot 2.0 Trust Root CA - 03
12/08/2043 12:00:00 PM                  true
9DD6CB72-AE62-4939-8D63-D2155ED945B7    OISTE WISeKey Global
Root GB CA           OISTE WISeKey Global Root GB CA
12/01/2039 03:10:31 PM                  true
... ... (truncated for brevity) ... ...
39BF1C37-C771-40C0-A9C8-ACD2F2202FC5    Autoridade Certificadora
Raiz Brasile...  Autoridade Certificadora Raiz Brasile...
7/29/2021 7:17:10 PM                    true
8B91B839-D876-4230-B809-9337EBB313CF    OU=sigov-ca, O=state-
institutions, C=si   OU=sigov-ca, O=state-institutions, C=si
1/10/2021 2:22:52 PM                    true
HostName>
```

set ssl-inspection advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure advanced settings for SSL Inspection.

Syntax

```
set ssl-inspection advanced-settings [ bypass-well-known-update-
services {true | false} ] [ validate-crl <validate-crl> ] [
validate-cert-expiration {true | false} ] [ validate-unreachable-
crl {true | false} ] [ track-validation-errors {none | alert |
log} ] [ retrieve-intermediate-ca-certificate {true | false} ] [
log-empty-ssl-connections {true | false} ] [ additional-https-
ports <additional-https-ports> ] [ validate-untrusted-certificates
<validate-untrusted-certificates>]
```

Parameters

Parameter	Description
additional-https-ports	Configures additional HTTPS ports for SSL inspection (a comma separated list of ports or port ranges. See *IANA Service Name and Port Number Registry*.
bypass-well-known-update-services	Controls whether to bypass (`true`) or not (`false`) the SSL Inspection of traffic to well known software update services.
log-empty-ssl-connections	Controls whether to log (`true`) or not (`false`) the connections that were terminated by the client before data was sent (which might indicate the client did not install CA certificate).
retrieve-intermediate-ca-certificate	Controls whether to validate (`true`) or not (`false`) all intermediate CA certificates in the certificate chain.
track-validation-errors	Configures how to track the SSL Inspection validation: ▪ `none` - Do not track ▪ `log` - Generate a regular log ▪ `alert` - Generate an alert log

Parameter	Description
validate-cert-expiration	Controls whether to drop (`true`) or not (`false`) connections that present an expired certificate.
validate-crl	Controls whether to drop (`true`) or not (`false`) connections that present a revoked certificate.
validate-unreachable-crl	Controls whether to drop (`true`) or not (`false`) connections that present a certificate with an unreachable CRL.
validate-untrusted-certificates	Controls whether to drop (`true`) or not (`false`) connections that present an untrusted server certificate.

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show advanced settings for SSL Inspection.

Syntax

```
show ssl-inspection advanced-settings
```

Example Command

```
show ssl-inspection advanced-settings
```

set bypass-crl

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Bypass the CRL validation if the CRL contains more entries than the defined limit.

See *"show bypass-crl" on page 1214*.

Syntax

```
set bypass-crl bypassLargeCRL <VALUE>
```

Parameters

Parameter	Description
bypassLargeCRL	Configures the bypass limit. Default = 10000. To disable the bypass limit, configure the value 0.

Example Command

```
set bypass-crl bypassLargeCRL 999
```

show bypass-crl

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configured limit of entries in the CRL to bypass the CRL validation.

See *"set bypass-crl" on page 1213*.

Syntax

```
show bypass-crl
```

cipher_util

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Allows the user to configure the ciphers for SSL Inspection and Multi portal.

Syntax

In Expert mode, run:

```
cipher_util
```

You get these options:

```
Which blade would you like to configure?
(1)         SSL Inspection
(2)         Multi Portal

Select Option
(1)                 Print Configuration by Priority
(2)                 Enable Ciphers
(3)                 Disable Ciphers
(4)                 Re-Order Enabled Ciphers Priority
(Q)                 Quit
```

Parameters

Parameter	Description
Print Configuration by Priority	Prints all the ciphers that are enabled by priority (by default or by option 4) and also the disabled ciphers.
Enable Ciphers	Enable the use of ciphers for SSL Inspection / Multi Portal.
Disable Ciphers	Disable the use of ciphers for SSL Inspection / Multi Portal.
Re-order Enabled Ciphers Priority	You can prioritize the ciphers by any order you wish. **Note** - You must fill the entire enabled ciphers before you can change the order of priority.
Quit	Quit the tool.

Configuring Stateful Inspection Parameters

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure advanced parameters for Stateful Inspection.

set stateful-inspection advanced-settings allow-ipv6

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to inspect or not IPv6 traffic.

Syntax

```
set stateful-inspection advanced-settings allow-ipv6 {true |
false}
```

Parameters

Parameter	Description
allow-ipv6	Allows (`true`) or denies (`false`) the IPv6 traffic to pass without inspection. The default is `false`.

Example Command

```
set stateful-inspection advanced-settings allow-ipv6 false
```

set stateful-inspection advanced-settings tcp-timeout

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the timeout (in seconds) for TCP virtual sessions.

The default is 3600 seconds.

Syntax

```
set stateful-inspection advanced-settings tcp-timeout 60-86400
```

Example Command

```
set stateful-inspection advanced-settings tcp-timeout 1800
```

set stateful-inspection advanced-settings tcp-end-timeout

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the timeout (in seconds) for TCP session end.

The default is 20 seconds.

Syntax

```
set stateful-inspection advanced-settings tcp-end-timeout 2-3600
```

Example Command

```
set stateful-inspection advanced-settings tcp-end-timeout 2
```

set stateful-inspection advanced-settings tcp-start-timeout

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the timeout (in seconds) for TCP session start.

The default is 25 seconds.

Syntax

```
set stateful-inspection advanced-settings tcp-start-timeout 5-3600
```

Example Command

```
set stateful-inspection advanced-settings tcp-start-timeout 5
```

set stateful-inspection advanced-settings udp-timeout

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the timeout (in seconds) for UDP virtual sessions.

The default is 40 seconds.

Syntax

```
set stateful-inspection advanced-settings udp-timeout 10-3600
```

Example Command

```
set stateful-inspection advanced-settings udp-timeout 20
```

set stateful-inspection advanced-settings icmp-timeout

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the timeout (in seconds) for ICMP virtual sessions.

The default is 30 seconds.

Syntax

```
set stateful-inspection advanced-settings icmp-timeout 10-3600
```

Example Command

```
set stateful-inspection advanced-settings icmp-timeout 10
```

set stateful-inspection advanced-settings other-timeout

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the timeout (in seconds) for IP virtual sessions other than TCP, UDP, and ICMP.

The default is 60 seconds.

Syntax

```
set stateful-inspection advanced-settings other-timeout 10-3600
```

Example Command

```
set stateful-inspection advanced-settings other-timeout 30
```

set stateful-inspection advanced-settings udp-reply

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to accept or drop stateful UDP replies for unknown services.

Syntax

```
set stateful-inspection advanced-settings udp-reply {true | false}
```

Parameters

Parameter	Description
udp-reply	Accept (`true`) or drops (`false`) the stateful UDP replies for unknown services. The default is `true`.

Example Command

```
set stateful-inspection advanced-settings udp-reply false
```

set stateful-inspection advanced-settings icmp-reply

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to accept or drop ICMP Reply packets for ICMP Request packets that were accepted by the Security Policy.

Syntax

```
set stateful-inspection advanced-settings icmp-reply {true |
false}
```

Parameters

Parameter	Description
icmp-reply	Accept (`true`) or drops (`false`) the ICMP Reply packets. The default is `true`.

Example Command

```
set stateful-inspection advanced-settings icmp-reply true
```

set stateful-inspection advanced-settings other-reply

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to accept or drop stateful IP replies for unknown services other than TCP, UDP, and ICMP.

Syntax

```
set stateful-inspection advanced-settings other-reply {true |
false}
```

Parameters

Parameter	Description
allow-ipv6	Allows (`true`) or denies (`false`) the IP replies. The default is `true`.

Example Command

```
set stateful-inspection advanced-settings other-reply true
```

set stateful-inspection advanced-settings fw-allow-out-of-state-tcp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to drop or accept the out-of-state TCP packets.

Syntax

```
set stateful-inspection advanced-settings fw-allow-out-of-state-
tcp {0 | 1}
```

Parameters

Parameter	Description
fw-drop-out-of-state-icmp	Accepts (`1`) or drops (`0`) the out-of-state TCP packets. The default is `0`.

Example Command

```
set stateful-inspection advanced-settings fw-allow-out-of-state-
tcp 1
```

set stateful-inspection advanced-settings fw-drop-out-of-state-icmp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to drop or accept the out-of-state ICMP packets.

Syntax

```
set stateful-inspection advanced-settings fw-drop-out-of-state-
icmp {0 | 1}
```

Parameters

Parameter	Description
fw-drop-out-of-state-icmp	Drops (`1`) or accepts (`0`) the out-of-state ICMP packets. The default is `1`.

Example Command

```
set stateful-inspection advanced-settings fw-drop-out-of-state-
icmp 1
```

set stateful-inspection advanced-settings fw-log-out-of-state-tcp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to generate logs for out-of-state TCP packets.

Syntax

```
set stateful-inspection advanced-settings fw-log-out-of-state-tcp
{0 | 1}
```

Parameters

Parameter	Description
fw-log-out-of-state-tcp	Enables (`1`) or disables (`0`) the logging of out-of-state TCP packets. The default is `0`.

Example Command

```
set stateful-inspection advanced-settings fw-log-out-of-state-tcp
1
```

set stateful-inspection advanced-settings fw-log-out-of-state-icmp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to generate logs for out-of-state ICMP packets.

Syntax

```
set stateful-inspection advanced-settings fw-log-out-of-state-icmp
{0 | 1}
```

Parameters

Parameter	Description
fw-log-out-of-state-icmp	Enables (`1`) or disables (`0`) the logging of out-of-state ICMP packets. The default is `0`.

Example Command

```
set stateful-inspection advanced-settings fw-log-out-of-state-icmp
1
```

set stateful-inspection advanced-settings icmp-errors

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to accept or drop ICMP Error packets, which refer to another non-ICMP connection that was accepted by the Security Policy.

Syntax

```
set stateful-inspection advanced-settings icmp-errors {true |
false}
```

Parameters

Parameter	Description
icmp-errors	Accept (`true`) or drops (`false`) the ICMP Error packets. The default is `true`.

Example Command

```
set stateful-inspection advanced-settings icmp-errors true
```

set stateful-inspection advanced-settings dpi-lan-lan

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to perform deep packet inspection on traffic between LAN networks.

Syntax

```
set stateful-inspection advanced-settings dpi-lan-lan {true |
false}
```

Parameters

Parameter	Description
dpi-lan-lan	Enables (`true`) or disables (`false`) the deep packet inspection. The default is `false`.

Example Command

```
set stateful-inspection advanced-settings dpi-lan-lan false
```

set stateful-inspection advanced-settings dpi-lan-dmz

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to perform deep packet inspection on traffic between LAN and DMZ networks.

Syntax

```
set stateful-inspection advanced-settings dpi-lan-dmz{true |
false}
```

Parameters

Parameter	Description
dpi-lan-dmz	Enables (`true`) or disables (`false`) the deep packet inspection. The default is `true`.

Example Command

```
set stateful-inspection advanced-settings dpi-lan-dmz true
```

set stateful_inspection advanced-settings traceroute-max-ttl

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the maximal TTL value for traceroute packets.

The default TTL is 29.

Syntax

```
set stateful-inspection advanced-settings traceroute-max-ttl 0-64
```

Example Command

```
set stateful-inspection advanced-settings traceroute-max-ttl 30
```

show stateful-inspection advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configured stateful inspection advanced settings.

Syntax

```
show stateful-inspection advanced-settings
```

Example Output

```
HostName> show stateful-inspection advanced-settings
tcp-end-timeout:              20
other-timeout:                60
icmp-reply:                   true
dpi-lan-dmz:                  true
tcp-timeout:                  3600
udp-timeout:                  40
other-reply:                  true
fw-allow-out-of-state-tcp:    0
fw-log-out-of-state-tcp:      0
udp-reply:                    true
traceroute-max-ttl:           29
allow-ipv6:                   false
icmp-errors:                  true
fw-drop-out-of-state-icmp:    true
icmp-timeout:                 30
dpi-lan-lan:                  false
tcp-start-timeout:            25
fw-log-out-of-state-icmp:     0

HostName>
```

Configuring Aggressive Aging

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Aggressive Aging.

Aggressive Aging is designed to optimize how the appliance is dealing with a large connection number by aggressively reducing the timeout of existing connections when necessary.

set aggressive-aging

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A number with no fractional part (integer)
connt-mem-high- watermark-pct	Memory consumption percentage limit A number with no fractional part (integer)
general	Enable aggressive aging of connections Type: Boolean (true/false)
icmp-timeout	ICMP connections reduced timeout 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

Parameter	Description
memory-conn-status	Choose when aggressive aging timeouts are enforced Options: both, connections, memory
other-timeout	Other IP protocols reduced timeout 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 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 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 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 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 A number with no fractional part (integer)
udp-timeout-enable	Enable reduced timeout for UDP connections Type: Boolean (true/false)

Example Command

```
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 advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for aggressive aging.

The aggressive aging mechanism closes the connections and removes them from the kernel tables when the specified conditions are met.

Syntax

```
set aggressive-aging advanced-settings connections
      [ general { true | false } ]
      [ connt-limit-high-watermark-pct 0-100 ]
      [ connt-mem-high-watermark-pct 0-100 ]
      [ tcp-timeout-enable { false | true [ tcp-timeout 0-
4294967295 ] } ]
      [ tcp-start-timeout-enable { false | true [ tcp-start-
timeout 0-4294967295 ] } ]
      [ tcp-end-timeout-enable { false | true [ tcp-end-timeout 0-
4294967295 ] } ]
      [ udp-timeout-enable { false | true [ udp-timeout 0-
4294967295 ]
      [ icmp-timeout-enable { false | true [ icmp-timeout 0-
4294967295 ] } ]
      [ pending-timeout-enable { false | true [ pending-timeout 0-
4294967295 } ]
      [ other-timeout-enable { false | true [ other-timeout 0-
4294967295 ] } ]
      [ memory-conn-status { connections | memory | both } ]
      [ log { log | none } ]
```

Parameters

Parameter	Description
general	Enables (`true`) or disables (`false`) the aggressive aging of connections
connt-limit-high-watermark-pct	Configures the connection table percentage limit (between 0 and 100%)
connt-mem-high-watermark-pct	Configures the memory consumption percentage limit (between 0 and 100%)
tcp-timeout-enable	Enables (`true`) or disables (`false`) the timeout for TCP sessions
tcp-timeout	Configures the TCP session timeout (between 0 and 4294967295 seconds)
tcp-start-timeout-enable	Enables (`true`) or disables (`false`) the timeout for TCP handshakes
tcp-start-timeout	Configures the TCP handshake timeout (between 0 and 4294967295 seconds)
tcp-end-timeout-enable	Enables (`true`) or disables (`false`) the timeout for TCP terminations
tcp-end-timeout	Configures the TCP termination timeout (between 0 and 4294967295 seconds)
udp-timeout-enable	Enables (`true`) or disables (`false`) the virtual session timeout for UDP connections
udp-timeout	Configures the UDP connections virtual session timeout (between 0 and 4294967295 seconds)
icmp-timeout-enable	Enables (`true`) or disables (`false`) the virtual session timeout for ICMP connections
icmp-timeout	Configures the ICMP connections virtual session timeout (between 0 and 4294967295 seconds)
other-timeout-enable	Enables (`true`) or disables (`false`) the virtual session timeout for non-TCP/UDP/ICMP connections

Parameter	Description
other-timeout	Configures the virtual session timeout (between 0 and 4294967295 seconds) for non-TCP/UDP/ICMP connections
pending-timeout-enable	Enables (`true`) or disables (`false`) the timeout connections that are pending data
pending-timeout	Configures the timeout (between 0 and 4294967295 seconds) for connections that are pending data
memory-conn-status	Configures when aggressive aging timeouts are enforced: ■ `connections` - When the number of connections reaches the configured threshold ■ `memory` - When memory consumption reaches the configured threshold ■ `both` - When both the number of connections and memory consumption reach the configured thresholds
log	Configures whether to generate a log (`log`) or not (`none`) for aggressive aging events

Note - The value 4294967295 is 2^{32}-1.

Example Command

```
set aggressive-aging advanced-settings connections connt-limit-
high-watermark-pct 80 connt-mem-high-watermark-pct 80 tcp-timeout-
enable true tcp-timeout 30 tcp-start-timeout-enable true tcp-
start-timeout 20 tcp-end-timeout-enable true tcp-end-timeout 60
udp-timeout-enable true udp-timeout 30 icmp-timeout-enable true
icmp-timeout 5 other-timeout-enable true other-timeout 40 general
true pending-timeout-enable true memory-conn-status both log log
```

show aggressive-aging

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows aggressive aging settings.

Syntax

```
show aggressive-aging
```

Example Command

```
show aggressive-aging
```

show aggressive-aging advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows aggressive aging advanced settings.

Syntax

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

Example Command

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

Configuring QoS Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure QoS settings.

add qos-rule

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new QoS rule.

Syntax

```
add qos-rule
      [ name <name> ]
      [ comment "<comment>" ]
      [ source <source> ]
      [ destination <destination> ]
      [ service <service> ]
      [ low-latency-rule true ]
      [ low-latency-rule false ]
            [ limit-bandwidth { false | true limit-percentage <1-
100> } ]
            [ guarantee-bandwidth { false | true guarantee-
percentage <1-100> } ]
      [ weight <weight> ]
      [ hours-range-enabled { false | true hours-range-from
<hours-range-from> hours-range-to <hours-range-to> } ]
      [ diffserv-mark { false | true diffserv-mark-val <1-63> } ]
      [ { position <position> | position-above <position-above> |
position-below <position-below> } ]
      [ log {log | none} ]
      [ vpn {true | false} ]
```

Parameters

Parameter	Description
comment	Configures the comment text. A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
destination	Network object that is the target of the connection.
diffserv-mark	Controls whether to use a DiffServ Mark - a way to mark connections so a third party handles it.
diffserv-mark-val	Configures the DiffServ Mark value. This marks packets to be given priority on the public network according to their DSCP. You can get the DSCP value from your ISP or private WAN administrator. To use this option, your ISP or private WAN must support DiffServ.
guarantee-bandwidth	Enables (`true`) or disables (`false`) traffic guarantee. Available only if `low-latency-rule` = `false`.
guarantee-percentage	Configures the traffic guarantee percentage. Available only if `guarantee-bandwidth` = `true`.
hours-range-enabled	Controls whether to enable this rule during specific hours of the day.
hours-range-from	Configures the start time during the day (in the format HH:MM) when to enable this rule. Available only if `hours-range-enabled` = `true`.
hours-range-to	Configures the end time during the day (in the format HH:MM) when to disable this rule. Available only if `hours-range-enabled` = `true`.

Parameter	Description
limit-bandwidth	Controls whether to limit traffic (`true`) or not (`false`). Available only if `low-latency-rule` = `false`.
limit-percentage	Configures the traffic limit percentage. Available only if `limit-bandwidth` = `true`.
log	Controls whether to generate a log for this rule.
low-latency-rule	Configures the Low (`false`) or Normal (`true`) latency for this rule. If you configure the Low (`false`) latency, you can also configure the limit and guarantee.
name	Name of this rule. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)
position	Specifies the order of the rule (a decimal number) in comparison to other manual rules.
position-above	Specifies the relative order of the rule (a decimal number) in comparison to other manual rules.
position-below	Specifies the relative order of the rule (a decimal number) in comparison to other manual rules.
service	Specifies the service object. Press the TAB key to see the available options.
source	Specifies the Network object or User group that initiates the connection. Press the TAB key to see the available options.
vpn	Enables (`true`) or disables (`false`) this rule for traffic that passes over a VPN tunnel.
weight	Configures the traffic weight, relative to the weights configures in other QoS rules.

Example Command

```
add qos-rule name MyQosRule comment "QoS for HTTP from Internal to
External" source MyInternalNetwork destination MyExternalNetwork
service HTTP low-latency-rule false limit-bandwidth true limit-
percentage 15 guarantee-bandwidth true guarantee-percentage 30
weight 30 hours-range-enabled true hours-range-from 20:00 hours-
range-to 23:00 diffserv-mark true diffserv-mark-val 5 position 2
log none vpn true
```

set qos advanced-settings qos-logging

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables/Disables QoS logging.

Syntax

```
set qos advanced-settings qos-logging {true | false}
```

Example Command

```
set qos advanced-settings qos-logging true
```

set qos default-policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the default QoS policy.

Syntax

```
set qos default-policy [ limit-bandwidth-consuming-applications {
false | true [ limit-upload-traffic {true | false} ] [ upload-
limit <upload-limit> ] [ limit-download-traffic {true | false} ] [
download-limit <download-limit> ] } ] [ guarantee-bandwidth-to-
configured-traffic {on | off} [ 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 {on | off} ]
```

Parameters

Parameter	Description
limit-upload-traffic	
upload-limit	
limit-download-traffic	
download-limit	
guarantee-bandwidth-to-configured-traffic	
guarantee-bandwidth-percentage	
guarantee-bandwidth-traffic	
guarantee-bandwidth-on-services	
ensure-low-latency-for-delay-sensitive-services	

Example Command

```
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 mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables/Disables the QoS.

Syntax

```
set qos mode {true | false}
```

Example Command

```
set qos mode true
```

set qos delay-sensitive-service remove service

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set qos delay-sensitive-service remove service MyService
```

set qos delay-sensitive-service add service

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set qos delay-sensitive-service add service MyService
```

set qos guarantee-bandwidth-selected-services add service

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set qos guarantee-bandwidth-selected-services add service
MyService
```

set qos guarantee-bandwidth-selected-services remove service

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set qos guarantee-bandwidth-selected-services remove service
MyService
```

set qos low-latency-traffic maximum-percentage-of-bandwidth

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced QoS settings.

Syntax

```
set qos low-latency-traffic maximum-percentage-of-bandwidth
<percentage>
```

<*maximum-percentage-of-bandwidth*>

Parameters

Parameter	Description
maximum-percentage-of-bandwidth	

Example Command

```
set qos low-latency-traffic maximum-percentage-of-bandwidth 80
```

set qos-rule idx

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
destination	Network object that is the target of the connection

Parameter	Description
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 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)
guarantee-percentage	Traffic guarantee percentage 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 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) Press TAB to see available options

Parameter	Description
name	name A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
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 A number with no fractional part (integer)

Example Command

```
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 MyQosRule position 2 disabled true
```

set qos-rule name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
destination	Network object that is the target of the connection

Parameter	Description
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 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)
guarantee-percentage	Traffic guarantee percentage 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 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) Press TAB to see available options
name	name A string of alphanumeric characters **without** space between them: ▪ `a-z` (lower-case letters) ▪ `A-Z` (upper-case letters) ▪ `0-9` (digits)

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
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 A number with no fractional part (integer)

Example Command

```
set qos-rule name MyQosRule 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 position 2 disabled true
```

delete qos-rule idx

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
delete qos-rule idx 3.141
```

delete qos-rule name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Specifies the name of the QoS rule. Press the TAB key to see the available options.

Example Command

```
delete qos-rule name MyQoSRule
```

show qos

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the policy of the QoS blade.

Syntax

```
show qos
```

Example Command

```
show qos
```

show qos advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced settings of the QoS blade.

Syntax

```
show qos advanced-settings
```

Example Command

```
show qos advanced-settings
```

show qos delay-sensitive-services

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the group of services that are considered delay sensitive.

Syntax

```
show qos delay-sensitive-services
```

Parameters

Parameter	Description
n/a	

Example Command

```
show qos delay-sensitive-services
```

show qos guarantee-bandwidth-selected-services

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the group of services that can be guaranteed bandwidth in the QoS default policy.

Syntax

```
show qos guarantee-bandwidth-selected-services
```

Example Command

```
show qos guarantee-bandwidth-selected-services
```

show qos-rule name position

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration of a QoS rule by name.

Syntax

```
show qos-rule name <name> position <position>
```

Parameters

Parameter	Description
name	Specifies the name of the QoS rule. Press the TAB key to see the available options.
position	The order of the rule in comparison to other manual rules (a decimal number)

Example Command

```
show qos-rule name MyQoSRule position 2
```

show qos-rule

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show qos-rule idx 3.141 position 2
```

show qos-rules position

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A number with no fractional part (integer)

Example Command

```
show qos-rules position 2
```

Configuring Hotspot Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure hotspot settings.

set hotspot

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
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 A string that contains only printable characters.
portal-title	The title of the hotspot portal 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

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

Example Command

```
set hotspot require-auth true auth-mode allow-all allowed-group
MyUserGroup 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 add exception

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set hotspot add exception TEXT
```

set hotspot remove exception

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set hotspot remove exception TEXT
```

set hotspot advanced-settings activation

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced hotspot settings.

Syntax

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

Parameters

Parameter	Description
n/a	

Example Command

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

set hotspot advanced-settings prevent-simultaneous-login

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Prevents/Allows simultaneous login to hotspot.

Syntax

```
set hotspot advanced-settings prevent-simultaneous-login {true |
false}
```

Example Command

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

show hotspot

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows hotspot configuration.

Syntax

```
show hotspot
```

Example Command

```
show hotspot
```

show hotspot advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows hotspot advanced settings.

Syntax

```
shows hotspot advanced-settings
```

Example Command

```
shows hotspot advanced-settings
```

Working with Cellular Modem

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to work with Cellular Modem.

show cellular-modem-status

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the status of the cellular (LTE) modem.

Syntax

```
show cellular-modem-status
```

Parameters

Parameter	Description
N/A	

Example Command

```
show cellular-modem-status
```

Working with Zero Touch

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to work with Zero Touch.

set cloud-deployment

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures different settings for Zero Touch deployment. Command is relevant to preset files.

See *"show cloud-deployment" on page 1279*.

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 A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '-' (minus)
template	Template Type: String

Example Command

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

show cloud-deployment

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of cloud management connection (Zero Touch).

See *"set cloud-deployment" on page 1278*.

Syntax

```
show cloud-deployment
```

Example Output

```
cloud-url:                      zerotouch.checkpoint.com
verify-certificate:             on
mode:                           on
```

set cloud-notification

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables and disables notification types for Zero Touch.

See *"show cloud-notifications" on page 1281*.

Syntax

```
set cloud-notification <Notification-Type> mode {off | on}
```

Parameters

Parameter	Description
notification-type	Specifies the notification type. **Note** - To see the available notification types, run this command: *"show cloud-notifications" on page 1281*

Example Command

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

show cloud-notifications

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the status for all types of notifications.

See *"set cloud-notification" on page 1280*.

Syntax

```
show cloud-notifications
```

Example Output

```
notification-type                                                    mode
license-expired                                                      true
license-about-to-expire                                              true
license-activated                                                    true
infected-device                                                      true
malicious-file-blocked                                               true
malicious-file-downloaded                                            true
firmware-upgrade-available                                           true
new-device                                                           true
system-up                                                            true
unexpected-reboot                                                    true
primary-internet-up                                                  true
secondary-internet-up                                                true
malicious-mail-blocked                                               true
malicious-mail-received                                              true
suppressed-notifications                                             true
reconnected-device                                                   true
flash-memory-lifetime-used                                           true
vpn-tunnel-creation                                                  true
vpn-tunnel-down                                                      true
vpn-certificate-about-to-expire                                      true
vpn-certificate-expired                                              true
partition-capacity-is-about-to-be-full                               true
new-iot-asset                                                        true
iot-asset-access                                                     true
vpn-peer-link-restored                                               true
vpn-peer-link-not-responding                                         true
sdwan-steering-change-isp-down                                       true
sdwan-steering-change-quality                                        true
isp-down                                                             true
isp-up                                                               true
cluster-change                                                       true
administrator-logged-in                                              true
administrator-logged-in-to-expert-shell                              true
cellular data usage                                                  true
vpn-tunnel-test-failure-caused-tunnel-deletion                       true
vpn-information-notification                                         true
suppressed-notifications summary                                     true
```

set zero-touch

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure parameters for the Zero Touch service.

See *"show zero-touch" on page 1284*.

Syntax

```
set zero-touch [ cloud-url <cloud-url> ] [ mode {off | on} ] [
verify-certificate {off | on ]
```

Parameters

Parameter	Description
cloud-url	Specifies the IP address or URL of the cloud service. Default: `zerotouch.checkpoint.com`
mode	Controls whether the appliance constantly tries (`on`) or does not try (`off`) to fetch its configuration from the Zero Touch server if the First Time Configuration Wizard is not started. Default: `on`
verify-certificate	Controls whether the appliance verifies (`on`) or does not verify (`off`) the SSL certificate of the Zero Touch server. Default: `on` **Best Practice** - Do not disable this option.

Example Command

```
set zero-touch cloud-url zerotouch.checkpoint.com verify-
certificate on mode on
```

show zero-touch

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the parameters configured for the Zero Touch service.

See *"set zero-touch" on page 1283*.

Syntax

```
show zero-touch
```

Example Output

```
cloud-url:                      zerotouch.checkpoint.com
verify-certificate:             on
mode:                           on
```

test zero-touch-request

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Test the procedure of receiving configuration from Zero Touch.

The appliance connects to Zero Touch and shows the received configuration without enforcing it.

You can save the received configuration to the `/storage/zt_cfg.clish` file.

Syntax

```
test zero-touch-request [save-config-as file]
```

Parameters

Optional Parameter	Description
save-config-as file	Save received configuration to the `/storage/zt_cfg.clish` file.

Example Command

```
test zero-touch-request save-config-as file
```

Working with Cloud Services (SMP)

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to work with Cloud Services (SMP).

set cloud-services

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

set cloud-services advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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> ]
```

Example Command

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

show cloud-services

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced settings of cloud management connection.

Syntax

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

Parameters

Parameter	Description
n/a	

Example Command

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

show cloud-services status

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the current status of the cloud management connection.

Syntax

```
show cloud-services status
```

Parameters

Parameter	Description
n/a	

Example Command

```
show cloud-services status
```

show cloud-services connection-details

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows connection details for cloud management connection.

Syntax

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

Parameters

Parameter	Description
n/a	

Example Command

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

fetch cloud-services policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Fetch configuration now from your Cloud Services Security Management Server.

Syntax

```
fetch cloud-services policy
```

Parameters

Parameter	Description
n/a	

Example Command

```
fetch cloud-services policy
```

reconnect cloud-services

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Force a manual reconnection to Cloud Services.

Syntax

```
reconnect cloud-services
```

Parameters

Parameter	Description
n/a	

Example Command

```
reconnect cloud-services
```

send cloud-report

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

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

show cloud-service managed-blades

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the currently managed blades by the cloud management.

Syntax

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

Parameters

Parameter	Description
n/a	

Example Command

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

show cloud-services managed-services

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the currently managed services by the cloud management.

Syntax

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

Parameters

Parameter	Description
n/a	

Example Command

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

test cloud-connectivity

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Checks the connection to Cloud Management:

Port	Purpose
TCP 18191	Fetch a policy or configuration
TCP 18210	Pull certificates
TCP 18264	Download a Certificate Authority CRL
TCP 443	Web services (initial connection, upgrade service, report data upload)

Syntax

```
test cloud-connectivity [service-center-addr <IP address of FQDN of Server>]
```

Parameters

Optional Parameter	Description
service-center-addr	Specifies the IP address of FQDN of the Cloud Management Server

Example Command

```
test cloud-connectivity
```

generate report cloud-report

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Generate a cloud report.

In addition, see the "`fw smbcloud_report_pdf`" command in *"fw commands" on page 1701*.

Syntax

```
generate report type {monthly | daily | weekly | hourly}
```

Example Command

```
generate report type hourly
```

"Firmware Upgrade" Cloud Services

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

This section provides commands to work with "Firmware Upgrade" Cloud Services.

set cloud-services-firmware-upgrade

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 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 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 Command

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

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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>
```

Example Command

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

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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Example Command

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

show cloud-services-firmware-upgrade

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration of the "Firmware Upgrade" Cloud Services.

Syntax

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

Example Command

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

show cloud-services-firmware-upgrade advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Syntax

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

Example Command

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

Configuring Management as a Service (MaaS)

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Management as a Service (MaaS) settings.

connect maas

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Connect to Management as a Service (MaaS) to manage policy, log analysis, and reporting log retention.

Syntax

```
connect maas auth-token <auth-token>
```

Parameters

Parameter	Description
auth-token	Authentication token is used for connecting to MAAS Type: base64

Example Command

```
connect maas auth-token base64
```

set maas

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the settings for Management as a Service (MaaS).

Syntax

```
set maas mode <mode>
```

Parameters

Parameter	Description
mode	Connection to MAAS mode Options: enable, disable, stop-using

Example Command

```
set maas mode enable
```

show maas

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show if connected to Management as a Service (MaaS).

Syntax

```
show maas
```

Example Command

```
show maas
```

Configuring the "Reach My Device" Service

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the "Reach My Device" feature.

This feature lets you connect remotely to the appliance from the Internet through a dedicated Check Point cloud service.

You get two dedicated URLs for your appliance:

- To connect to the WebUI:

  ```
  https://<HostName>-web.smbrelay.checkpoint.com
  ```

- To connect to the CLI:

  ```
  https://<HostName>-shell.smbrelay.checkpoint.com
  ```

Such configuration is very useful when the appliance is behind a NAT device or firewall, and cannot be reached directly.

In addition, the feature makes it easier to access an appliance with a dynamically assigned IP address.

set reach-my-device

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the "Reach My Device" feature.

Syntax

```
set reach-my-device
      advanced-settings
      existing-host-name
            true validation-token <Token>
            false host-name <HostName>
      get-tunnel-mode-interval <3600-86400>
      host-name <HostName>
      mode {on | off}
      poll-interval <3-60>
```

Parameters

Parameter	Description
advanced-settings	Configures the advanced settings. See *"set reach-my-device advanced-settings" on page 1311*.
existing-host-name	Controls which hostname to use to register this appliance in the Check Point cloud service: ■ `true` - Use the current configured hostname. ■ `false` - Use the specified hostname.
get-tunnel-mode-interval	Configures the time interval (in seconds) for the appliance to get the tunnel mode from the Check Point cloud service. Valid values: 3600 - 86400 seconds. Default: 43200 seconds. **Best Practice** - Do not change the default value.

Parameter	Description
host-name	When you specify "`existing-host-name false`", this parameter configures the appliance hostname to register in the Check Point cloud service. A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) **Important** - If you change the hostname, all WatchTower mobile app users must pair their mobile devices again.
mode	Enables (`true`) or disables (`false`) the Reach My Device feature.
poll-interval	Configures the time interval (in seconds) for the appliance to test the connection to the Check Point cloud service. Valid values: 3 - 60 seconds. Default: 6 seconds. **Best Practice** - Do not change the default value.
validation-token	Configures a one-time validation token. You create this token. This token verifies that an existing hostname belongs to this appliance owner. A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)

Example Command

```
set reach-my-device mode true existing-host-name true validation-
token MyToken123
```

set reach-my-device advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings of the "Reach My Device" feature.

Syntax

```
set reach-my-device advanced-settings
      ignore-ssl-cert {true | false}
      server-addr <URL>
```

Parameters

Parameter	Description
ignore-ssl-cert	Specifies whether to ignore (`true`) or not (`false`) the SSL certificate of the Check Point cloud service. Default: `false`
server-addr	Configures the URL for the Check Point cloud service. Default: `smbrelay.checkpoint.com` **Best Practice** - Do not change the default value.

show reach-my-device

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of the "Reach My Device" feature.

Syntax

```
show reach-my-device [advanced-settings]
```

Example Output 1

```
MyGateway> show reach-my-device
reach-my-device-server-addr:  smbrelay.checkpoint.com
get-tunnel-mode-interval:     43200
host-name:                    MyGateway
validation-token:             MyToken123
mode:                         true
poll-interval:                6

web: https://MyGateway-web.smbrelay.checkpoint.com
cli: https://MyGateway-shell.smbrelay.checkpoint.com
MyGateway>
```

Example Output 2

```
MyGateway> show reach-my-device advanced-settings
ignore-ssl-cert:              false
reach-my-device-server-addr:  smbrelay.checkpoint.com

MyGateway>
```

Working with Internal Certificates

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to work with internal certificates.

add internal-certificate

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add an internal certificate.

See:

- *"delete internal-certificate" on the next page*
- *"show internal-certificate" on page 1316*
- *"show internal-certificates" on page 1317*

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 Command

```
add internal-certificate certificate-name TEXT p12-password
QWEDFRGH4 url ftpUrl less-secure true
```

delete internal-certificate

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete an internal certificate.

See:

- *"add internal-certificate" on the previous page*
- *"show internal-certificate" on page 1316*
- *"show internal-certificates" on page 1317*

Syntax

```
delete internal-certificate name <name>
```

Parameters

Parameter	Description
name	Name of the internal certificate Type: String

Example Command

```
delete internal-certificate name TEXT
```

set device-details auth-cert

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the authentication certificate for WebUI on this device.

You can see and install the certificates in WebUI > **VPN** view > **Certificates** > **Installed Certificates**.

See:

- *"show device-details" on page 1716*
- *"add internal-certificate" on page 1313*

Syntax

```
set device-details auth-cert { defaultCert | <Installed
Certificate> }
```

Parameters

Parameter	Description
auth-cert	The authentication certificate. Press the TAB key to see the available options.

Example Command

```
set device-details auth-cert defaultCert
```

show device-details

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of basic device details - hostname, country, default certificate.

See:

- *"set device-details auth-cert" on page 1709*
- *"set device-details country" on page 1710*
- *"set device-details hostname" on page 1711*

Syntax

```
show device-details
```

Example 1

```
Gateway-ID-7F95E42D> show device-details
hostname:                       Gateway-ID-7F95E42D
country:                        united-states
auth-cert:                      Default Web Portal Certificate

Gateway-ID-7F95E42D>
```

Example 2

```
Gateway-ID-7F95E42D> show device-details
hostname:                       Gateway-ID-7F95E42D
country:                        united-states
auth-cert:                      Default VPN and Cluster certificate

Gateway-ID-7F95E42D>
```

show internal-certificate

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show an internal certificate.

See:

- *"add internal-certificate" on page 1313*
- *"delete internal-certificate" on page 1314*
- *"show internal-certificates" below*

Syntax

```
show internal-certificate name <name>
```

Parameters

Parameter	Description
name	Name of the internal certificate Type: String

Example Command

```
show internal-certificate name TEXT
```

show internal-certificates

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show all internal certificates.

See:

- *"add internal-certificate" on page 1313*
- *"delete internal-certificate" on page 1314*
- *"show internal-certificate" on the previous page*

Syntax

```
show internal-certificates
```

Parameters

Parameter	Description
n/a	

Example Command

```
show internal-certificates
```

Working with the ICA Certificate

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to work with the Internal Certificate Authority (ICA) certificate.

set internal-ca-certificate

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Create the Internal Certificate Authority (ICA) certificate.

Syntax

```
set internal-ca-certificate certificate-name <certificate-name>
p12-password <p12-password> common-name <common-name> cert-base64-
encoding <cert-base64-encoding>
```

Parameters

Parameter	Description
cert-base64-encoding	Certificate file in base64 format Type: base64
certificate-name	Informal representation for the certificate Type: String
common-name	The Common Name is typically composed of Host + Domain Name Type: ipv4OrIpv6OrHost
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

Example Command

```
set internal-ca-certificate certificate-name TEXT p12-password
QWEDFRGH4 common-name ipv4OrIpv6OrHost cert-base64-encoding base64
```

show internal-ca-certificate

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show information about the Internal Certificate Authority (ICA) certificate.

Syntax

```
show internal-ca-certificate
```

Example Command

```
show internal-ca-certificate
```

Example Output

```
common-name: O=00:1C:7F:00:01:5C..it8uv8
valid-from: Sun Mar 7 11:29:50 2021
valid-until: Fri Jan 1 05:14:07 2038
fingerprint: BYE OATH ALIA RICK BODE GEAR WORK OK IF MEN GAVE MALI
```

re-initialize internal-ca-certificate

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Initializes internal certificates:

- Internal Certificate Authority (ICA) certificate
- Internal VPN certificate

Syntax

```
re-initialize internal-ca-certificate [host-ip-address <Common
Name>] [internal-ca-dn <Certificate DN>] [internal-ca-expiration
<Years>] [internal-cert-expiration <Years>]
```

Parameters

Parameter	Description
host-ip-address	Specifies the Common Name. Usually, composed of Host Name and Domain Name (for example: `myhost.example.com`).
internal-ca-dn	Specifies the Certificate DN (for example: `O=example,CN=*.example.com`). Must contain at least the organization. Must not contain spaces.
internal-ca-expiration	Specifies the number of years the internal CA certificate is valid.
internal-cert-expiration	Specifies the number of years the internal VPN certificate is valid.

Example Command

```
re-initialize internal-ca-certificate internal-ca-dn
"CN=SMP,OU=MyCompany,O=MyCompany,CN=*.MyCompany.com" internal-
cert-expiration 10
```

Working with IoT Statistics

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to work with IoT statistics.

set iot-stats

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Enables or disables the collection of IoT protection statistics.

See *"show iot-stats" on page 1336*.

Syntax

```
set iot-stats mode { on | off }
```

Example Command

```
set iot-stats mode on
```

show iot-stats

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows whether the collection of IoT protection statistics is enabled or not.

See *"set iot-stats" on page 1335*.

Syntax

```
show iot-stats
```

Example Output

```
mode:                                on
```

Configuring IoT Protection

In the R81.10.X releases, this feature is available starting from the R81.10.10 version.

This section provides commands for the IoT protection.

When you enable the IoT blade on the appliance, it recognizes each IoT device that connects to WiFi provided by your appliance and automatically enforces practices (policy set by the particular vendor) in the preconfigured IoT policy.

You do not need to configure the policy for each IoT device that connects to your appliance.

General rules for IoT are preconfigured. For example, the appliance always allows traffic to some domains, and always blocks traffic to other domains. You can make some changes to the policy.

Workflow:

1. Configure the settings for the IoT device type (asset):
   a. Examine the current settings:

      "show iot-device-type" on page 1328

   b. Add an IoT device type (asset):

      "add iot-device-type" on page 1325

   c. Configure the applicable settings:

      "set iot-device-type" on page 1326

2. Configure the IoT policy:
   a. Add an IoT policy for an IoT device type:
   b. Configure how to handle traffic for new discovered IoT features:

      "set iot-protection-policy newly-discovered-functions" on page 1333

   c. Configure the monitor mode:

      "set iot-protection-policy monitor-mode" on page 1332

   d. Examine the policy settings:

      "show iot-protection-policy" on page 1334

3. Configure the collection of IoT protection statistics:
   a. Examine the current settings:

      "show iot-stats" on page 1336

b. Configure the applicable settings:

"set iot-stats" on page 1335

4. Enable the IoT protection:

"set iot-protection-policy mode" on page 1331

5. Examine the current settings:

"show iot-device-type" on page 1328

6. Examine the list of IoT device vendors:

"show iot-vendor-to-assets" on page 1337

add iot-device-type

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

With this command, you can add an allowed domain that a specific IoT asset type can access.

See also:

- *"set iot-device-type" on page 1326*
- *"show iot-device-type" on page 1328*

Syntax

```
add iot-device-type  <device-type-name> <IoT Device Type> allowed-
domain <Domain-Name>
```

Parameters

Parameter	Description
iot-device-type	Type of the IoT asset.
device-type-name	Name of the device
domain-name	Name of the allowed domain.

Example Command

```
add iot-device-type printer allowed-domain google.com
```

set iot-device-type

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

With this command, you can change the Internet access for a specific IoT asset type and whether to generate logs for this traffic.

See also:

- *"add iot-device-type" on page 1325*
- *"show iot-device-type" on page 1328*

Syntax

```
set iot-device-type device-type-name <IoT Device Type>
      access-to-internet { block | inactive | monitor | prevent }
      log { true | false }
```

Parameters

Parameter	Description
iot-device-type	Type of the IoT asset.
device-type-name	Name of the device
access-to-internet	Specifies the type of Internet access: ■ `block` - Completely blocks all internet access. ■ `inactive` - IoT protection is not enabled. ■ `monitor` - It is possible to access all domains but logs all traffic. ■ `prevent` - It is possible to access only domains or IP addresses of the same practices.
log	Enables (`true`) or disables (`false`) the logs for this traffic. Default: `false`

Example Commands

```
set iot-device-type device-type-name printer access-to-internet
block
```

```
set iot-device-type device-type-name printer log true
```

show iot-device-type

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows information for the IoT devices (assets) connected to the appliance.

See also:

- *"add iot-device-type" on page 1325*
- *"set iot-device-type" on page 1326*

Syntax to see the information for all device types

```
show iot-device-type
```

Syntax to see the information for the specified device type

```
show iot-device-type device-type-name <IoT Device Type>
```

Example Output - shows all device types (truncated)

```
MyGw> show iot-device-type
... ...
iot-device-type:        printer
access-to-internet:   prevent
assets-count:         0
vendors:
approved-destinations: google.com
allowed-domain:
log:                  false

iot-device-type:         ip-camera
access-to-internet:    prevent
assets-count:          0
vendors:
approved-destinations: google.com
allowed-domain:
log:                   false

iot-device-type:         media-player
access-to-internet:    inactive
assets-count:          0
vendors:
approved-destinations:
allowed-domain:
log:                   false
... ...
MyGw>
```

Example Output - shows the information for a specified device type

```
MyGw> show iot-device-type device-type-name printer
access-to-internet:           prevent
assets-count:                 0
vendors:
approved-destinations:
allowed-domain:
log:
recognitionRank:
blockCount:                   0
infectedCount:                0
unprotectedCount:             0
lowConfidenceCount:
assetsForUnauthorizedDestinationsCount:0
isNoPracticeCount:            0
isMonitoringFunction:

MyGW>
```

set iot-protection-policy mode

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Enables or disables the IoT protection feature on the appliance.

See also:

- *"set iot-protection-policy monitor-mode" on page 1332*
- *"set iot-protection-policy newly-discovered-functions" on page 1333*
- *"show iot-protection-policy" on page 1334*

Syntax

```
set iot-protection-policy mode { on | off }
```

Example Command

```
set iot-protection-policy on
```

set iot-protection-policy monitor-mode

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Enables or disables the monitor-only mode in the IoT protection.

In the monitor-only mode, the IoT protection accept traffic from all IoT devices (assets).

See also:

- *"set iot-protection-policy newly-discovered-functions" on page 1333*
- *"show iot-protection-policy" on page 1334*

Syntax

```
set iot-protection-policy monitor-mode { on | off }
```

Example Command

```
set iot-protection-policy monitor-mode on
```

set iot-protection-policy newly-discovered-functions

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

With this command, you can change how the IoT protection handles traffic from a newly connected IoT device (asset).

See also:

- *"set iot-protection-policy monitor-mode" on page 1332*
- *"show iot-protection-policy" on page 1334*

Syntax

```
set iot-protection-policy newly-discovered-functions <Mode>
```

Parameters

Parameter	Description
mode	Specifies how to handle traffic from a newly connected IoT device (asset): ■ `always-prevent` - Always prevent ■ `always-monitor` - Always monitor and allow ■ `according-to-custom_table` - According to the predefined Check Point policy: • prevent traffic from device types "Printer" and "IP camera". • detect and allow traffic from all other device types.

Example:

```
set iot-protection-policy newly-discovered-functions according-to-
custom_table
```

show iot-protection-policy

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows the status of the IoT protection:

- Is the feature enabled or not (*"set iot-protection-policy mode" on page 1331*)
- Does the feature work in the monitor-only mode or not (*"set iot-protection-policy monitor-mode" on page 1332*)

See also:

- *"set iot-protection-policy monitor-mode" on page 1332*
- *"set iot-protection-policy newly-discovered-functions" on page 1333*

Syntax

```
show iot-protection-policy
```

Example Output

```
mode:                   on
monitor-mode:           off
```

set iot-stats

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Enables or disables the collection of IoT protection statistics.

See *"show iot-stats" on page 1336*.

Syntax

```
set iot-stats mode { on | off }
```

Example Command

```
set iot-stats mode on
```

show iot-stats

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows whether the collection of IoT protection statistics is enabled or not.

See *"set iot-stats" on page 1335*.

Syntax

```
show iot-stats
```

Example Output

```
mode:                                on
```

show iot-vendor-to-assets

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows vendors of the detected IoT devices.

Syntax to see all vendors

```
show iot-vendor-to-assets
```

Syntax to see the specified vendor

```
show iot-vendor-to-assets vendor <Vendor-Name>
```

Working with Mobile Devices

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to work with Mobile devices.

add mobile-invitation administrator

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Invitation for a new mobile device.

Syntax

```
add mobile-invitation administrator name <administrator name>
```

Parameters

Parameter	Description
administrator name	Administrator Name A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '_' (underscore)

Example Command

```
add mobile-invitation administrator name admin
```

set mobile-settings advanced-settings pairing-code-expiration

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the expiration timeout (in seconds) for the pairing code for a mobile device.

Syntax

```
set mobile-settings advanced-settings pairing-code-expiration
<expiration>
```

Parameters

Parameter	Description
pairing-code-expiration	Number of seconds until the pairing code expires.

Example Command

```
set mobile-settings advanced-settings pairing-code-expiration 10
```

set mobile-settings advanced-settings not-cloud-server

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the cloud server URL used for sending mobile notifications.

Syntax

```
set mobile-settings advanced-settings not-cloud-server <URL>
```

Example Command

```
set mobile-settings advanced-settings not-cloud-server
https://myurl.example.com
```

show mobile-settings advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show configured advanced settings for a mobile device.

Syntax

```
show mobile-settings advanced-settings
```

Example Command

```
show mobile-settings advanced-settings
```

show mobile-invitation id

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show an invitation for a new mobile device.

Syntax

```
show mobile-invitation id <invitation-id>
```

Parameters

Parameter	Description
invitation-id	Invitation ID Press the TAB key to see the available options.

Example Command

```
show mobile-invitation id 10
```

show mobile-push-notifications

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show mobile push notifications.

Syntax

```
show mobile-push-notifications
```

Example Command

```
show mobile-push-notifications
```

revoke mobile-device id

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Remove mobile device from the list of associated devices.

Syntax

```
revoke mobile-device id <id>
```

Parameters

Parameter	Description
id	Device ID Press the TAB key to see the available options.

Example Command

```
revoke mobile-device id 2
```

Configuring Site-to-Site VPN

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Site-to-Site VPN settings.

add vpn site

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new remote VPN site for Site-to-Site VPN.

Syntax

```
add vpn site name <name> remote-site-link-selection connection-
initiated-only-from-remote-site auth-method
      preshared-secret password <password>
            [ aggressive-mode-enabled false ]
            [ aggressive-mode-enabled true aggressive-mode-DH-
group <aggressive-mode-DH-group> ]
                  [ aggressive-mode-enable-peer-id { false | true
aggressive-mode-peer-id-type {domain-name | user-name} aggressive-
mode-peer-id <aggressive-mode-peer-id> } ]
                  [ aggressive-mode-enable-gateway-id { false |
true aggressive-mode-gateway-id-type {domain-name | user-name}
aggressive-mode-gateway-id <aggressive-mode-gateway-id> } ]
            [ disable-nat {true | false} ]
            [ enabled {true | false} ]
            [ enable-perfect-forward-secrecy { false | true [
phase2-dh <phase2-dh> ] } ]
            [ enc-method <enc-method> ]
            [ enc-profile <enc-profile> ]
            [ is-check-point-site { false | true [ enable-
permanent-vpn-tunnel {true | false} ] } ]
            [ link-selection-probing-method {ongoing | one-time} ]
            [ match-cert-dn { false | true match-cert-dn-string
<match-cert-dn-string> } ]
            [ match-cert-e-mail { false | true match-cert-e-mail-
string <match-cert-e-mail-string> } ]
            [ match-cert-ip {true | false} ]
            [ phase1-reneg-interval <phase1-reneg-interval> ]
            [ phase2-reneg-interval <phase2-reneg-interval> ]
            [ remote-site-enc-dom-type <remote-site-enc-dom-type>
]
            [ use-trusted-ca {internal_ca | anyCa} ]
      certificate
            [ aggressive-mode-enabled false ]
            [ aggressive-mode-enabled true aggressive-mode-DH-
group <aggressive-mode-DH-group> ]
                  [ aggressive-mode-enable-peer-id { false | true
aggressive-mode-peer-id-type {domain-name | user-name} aggressive-
mode-peer-id <aggressive-mode-peer-id> } ]
                  [ aggressive-mode-enable-gateway-id { false |
true aggressive-mode-gateway-id-type {domain-name | user-name}
aggressive-mode-gateway-id <aggressive-mode-gateway-id> } ]
            [ disable-nat {true | false} ]
            [ enabled {true | false} ]
            [ enable-perfect-forward-secrecy { false | true [
phase2-dh <phase2-dh> ] } ]
```

```
            [ enc-method <enc-method> ]
            [ enc-profile <enc-profile> ]
            [ is-check-point-site { false | true [ enable-
permanent-vpn-tunnel {true | false} ] } ]
            [ link-selection-probing-method {ongoing | one-time} ]
            [ match-cert-dn { false | true match-cert-dn-string
<match-cert-dn-string> } ]
            [ match-cert-e-mail { false | true match-cert-e-mail-
string <match-cert-e-mail-string> } ]
            [ match-cert-ip {true | false} ]
            [ phase1-reneg-interval <phase1-reneg-interval> ]
            [ phase2-reneg-interval <phase2-reneg-interval> ]
            [ remote-site-enc-dom-type <remote-site-enc-dom-type>
]
            [ use-trusted-ca {internal_ca | anyCa} ]
```

```
add vpn site name <name> remote-site-link-selection high-
availability link-selection-multiple-addrs addr <link-selection-
multiple-addrs addr> auth-method
      preshared-secret password <password>
            [ aggressive-mode-enabled false ]
            [ aggressive-mode-enabled true aggressive-mode-DH-
group <aggressive-mode-DH-group> ]
                  [ aggressive-mode-enable-peer-id { false | true
aggressive-mode-peer-id-type {domain-name | user-name} aggressive-
mode-peer-id <aggressive-mode-peer-id> } ]
                  [ aggressive-mode-enable-gateway-id { false |
true aggressive-mode-gateway-id-type {domain-name | user-name}
aggressive-mode-gateway-id <aggressive-mode-gateway-id> } ]
            [ disable-nat {true | false} ]
            [ enabled {true | false} ]
            [ enable-perfect-forward-secrecy { false | true [
phase2-dh <phase2-dh> ] } ]
            [ enc-method <enc-method> ]
            [ enc-profile <enc-profile> ]
            [ is-check-point-site { false | true [ enable-
permanent-vpn-tunnel {true | false} ] } ]
            [ link-selection-probing-method {ongoing | one-time} ]
            [ match-cert-dn { false | true match-cert-dn-string
<match-cert-dn-string> } ]
            [ match-cert-e-mail { false | true match-cert-e-mail-
string <match-cert-e-mail-string> } ]
            [ match-cert-ip {true | false} ]
            [ phase1-reneg-interval <phase1-reneg-interval> ]
            [ phase2-reneg-interval <phase2-reneg-interval> ]
            [ remote-site-enc-dom-type <remote-site-enc-dom-type>
]
            [ use-trusted-ca {internal_ca | anyCa} ]
      certificate
            [ aggressive-mode-enabled false ]
            [ aggressive-mode-enabled true aggressive-mode-DH-
group <aggressive-mode-DH-group> ]
                  [ aggressive-mode-enable-peer-id { false | true
aggressive-mode-peer-id-type {domain-name | user-name} aggressive-
mode-peer-id <aggressive-mode-peer-id> } ]
                  [ aggressive-mode-enable-gateway-id { false |
true aggressive-mode-gateway-id-type {domain-name | user-name}
aggressive-mode-gateway-id <aggressive-mode-gateway-id> } ]
            [ disable-nat {true | false} ]
            [ enabled {true | false} ]
            [ enable-perfect-forward-secrecy { false | true [
phase2-dh <phase2-dh> ] } ]
```

```
            [ enc-method <enc-method> ]
            [ enc-profile <enc-profile> ]
            [ is-check-point-site { false | true [ enable-
permanent-vpn-tunnel {true | false} ] } ]
            [ link-selection-probing-method {ongoing | one-time} ]
            [ match-cert-dn { false | true match-cert-dn-string
<match-cert-dn-string> } ]
            [ match-cert-e-mail { false | true match-cert-e-mail-
string <match-cert-e-mail-string> } ]
            [ match-cert-ip {true | false} ]
            [ phase1-reneg-interval <phase1-reneg-interval> ]
            [ phase2-reneg-interval <phase2-reneg-interval> ]
            [ remote-site-enc-dom-type <remote-site-enc-dom-type>
]
            [ use-trusted-ca {internal_ca | anyCa} ]
```

```
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>
            [ aggressive-mode-enabled false ]
            [ aggressive-mode-enabled true aggressive-mode-DH-
group <aggressive-mode-DH-group> ]
                  [ aggressive-mode-enable-peer-id { false | true
aggressive-mode-peer-id-type {domain-name | user-name} aggressive-
mode-peer-id <aggressive-mode-peer-id> } ]
                  [ aggressive-mode-enable-gateway-id { false |
true aggressive-mode-gateway-id-type {domain-name | user-name}
aggressive-mode-gateway-id <aggressive-mode-gateway-id> } ]
            [ disable-nat {true | false} ]
            [ enabled {true | false} ]
            [ enable-perfect-forward-secrecy { false | true [
phase2-dh <phase2-dh> ] } ]
            [ enc-method <enc-method> ]
            [ enc-profile <enc-profile> ]
            [ is-check-point-site { false | true [ enable-
permanent-vpn-tunnel {true | false} ] } ]
            [ link-selection-probing-method {ongoing | one-time} ]
            [ match-cert-dn { false | true match-cert-dn-string
<match-cert-dn-string> } ]
            [ match-cert-e-mail { false | true match-cert-e-mail-
string <match-cert-e-mail-string> } ]
            [ match-cert-ip {true | false} ]
            [ phase1-reneg-interval <phase1-reneg-interval> ]
            [ phase2-reneg-interval <phase2-reneg-interval> ]
            [ remote-site-enc-dom-type <remote-site-enc-dom-type>
]
            [ use-trusted-ca {internal_ca | anyCa} ]
      certificate
            [ aggressive-mode-enabled false ]
            [ aggressive-mode-enabled true aggressive-mode-DH-
group <aggressive-mode-DH-group> ]
                  [ aggressive-mode-enable-peer-id { false | true
aggressive-mode-peer-id-type {domain-name | user-name} aggressive-
mode-peer-id <aggressive-mode-peer-id> } ]
                  [ aggressive-mode-enable-gateway-id { false |
true aggressive-mode-gateway-id-type {domain-name | user-name}
aggressive-mode-gateway-id <aggressive-mode-gateway-id> } ]
            [ disable-nat {true | false} ]
            [ enabled {true | false} ]
            [ enable-perfect-forward-secrecy { false | true [
phase2-dh <phase2-dh> ] } ]
```

```
            [ enc-method <enc-method> ]
            [ enc-profile <enc-profile> ]
            [ is-check-point-site { false | true [ enable-
permanent-vpn-tunnel {true | false} ] } ]
            [ link-selection-probing-method {ongoing | one-time} ]
            [ match-cert-dn { false | true match-cert-dn-string
<match-cert-dn-string> } ]
            [ match-cert-e-mail { false | true match-cert-e-mail-
string <match-cert-e-mail-string> } ]
            [ match-cert-ip {true | false} ]
            [ phase1-reneg-interval <phase1-reneg-interval> ]
            [ phase2-reneg-interval <phase2-reneg-interval> ]
            [ remote-site-enc-dom-type <remote-site-enc-dom-type>
]
            [ use-trusted-ca {internal_ca | anyCa} ]
```

```
add vpn site name <name> remote-site-link-selection ip-address
remote-site-ip-address <remote-site-ip-address> is-site-behind-
static-nat false
add vpn site name <name> remote-site-link-selection 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>
            [ aggressive-mode-enabled false ]
            [ aggressive-mode-enabled true aggressive-mode-DH-
group <aggressive-mode-DH-group> ]
                  [ aggressive-mode-enable-peer-id { false | true
aggressive-mode-peer-id-type {domain-name | user-name} aggressive-
mode-peer-id <aggressive-mode-peer-id> } ]
                  [ aggressive-mode-enable-gateway-id { false |
true aggressive-mode-gateway-id-type {domain-name | user-name}
aggressive-mode-gateway-id <aggressive-mode-gateway-id> } ]
            [ disable-nat {true | false} ]
            [ enabled {true | false} ]
            [ enable-perfect-forward-secrecy { false | true [
phase2-dh <phase2-dh> ] } ]
            [ enc-method <enc-method> ]
            [ enc-profile <enc-profile> ]
            [ is-check-point-site { false | true [ enable-
permanent-vpn-tunnel {true | false} ] } ]
            [ link-selection-probing-method {ongoing | one-time} ]
            [ match-cert-dn { false | true match-cert-dn-string
<match-cert-dn-string> } ]
            [ match-cert-e-mail { false | true match-cert-e-mail-
string <match-cert-e-mail-string> } ]
            [ match-cert-ip {true | false} ]
            [ phase1-reneg-interval <phase1-reneg-interval> ]
            [ phase2-reneg-interval <phase2-reneg-interval> ]
            [ remote-site-enc-dom-type <remote-site-enc-dom-type>
]
            [ remote-site-ipv6-address <remote-site-ipv6-address>
]
            [ use-trusted-ca {internal_ca | anyCa} ]
      certificate
            [ aggressive-mode-enabled false ]
            [ aggressive-mode-enabled true aggressive-mode-DH-
group <aggressive-mode-DH-group> ]
                  [ aggressive-mode-enable-peer-id { false | true
aggressive-mode-peer-id-type {domain-name | user-name} aggressive-
mode-peer-id <aggressive-mode-peer-id> } ]
```

```
                  [ aggressive-mode-enable-gateway-id { false |
true aggressive-mode-gateway-id-type {domain-name | user-name}
aggressive-mode-gateway-id <aggressive-mode-gateway-id> } ]
            [ disable-nat {true | false} ]
            [ enabled {true | false} ]
            [ enable-perfect-forward-secrecy { false | true [
phase2-dh <phase2-dh> ] } ]
            [ enc-method <enc-method> ]
            [ enc-profile <enc-profile> ]
            [ is-check-point-site { false | true [ enable-
permanent-vpn-tunnel {true | false} ] } ]
            [ link-selection-probing-method {ongoing | one-time} [
remote-site-ipv6-address <remote-site-ipv6-address> ] ]
            [ match-cert-dn { false | true match-cert-dn-string
<match-cert-dn-string> } ]
            [ match-cert-e-mail { false | true match-cert-e-mail-
string <match-cert-e-mail-string> } ]
            [ match-cert-ip {true | false} ]
            [ phase1-reneg-interval <phase1-reneg-interval> ]
            [ phase2-reneg-interval <phase2-reneg-interval> ]
            [ remote-site-enc-dom-type <remote-site-enc-dom-type>
]
            [ use-trusted-ca {internal_ca | anyCa} ]
```

```
add vpn site name <name> remote-site-link-selection load-sharing
link-selection-multiple-addrs addr <link-selection-multiple-addrs
addr> auth-method
      preshared-secret password <password>
            [ aggressive-mode-enabled false ]
            [ aggressive-mode-enabled true aggressive-mode-DH-
group <aggressive-mode-DH-group> ]
                  [ aggressive-mode-enable-peer-id { false | true
aggressive-mode-peer-id-type {domain-name | user-name} aggressive-
mode-peer-id <aggressive-mode-peer-id> } ]
                  [ aggressive-mode-enable-gateway-id { false |
true aggressive-mode-gateway-id-type {domain-name | user-name}
aggressive-mode-gateway-id <aggressive-mode-gateway-id> } ]
            [ disable-nat {true | false} ]
            [ enabled {true | false} ]
            [ enable-perfect-forward-secrecy { false | true [
phase2-dh <phase2-dh> ] } ]
            [ enc-method <enc-method> ]
            [ enc-profile <enc-profile> ]
            [ is-check-point-site { true [ enable-permanent-vpn-
tunnel {true | false} ] | false } ]
            [ link-selection-probing-method {ongoing | one-time} ]
            [ match-cert-dn { false | true match-cert-dn-string
<match-cert-dn-string> } ]
            [ match-cert-e-mail { false | true match-cert-e-mail-
string <match-cert-e-mail-string> } ]
            [ match-cert-ip {true | false} ]
            [ phase1-reneg-interval <phase1-reneg-interval> ]
            [ phase2-reneg-interval <phase2-reneg-interval> ]
            [ remote-site-enc-dom-type <remote-site-enc-dom-type>
]
            [ use-trusted-ca {internal_ca | anyCa} ]
      certificate
            [ aggressive-mode-enabled false ]
            [ aggressive-mode-enabled true aggressive-mode-DH-
group <aggressive-mode-DH-group> ]
                  [ aggressive-mode-enable-peer-id { false | true
aggressive-mode-peer-id-type {domain-name | user-name} aggressive-
mode-peer-id <aggressive-mode-peer-id> } ]
                  [ aggressive-mode-enable-gateway-id { false |
true aggressive-mode-gateway-id-type {domain-name | user-name}
aggressive-mode-gateway-id <aggressive-mode-gateway-id> } ]
            [ disable-nat {true | false} ]
            [ enabled {true | false} ]
            [ enable-perfect-forward-secrecy { false | true [
phase2-dh <phase2-dh> ] } ]
```

```
            [ enc-method <enc-method> ]
            [ enc-profile <enc-profile> ]
            [ is-check-point-site { false | true [ enable-
permanent-vpn-tunnel {true | false} ] } ]
            [ link-selection-probing-method {ongoing | one-time} ]
            [ match-cert-dn { false | true match-cert-dn-string
<match-cert-dn-string> } ]
            [ match-cert-e-mail { false | true match-cert-e-mail-
string <match-cert-e-mail-string> } ]
            [ match-cert-ip {true | false} ]
            [ phase1-reneg-interval <phase1-reneg-interval> ]
            [ phase2-reneg-interval <phase2-reneg-interval> ]
            [ remote-site-enc-dom-type <remote-site-enc-dom-type>
]
            [ use-trusted-ca {internal_ca | anyCa} ]
```

Parameters

Parameter	Description
aggressive-mode-DH-group	Configures 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.
aggressive-mode-enable-peer-id	Indicates if peer ID matching will be used. This adds a layer of security to the aggressive mode.
aggressive-mode-enabled	Main mode is used. It is less recommended if the remote site supports IPSec main mode.
aggressive-mode-gateway-id	Configures the gateway ID that will be used for matching when configured to
aggressive-mode-gateway-id-type	Configures the type of gateway ID that will be used for matching when configured.
aggressive-mode-peer-id	Configures the peer ID that will be used for matching when configured to
aggressive-mode-peer-id-type	Configures the type of peer ID that will be used for matching when configured

Parameter	Description
auth-method	Configures the type of authentication used when connecting to the remote site Press the TAB key to see the available options.
disable-nat	Disables NAT for traffic to/from the remote site. Useful when one of the internal networks contains a server
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.
enable-permanent-vpn-tunnel	VPN Tunnels are constantly kept active and as a result, make it easier to recognize malfunctions and connectivity problems
enabled	Configures whether or not the remote site is enabled
enc-method	Configures the encryption method: ■ `ike-v1` ■ `ike-v2` ■ `prefer-ike-v2`
enc-profile	Specifies the encryption profile (one of predefined profiles or custom)
is-check-point-site	Specifies the if the remote site is a Check Point Security Gateway
is-site-behind-static-nat	Specifies if the remote site is behind static NAT
link-selection-multiple-addrs addr	Configures the IP address
link-selection-probing-method	Configures the type of probing used for link selection when multiple IP addresses are configured for the remote site
match-cert-dn	Specifies if certificate matching should match the DN string in the certificate to the configured DN string
match-cert-dn-string	Configures the configured DN string for certificate matching
match-cert-e-mail	Specifies if certificate matching should match the E-mail string in the certificate to the configured E-mail string
match-cert-e-mail-string	Configures the E-mail string for certificate matching

Parameter	Description
match-cert-ip	Specifies if certificate matching should match IP address in the certificate to the site's IP address
name	Configures the Site name. A string that begins with a letter and contain up to 32 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore)
password	Configures the preshared secret (minimum 6 characters) to be used when authentication method is configured as such
phase1-reneg-interval	Configures the period (from 5 to 70000 minutes) between each IKE SA renegotiation
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	Configures the period (from 120 to 86400 seconds) between each IPSec SA renegotiation.
remote-site-enc-dom-type	Configures the method of defining the remote site's encryption domain Options: ■ `enc-dom-hidden-behind-remote-site` ■ `manually-defined-enc-dom` ■ `route-all-traffic-to-site` ■ `route-based-vpn`
remote-site-host-name	Configures the host name of the remote site
remote-site-ip-address	Configures the IPv4 address of the remote site
remote-site-ipv6-address	Configures the IPv6 address of the remote site

Parameter	Description
remote-site-link-selection	Configures the method of determining the destination IP address/s of the remote site Press the TAB key to see the available options.
static-nat-ip	Configures the external IP address through static NAT used by the remote site
use-trusted-ca	Specifies if a specific trusted CA is used for matching the remote site's certificate or all configured trusted CAs

Example Command

```
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 Group1 is-check-point-site true enable-permanent-vpn-
tunnel true disable-nat true aggressive-mode-enabled true
aggressive-mode-DH-group Group1 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
mycert 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 Group1 is-check-point-site
true enable-permanent-vpn-tunnel true disable-nat true aggressive-
mode-enabled true aggressive-mode-DH-group Group1 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 internal-ca match-cert-ip true match-cert-dn true
match-cert-dn-string mycert 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 Group1 is-check-point-site
true enable-permanent-vpn-tunnel true disable-nat true aggressive-
mode-enabled true aggressive-mode-DH-group Group1 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 Group1 is-check-
point-site true enable-permanent-vpn-tunnel true disable-nat true
aggressive-mode-enabled true aggressive-mode-DH-group Group1
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 mycert match-cert-e-mail true match-
cert-e-mail-string MyEmail@mail.com link-selection-probing-method
ongoing
```

delete vpn site name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete an existing VPN site by name.

Syntax

```
delete vpn site name <name>
```

Parameters

Parameter	Description
name	Site name Press the TAB key to see the available options.

Example Command

```
delete vpn site name site17
```

delete vpn site all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete all existing VPN sites.

Syntax

```
delete vpn site all
```

show vpn site

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of a remote VPN site.

Syntax

```
show vpn site <site>
```

Parameters

Parameter	Description
site	Site name Press the TAB key to see the available options.

Example Command

```
show vpn site site17
```

show vpn sites

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show all configured remote VPN sites.

Syntax

```
show vpn sites
```

show vpn site-to-site

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the global settings for Site-to-Site VPN.

Syntax

```
show vpn site-to-site [advanced-settings]
```

Example Output 1

```
HostName> show vpn site-to-site
mode:                           on
default-access-to-lan:          accept
track:                          log
local-encryption-domain:        auto
encryption-domains:
manual-source-ip-address:
source-ip-address-selection:    automatically
outgoing-interface-selection:   routing-table
use-dpd-responder-mode:         false
tunnel-health-monitor-mode:     tunnel-test
ike-v2-global-gateway-id:       HostName

HostName>
```

Example Output 2

```
HostName> show vpn site-to-site advanced-settings
sync-sa-with-other-cluster-members:200000
period-before-crl-valid:      7200
delete-tunnel-sas-on-tt-fail: true
udp-encapsulation-for-firewalls-and-proxies:true
copy-diff-serv-from-ipsec-packet:false
dpd-triggers-new-ike-negotiation:true
tunnel-test-from-internal:    false
outgoing-rulebase-match:      false
ike-dos-protection-known-sites:none
enable-link-selection:        true
limit-open-sas:               20
copy-diff-serv-to-ipsec-packet:true
delete-ipsec-sas-on-ikes-delete:false
keep-dont-fragment-flag-on-packet:false
log-vpn-packet-handling-errors:log
permanent-tunnel-up-track:    log
vpn-tunnel-sharing:           subnets
vpn-configuration-and-key-exchange-errors:log
no-local-dns-encrypt:         false
is-admin-access-agnostic:     true
keep-ikesa-keys:              auto-mode
maximum-concurrent-ike-negotiations:200
delete-ike-sas-from-a-dead-peer:true
local-conns-from-internal:    false
check-validity-of-ipsec-reply-packets:false
ike-dos-protection-unknown-sites:none
bypass-psl-inspection:        false
reply-from-same-ip:           true
log-vpn-outgoing-link:        none
maximum-concurrent-vpn-tunnels:10000
log-notification-for-administrative-actions:log
log-vpn-successful-key-exchange:log
reply-from-incoming-interface:false
timeout-for-an-rdp-packet-reply:10
perform-ike-using-cluster-ip: true
period-after-crl-not-valid:   1800
permanent-tunnel-down-track:  log
ike-use-largest-possible-subnets:true
no-local-conns-encrypt:       false

HostName>
```

show vpn-tunnel-info

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows all IKE (Internet Key Exchange) and IPsec (Internet Protocol Security) SAs (Security Associations) for the VPN tunnel.

Syntax

```
show vpn-tunnel-info
```

Example Output

```
HostName> show vpn-tunnel-info

Peer  192.168.32.68 , VPN_Site1 SAs:

        IKE SA <70f600e63d0bc314,472fb69a37c8a05e>

Peer  192.168.32.68 , VPN_Site1 SAs:

        IKE SA <70f600e63d0bc314,472fb69a37c8a05e>
                INBOUND:
                        1. 0xcaf05301   (i: 3)
                OUTBOUND:
                        1. 0xa9a08fc4   (i: 3)


HostName>
```

Configuring Settings for a Specified Site-to-Site VPN

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

This section provides commands to configure settings for a specified Site-to-Site VPN.

Enter this command and press the TAB key to see the available options:

```
set vpn
```

set vpn site

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures an existing Site-to-Site VPN object.

Enter this command and press the TAB key to see the available options:

```
set vpn site <VPN-site-name>
```

Syntax

```
set vpn site <VPN-site-name>
      [ aggressive-mode-enable-gateway-id { false | true
aggressive-mode-gateway-id-type <aggressive-mode-gateway-id-type>
aggressive-mode-gateway-id <aggressive-mode-gateway-id> } ]
      [ aggressive-mode-enable-peer-id { false | true aggressive-
mode-peer-id-type <aggressive-mode-peer-id-type> aggressive-mode-
peer-id <aggressive-mode-peer-id> } ]
      [ aggressive-mode-enabled { false | true aggressive-mode-DH-
group <aggressive-mode-DH-group> } ]
      [ auth-method { certificate | preshared-secret password
<password> } ]
      [ disable-nat {true | false} ]
      [ enabled {true | false} ]
      [ enable-perfect-forward-secrecy { false | true [ phase2-dh
<phase2-dh> ] } ]
      [ enc-method <enc-method> ]
      [ enc-profile <enc-profile> ]
      [ ike-v2-use-identifiers { false | true ike-v2-peer-id <ike-
v2-peer-id> gateway-id-source { override-global-identifier ike-v2-
gateway-id-override <ike-v2-gateway-id-override> | use-global-
identifier } } ]
      [ is-check-point-site { false | true [ enable-permanent-vpn-
tunnel {true | false} ] } ]
      [ is-site-behind-static-nat {true | false} ]
      [ link-selection-primary-addr <link-selection-primary-addr>
]
      [ link-selection-probing-method <link-selection-probing-
method> ]
      [ match-cert-dn { false | true match-cert-dn-string <match-
cert-dn-string> } ]
      [ match-cert-e-mail { false | true match-cert-e-mail-string
<match-cert-e-mail-string> } ]
      [ match-cert-ip {true | false} ]
      [ name <name> ]
      [ phase1-reneg-interval 5-70000 ]
      [ phase2-reneg-interval 120-86400 ]
      [ remote-site-enc-dom-type <remote-site-enc-dom-type> ]
      [ remote-site-host-name <remote-site-host-name> ]
      [ remote-site-ip-address <remote-site-ipv4-address> ]
      [ remote-site-ipv6-address <remote-site-ipv6-address> ]
      [ remote-site-link-selection <remote-site-link-selection> ]
      [ static-nat-ip <static-nat-ip> ]
      [ use-trusted-ca <use-trusted-ca> ]
```

Parameters

Parameter	Description
aggressive-mode-DH-group	Determine the strength of the key when aggressive mode is enabled The higher the group number, the stronger and more secure the key is Press the TAB key to see the available options: ■ `Group1` - Group 1 (768 bit) ■ `Group2` - Group 2 (1024 bit) ■ `Group5` - Group 5 (1536 bit) ■ `Group14` - Group 14 (2048 bit) ■ `Group19` - Group 19 (256-bit ECP) ■ `Group20` - Group 20 (384-bit ECP)
aggressive-mode-enable-gateway-id	Indicates whether to use (`true`) or not (`false`) the gateway ID matching This adds a layer of security to aggressive mode This parameter is mutually exclusive with the parameter "`aggressive-mode-enable-peer-id`"
aggressive-mode-enable-peer-id	Indicates whether to use (`true`) or not (`false`) the peer ID matching This adds a layer of security to aggressive mode This parameter is mutually exclusive with the parameter "`aggressive-mode-enable-gateway-id`"
aggressive-mode-enabled	Indicates if aggressive mode, a less secure negotiation protocol compared to the Main mode, is used It is less recommended if the remote VPN site supports IPSec main mode
aggressive-mode-gateway-id	The gateway ID that will be used for matching when configured to
aggressive-mode-gateway-id-type	Indicates the type of gateway ID that will be used for matching when configured: ■ `domain-name` ■ `user-name`
aggressive-mode-peer-id	The peer ID that will be used for matching when configured to

Parameter	Description
aggressive-mode-peer-id-type	Indicates the type of peer ID that will be used for matching when configured: ■ `domain-name` ■ `user-name`
auth-method	Indicates the type of authentication used when connecting to the remote VPN site Press TAB to see available options
disable-nat	Disables (`true`) or enables (`false`) the NAT for traffic to or from the remote VPN site Useful when one of the internal networks contains a server
enable-perfect-forward-secrecy	Enables (`true`) or disables (`false`) the Perfect Forward Secrecy When enabled, it makes that a session key will not be compromised if one of the (long-term) private keys is compromised in the future
enable-permanent-vpn-tunnel	Controls whether to constantly keep the VPN Tunnels active (`true`) or not (`false`) If a VPN Tunnel is active, it is easier to recognize malfunctions and connectivity problems
enabled	Indicates whether the remote VPN site is enabled (`true`) or not (`false`)
enc-method	Indicates which encryption method is used: ■ `ike-v1` ■ `ike-v2` ■ `prefer-ike-v2`
enc-profile	Encryption profile (one of predefined profiles or custom)
gateway-id-source	Indicates whether the gateway ID in the IKEv2 encryption protocol is the global Gateway ID or an overridden one Press TAB to see available options
ike-v2-gateway-id-override	The gateway ID when overriding the global gateway ID in the IKEv2 encryption protocol
ike-v2-peer-id	The peer ID used in the IKEv2 encryption protocol
ike-v2-use-identifiers	Indicates whether the IKEv2 encryption protocol should use peer ID and gateway ID identifiers

Parameter	Description
is-check-point-site	Controls whether the remote VPN site is connected through a Check Point Security Gateway (`true`) or not (`false`)
is-site-behind-static-nat	When connection type is IP address, this indicates if it is behind a static NAT (`true`) or not (`false`)
link-selection-primary-addr	Specifies the primary IP address for the link selection
link-selection-probing-method	The type of probing used for link selection when multiple IP addresses are configured for the remote VPN site ■ `ongoing` ■ `one-time`
match-cert-dn	Specifies if certificate matching should (`true`) or should not (`false`) match the DN string in the certificate to the configured DN string
match-cert-dn-string	Specifies the configured DN string for certificate matching
match-cert-e-mail	Indicates if certificate matching should (`true`) or should not (`false`) match the E-mail string in the certificate to the configured E-mail string
match-cert-e-mail-string	Specifies the configured E-mail string for certificate matching
match-cert-ip	Indicates if certificate matching should (`true`) or should not (`false`) match IP address in the certificate to the site's IP address
name	Configures the new VPN site name
password	Pre-shared secret (minimum 6 characters) to be used when authentication method is configured as such
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 Press the TAB key to see the available options: ■ `Group1` - Group 1 (768 bit) ■ `Group2` - Group 2 (1024 bit) ■ `Group5` - Group 5 (1536 bit) ■ `Group14` - Group 14 (2048 bit) ■ `Group19` - Group 19 (256-bit ECP) ■ `Group20` - Group 20 (384-bit ECP)

Parameter	Description
phase2-reneg-interval	The period (between 120 and 86400 minutes, default 3600) between each IPsec SA renegotiation
phase1-reneg-interval	The period (between 5 and 70000 minutes, default 1440) between each IKE SA renegotiation
remote-site-enc-dom-type	The method of defining the remote VPN site's encryption domain. Press the TAB key to see the available options: ■ `enc-dom-hidden-behind-remote-site` ■ `manually-defined-enc-dom` ■ `route-all-traffic-to-site` ■ `route-based-vpn`
remote-site-host-name	Indicates the remote VPN site's host name when the link selection method is configured as such
remote-site-ip-address	Indicates the remote VPN site's single IPv4 address when the link selection method is configured as such
remote-site-ipv6-address	Indicates the remote VPN site's single IPv6 address when the link selection method is configured as such
remote-site-link-selection	Indicates the method of determining the destination IP address(es) of the remote VPN site: ■ `connection-initiated-only-from-remote-site` ■ `high-availability` ■ `host-name` ■ `ip-address` ■ `load-sharing`
site	Name of the existing VPN site Press the TAB key to see the available options.
static-nat-ip	Indicates an external routable IP address via static NAT used by the remote VPN site, when configured as such
use-trusted-ca	Indicates whether to use an Internal Certificate Authority or any configured Certificate Authority for matching the remote VPN site's certificate: ■ `internal_ca` ■ `anyCa`

Example Command

```
set vpn site site17 enabled true remote-site-enc-dom-type
manually-defined-enc-dom enc-profile virtual phase1-reneg-interval
3600 phase2-reneg-interval 7200 enable-perfect-forward-secrecy
true phase2-dh Group1 is-check-point-site true enable-permanent-
vpn-tunnel true disable-nat true aggressive-mode-enabled true
aggressive-mode-DH-group Group1 aggressive-mode-enable-peer-id
true aggressive-mode-peer-id-type domain-name aggressive-mode-
peer-id vpnAggressiveModePeerId ike-v2-use-identifiers true ike-
v2-peer-id vpnAggressiveModePeerId gateway-id-source override-
global-identifier ike-v2-gateway-id-override
vpnAggressiveModePeerId enc-method ike-v1 use-trusted-ca internal_
ca match-cert-ip true match-cert-dn true match-cert-dn-string
mycert 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 remote-site-ipv6-
address 2001:db8:3333:4444:5555:6666:7777:8888 is-site-behind-
static-nat true static-nat-ip 192.168.20.30 auth-method preshared-
secret password 12345678 link-selection-primary-addr 192.168.20.30
```

set vpn site ... fqdn

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

The user can set up a VPN connection with Harmony Connect.

IKEv2 is supported with a new key type for FQDN.

This commands allows the user to configure the FQDN for each VPN site.

This is the key value for the FQDN key type and must be coordinated with the Harmony Connect site.

Note - The default key value is the system's general FQDN.

Syntax

```
set vpn site <site_name> fqdn <fqdn>
```

Parameters

Parameter	Description
site	Name of the site.
fqdn	Key value of the FQDN key type.

Example Command

```
set vpn site MySite fqdn 123abc
```

set vpn site add remote-site-enc-dom-network-obj

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Specifies the Network Object name. Press the TAB key to see the available options.
site	Specifies the Site name. Press the TAB key to see the available options.

Example Command

```
set vpn site site17 add remote-site-enc-dom-network-obj
MyEncDomNetwork
```

set vpn site remove remote-site-enc-dom-network-obj

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Specifies the Network Object name. Press the TAB key to see the available options.
site	Specifies the Site name. Press the TAB key to see the available options.

Example Command

```
set vpn site site17 remove remote-site-enc-dom-network-obj
MyEncDomNetwork
```

set vpn site remove-all remote-site-enc-dom-network-obj

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Removes all network objects from the encryption 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	Specifies the Network Object name. Press the TAB key to see the available options.
site	Specifies the Site name. Press the TAB key to see the available options.

Example Command

```
set vpn site site17 remove-all remote-site-enc-dom-network-obj
MyEncDomNetwork
```

set vpn site add remote-site-enc-dom-route-excluded-network-obj

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Adds ability to exclude a network object or a particular IP address from being encrypted and sent through the site when "Route all traffic" is configured.

Note - You must first create the site and the network object.

See *"set vpn site add remote-site-enc-dom-network-obj" on page 1376*.

Syntax

```
set vpn site <site> add remote-site-enc-dom-route-excluded-
network-obj <network_object_name>
```

Parameters

Parameter	Description
site	Specifies the Site name. Press the TAB key to see the available options.
network_object_name	Specifies the Network Object to exclude. Press the TAB key to see the available options.

Example Command

```
set vpn site site17 add remote-site-enc-dom-route-excluded-
network-obj MyEncDomNetwork
```

set vpn site add link-selection-multiple-addrs

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Configures the IP address.
site	Specifies the Site name. Press the TAB key to see the available options.

Example Command

```
set vpn site site17 add link-selection-multiple-addrs addr 192.168.1.1
```

set vpn site remove link-selection-multiple-addrs

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Specifies the IP address. Press the TAB key to see the available options.
site	Specifies the Site name. Press the TAB key to see the available options.

Example Command

```
set vpn site site17 remove link-selection-multiple-addrs addr
192.168.1.1
```

set vpn site remove-all link-selection-multiple-addrs

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	Specifies the IP address. Press the TAB key to see the available options.
site	Specifies the Site name. Press the TAB key to see the available options.

Example Command

```
set vpn site site17 remove-all link-selection-multiple-addrs addr
192.168.1.1
```

set vpn site add custom-enc-phase1-enc

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options. ■ 3DES ■ AES-128 ■ AES-256 ■ CAST ■ DES
site	VPN site name Press the TAB key to see the available options.

Example Command

```
set vpn site site17 add custom-enc-phase1-enc AES-256
```

set vpn site remove custom-enc-phase1-enc

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options. ■ 3DES ■ AES-128 ■ AES-256 ■ CAST ■ DES
site	VPN site name Press the TAB key to see the available options.

Example Command

```
set vpn site site17 remove custom-enc-phase1-enc AES-256
```

set vpn site remove-all custom-enc-phase1-enc

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options. ■ 3DES ■ AES-128 ■ AES-256 ■ CAST ■ DES
site	VPN site name Press the TAB key to see the available options.

Example Command

```
set vpn site site17 remove-all custom-enc-phase1-enc AES-256
```

set vpn site add custom-enc-phase1-auth

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options. ■ AES-XCBC ■ MD5 ■ SHA1 ■ SHA256
site	VPN site name Press the TAB key to see the available options.

Example Command

```
set vpn site site17 add custom-enc-phase1-auth SHA256
```

set vpn site remove custom-enc-phase1-auth

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options.
site	VPN site name Press the TAB key to see the available options.

Example Command

```
set vpn site site17 remove custom-enc-phase1-auth AES-256
```

set vpn site remove-all custom-enc-phase1-auth

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options.
site	VPN site name Press the TAB key to see the available options.

Example Command

```
set vpn site site17 remove-all custom-enc-phase1-auth AES-256
```

set vpn site add custom-enc-phase1-dh-group

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options. ■ `Group1` ■ `Group2` ■ `Group5` ■ `Group14`
site	VPN site name Press the TAB key to see the available options.

Example Command

```
set vpn site site17 add custom-enc-phase1-dh-group Group1
```

set vpn site remove custom-enc-phase1-dh-group

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options. ■ Group1 ■ Group2 ■ Group5 ■ Group14
site	VPN site name Press the TAB key to see the available options.

Example Command

```
set vpn site site17 remove custom-enc-phase1-dh-group Group1
```

set vpn site remove-all custom-enc-phase1-dh-group

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options. ■ Group1 ■ Group2 ■ Group5 ■ Group14
site	VPN site name Press the TAB key to see the available options.

Example Command

```
set vpn site site17 remove-all custom-enc-phase1-dh-group Group1
```

set vpn site add custom-enc-phase2-enc

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options. ■ 3DES ■ AES-128 ■ AES-256 ■ AES-GCM-128 ■ AES-GCM-256 ■ CAST ■ CAST-40 ■ DES ■ DES-40CP
site	Specifies the Site name. Press the TAB key to see the available options.

Example Command

```
set vpn site site17 add custom-enc-phase2-enc AES-256
```

set vpn site remove custom-enc-phase2-enc

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options. ■ 3DES ■ AES-128 ■ AES-256 ■ AES-GCM-128 ■ AES-GCM-256 ■ CAST ■ CAST-40 ■ DES ■ DES-40CP
site	VPN site name Press the TAB key to see the available options.

Example Command

```
set vpn site site17 remove custom-enc-phase2-enc AES-256
```

set vpn site remove-all custom-enc-phase2-enc

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options. ■ 3DES ■ AES-128 ■ AES-256 ■ AES-GCM-128 ■ AES-GCM-256 ■ CAST ■ CAST-40 ■ DES ■ DES-40CP
site	Site name Press the TAB key to see the available options.

Example Command

```
set vpn site site17 remove-all custom-enc-phase2-enc AES-256
```

set vpn site add custom-enc-phase2-auth

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options. ■ AES-XCBC ■ MD5 ■ SHA1 ■ SHA256
site	VPN site name Press the TAB key to see the available options.

Example Command

```
set vpn site site17 add custom-enc-phase2-auth SHA256
```

set vpn site remove custom-enc-phase2-auth

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options. ■ AES-XCBC ■ MD5 ■ SHA1 ■ SHA256
site	VPN site name Press the TAB key to see the available options.

Example Command

```
set vpn site site17 remove custom-enc-phase2-auth SHA256
```

set vpn site remove-all custom-enc-phase2-auth

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options. ■ AES-XCBC ■ MD5 ■ SHA1 ■ SHA256
site	VPN site name Press the TAB key to see the available options.

Example Command

```
set vpn site site17 remove-all custom-enc-phase2-auth SHA256
```

Configuring Global Settings for Site-to-Site VPN

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

This section provides commands to configure global settings for Site-to-Site VPN.

Enter this command and press the TAB key to see the available options:

```
set vpn site-to-site advanced-settings
```

set vpn site-to-site

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure global settings for VPN site to site.

Syntax

```
set vpn site-to-site
      [ default-access-to-lan {accept | block} ]
      [ local-encryption-domain {auto | manual} ]
      [ manual-source-ip-address <manual-source-ip-address> ]
      [ mode {true | false} ]
      [ outgoing-interface-selection {routing-table | route-based-
probing} ]
      [ source-ip-address-selection {automatically | manually} ]
      [ track {log | none} ]
      [ tunnel-health-monitor-mode {dpd | tunnel-test}]
      [ use-dpd-responder-mode {true | false} ]
```

Parameters

Parameter	Description
default-access-to-lan	Allows (`accept`) or drops (`block`) the traffic from remote VPN sites
local-encryption-domain	Configures the local encryption domain automatically (using the local networks) or manually
manual-source-ip-address	A manually configured source IP address to be used (if configured to) for VPN tunnels
mode	Enables (`true`) or disables (`false`) the Site -to-Site VPN
outgoing-interface-selection	Configures the method, according to which the outgoing interface is selected for VPN traffic: ▪ `routing-table` - Selects an outgoing interface based on the routing table ▪ `route-based-probing` - Selects an outgoing interface based on the route probing

Parameter	Description
source-ip-address-selection	Selects whether the source IP address is chosen automatically according to the outgoing interface, or configured manually
track	Enables (`log`) or disables (`none`) the logging of traffic from remote VPN sites
tunnel-health-monitor-mode	Configures the VPN tunnel monitoring mechanism: ■ `dpd` - DPD mode ■ `tunnel-test` - Permanent Tunnel
use-dpd-responder-mode	Selects whether to use the DPD responder mode (`true`) or Permanent Tunnel based on the DPD mode (`false`)

Example Command

```
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 bypass-psl-inspection

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether VPN traffic bypasses the PSL inspection (Application Control, URL Filtering, IPS, Anti-Virus, Anti-Bot, Threat Prevention, Threat Emulation).

The default is "`false`".

Syntax

```
set vpn site-to-site advanced-settings bypass-psl-inspection {true
| false}
```

Example Command

```
set vpn site-to-site advanced-settings bypass-psl-inspection false
```

set vpn site-to-site check-validity-of-ipsec-reply-packets

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to check validity of IPsec reply packets.

The default is "`false`".

Syntax

```
set vpn site-to-site advanced-settings check-validity-of-ipsec-
reply-packets {true | false}
```

Example Command

```
set vpn site-to-site advanced-settings check-validity-of-ipsec-
reply-packets true
```

set vpn site-to-site copy-diff-serv-from-ipsec-packet

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to copy the DiffServ mark from encrypted / decrypted IPsec packets.

The default is "`false`".

Syntax

```
set vpn site-to-site advanced-settings copy-diff-serv-from-ipsec-
packet {true | false}
```

Example Command

```
set vpn site-to-site advanced-settings copy-diff-serv-from-ipsec-
packet true
```

set vpn site-to-site copy-diff-serv-to-ipsec-packet

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to copy the DiffServ mark to encrypted and decrypted IPsec packets.

The default is "`true`".

Syntax

```
set vpn site-to-site advanced-settings copy-diff-serv-to-ipsec-
packet {true | false}
```

Example Command

```
set vpn site-to-site advanced-settings copy-diff-serv-to-ipsec-
packet true
```

set vpn site-to-site delete-ike-sas-from-a-dead-peer

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to delete IKE SAs for a dead VPN peer.

The default is "`true`".

Syntax

```
set vpn site-to-site advanced-settings delete-ike-sas-from-a-dead-
peer {true | false}
```

Example Command

```
set vpn site-to-site advanced-settings delete-ike-sas-from-a-dead-
peer true
```

set vpn site-to-site delete-ipsec-sas-on-ikes-delete

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to delete IPsec SAs when the corresponding IKE SA is deleted.

Syntax

```
set vpn site-to-site advanced-settings delete-ipsec-sas-on-ikes-
delete {true | false}
```

Parameters

Parameter	Description
delete-ipsec-sas-on-ikes-delete	Deletes (`true`) or keeps (`false`) the IPsec SAs. The default is "`false`".

Example Command

```
set vpn site-to-site advanced-settings delete-ipsec-sas-on-ikes-
delete true
```

set vpn site-to-site delete-tunnel-sas-on-tt-fail

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to delete the tunnel SAs for an applicable VPN peer when Permanent VPN Tunnels are enabled and a Tunnel Test fails.

The default is "`true`".

Note - High Availability Cluster does **not** support this feature.

Syntax

```
set vpn site-to-site advanced-settings delete-tunnel-sas-on-tt-
fail {true | false}
```

Example Command

```
set vpn site-to-site advanced-settings delete-tunnel-sas-on-tt-
fail true
```

set vpn site-to-site dpd-triggers-new-ike-negotiation

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether DPD triggers a new IKE negotiation.

The default is "`true`".

Syntax

```
set vpn site-to-site advanced-settings dpd-triggers-new-ike-
negotiation {true | false}
```

Example Command

```
set vpn site-to-site advanced-settings dpd-triggers-new-ike-
negotiation true
```

set vpn site-to-site enable-link-selection

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether encrypted packets are routed through the best interface according to the VPN peer's IP address or probing.

The default is "`true`".

Best Practice - We do **not** recommended to change the value to "`false`".

Syntax

```
set vpn site-to-site advanced-settings enable-link-selection {true
| false}
```

Example Command

```
set vpn site-to-site advanced-settings enable-link-selection true
```

set vpn site-to-site enc-dom manual add name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options.

Example Command

```
set vpn site-to-site enc-dom manual add name MyNetwork
```

set vpn site-to-site enc-dom manual remove name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Press the TAB key to see the available options.

Example Command

```
set vpn site-to-site enc-dom manual remove name MyNetwork
```

set vpn site-to-site enc-dom manual remove-all name

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Removes the specified settings from the local encryption domain for Site-to-Site VPN.

Syntax

```
set vpn site-to-site enc-dom manual remove-all name <parameter>
```

Parameters

Parameter	Description
parameter	Press the TAB key to see the available options.: ■ `default-access-to-lan` - Allows traffic from remote VPN sites (by default) ■ `ike-v2-global-gateway-id` - Configures the global gateway identifier for the IKEv2 encryption protocol ■ `local-encryption-domain` - Indicates if the local encryption domain is configured manually or determined automatically using the local networks ■ `manual-source-ip-address` - Configures the source IP address for the VPN tunnels ■ `mode` - Enables or disables the Site-to-Site VPN ■ `outgoing-interface-selection` - Configures the method, according to which an outgoing interface is selected for VPN traffic ■ `source-ip-address-selection` - Select whether the source IP address is chosen automatically according to the outgoing interface, or configured manually ■ `track` - Enables and disables the logging for traffic from remote VPN sites ■ `tunnel-health-monitor-mode` - Configures the VPN tunnel monitor mechanism (can work with Permanent Tunnels or with the DPD mode) ■ `use-dpd-responder-mode` - Enables the DPD responder mode, or enables a Permanent Tunnel based on the DPD mode

Example Command

```
set vpn site-to-site enc-dom manual remove-all name track log
```

set vpn site-to-site ike-use-largest-possible-subnets

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to join adjacent subnets in IKE Quick Mode.

The default is "`true`".

Syntax

```
set vpn site-to-site advanced-settings ike-use-largest-possible-
subnets {true | false}
```

Example Command

```
set vpn site-to-site advanced-settings ike-use-largest-possible-
subnets true
```

set vpn site-to-site ike-dos-protection-known-sites

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls the protection against IKE DoS from known IP addresses.

Syntax

```
set vpn site-to-site advanced-settings ike-dos-protection-known-
sites <method>
```

Parameters

Parameter	Description
<method>	Configures the IKE DoS protection and its detection method: ■ `stateless` - Detects potential attackers based on stateless cookies ■ `puzzles` - Detects potential attackers based on puzzles (stateless cookies are hidden in puzzles) ■ `none` - Disables the IKE DoS protection (this is the default)

Example Command

```
set vpn site-to-site advanced-settings ike-dos-protection-known-
sites stateless
```

set vpn site-to-site ike-dos-protection-unknown-sites

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls the protection against IKE DoS from unidentified IP addresses.

Syntax

```
set vpn site-to-site advanced-settings ike-dos-protection-unknown-
sites <method>
```

Parameters

Parameter	Description
<method>	Configures the IKE DoS protection and its detection method: ■ `stateless` - Detects potential attackers based on stateless cookies ■ `puzzles` - Detects potential attackers based on puzzles (stateless cookies are hidden in puzzles) ■ `none` - Disables the IKE DoS protection (this is the default)

Example Command

```
set vpn site-to-site advanced-settings ike-dos-protection-unknown-
sites stateless
```

set vpn site-to-site is-admin-access-agnostic

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to exclude administrator access traffic to the appliance from being routed to a remote VPN site, even if all traffic should be routed to it.

The default is "`true`".

Syntax

```
set vpn site-to-site advanced-settings is-admin-access-agnostic
{true | false}
```

Example Command

```
set vpn site-to-site advanced-settings is-admin-access-agnostic
true
```

set vpn site-to-site keep-dont-fragment-flag-on-packet

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to keep the "Don't Fragment" flag in the packets during encryption and decryption.

Syntax

```
set vpn site-to-site advanced-settings keep-dont-fragment-flag-on-
packet {true | false}
```

Parameters

Parameter	Description
keep-dont-fragment-flag-on-packet	Keeps (`true`) or removes (`false`) the "Don't Fragment" flag. The default is "`false`".

Example Command

```
set vpn site-to-site advanced-settings keep-dont-fragment-flag-on-
packet true
```

set vpn site-to-site keep-ikesa-keys

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to keep IKE SA Keys.

Syntax

```
set vpn site-to-site advanced-settings keep-ikesa-keys <keep-ikesa-keys>
```

Parameters

Parameter	Description
keep-ikesa-keys	▪ `auto-mode` - Automatic mode (this is the default) ▪ `do-not-keep` - Does not keep the keys ▪ `keep` - Keeps the keys

Example Command

```
set vpn site-to-site advanced-settings keep-ikesa-keys do-not-keep
```

set vpn site-to-site limit-open-sas

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the maximum number of open SAs for each VPN peer.

Syntax

```
set vpn site-to-site advanced-settings limit-open-sas <threshold>
```

Parameters

Parameter	Description
<threshold>	An integer between 1 and 4,294,967,295. The default is 20.

Example Command

```
set vpn site-to-site advanced-settings limit-open-sas 50
```

set vpn site-to-site local-conns-from-internal

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether encrypted connections originating from this gateway use an internal interface's IP address as the connection's source IP address.

The default is "`false`".

Syntax

```
set vpn site-to-site advanced-settings local-conns-from-internal
{true | false}
```

Example Command

```
set vpn site-to-site advanced-settings local-conns-from-internal
false
```

set vpn site-to-site log-notification-for-administrative-actions

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to generate logs for VPN administrative events (for example, when a certificate is about to expire).

The default is to generate such logs.

Syntax

```
set vpn site-to-site advanced-settings log-notification-for-
administrative-actions {log | none}
```

Example Command

```
set vpn site-to-site advanced-settings log-notification-for-
administrative-actions none
```

set vpn site-to-site log-vpn-outgoing-link

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the logging of the outgoing VPN link.

Syntax

```
set vpn site-to-site advanced-settings log-vpn-outgoing-link
{alert | log | none}
```

Parameters

Parameter	Description
log-vpn-outgoing-link	Configures the logging: ■ `alert` - Generates only alerts ■ `log` - Generates only logs (this is the default) ■ `none` - Does not generate alerts or logs

Example Command

```
set vpn site-to-site advanced-settings log-vpn-outgoing-link alert
```

set vpn site-to-site log-vpn-packet-handling-errors

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the logging for VPN packet handling errors.

Syntax

```
set vpn site-to-site advanced-settings log-vpn-packet-handling-
errors {alert | log | none}
```

Parameters

Parameter	Description
log-vpn-packet-handling-errors	Configures the logging: ■ `alert` - Generates only alerts ■ `log` - Generates only logs (this is the default) ■ `none` - Does not generate alerts or logs

Example Command

```
set vpn site-to-site advanced-settings log-vpn-packet-handling-
errors alert
```

set vpn site-to-site log-vpn-successful-key-exchange

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the logging for VPN successful key exchange.

Syntax

```
set vpn site-to-site advanced-settings log-vpn-successful-key-
exchange {alert | log | none}
```

Parameters

Parameter	Description
log-vpn-successful-key-exchange	Configures the logging: ■ `alert` - Generates only alerts ■ `log` - Generates only logs (this is the default) ■ `none` - Does not generate alerts or logs

Example Command

```
set vpn site-to-site advanced-settings log-vpn-successful-key-
exchange alert
```

set vpn site-to-site maximum-concurrent-ike-negotiations

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the maximum number of concurrent VPN IKE negotiations.

Syntax

```
set vpn site-to-site advanced-settings maximum-concurrent-ike-
negotiations <threshold>
```

Parameters

Parameter	Description
<threshold>	An integer between 1 and 4,294,967,295. The default is 200.

Example Command

```
set vpn site-to-site advanced-settings maximum-concurrent-ike-
negotiations 300
```

set vpn site-to-site maximum-concurrent-vpn-tunnels

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the maximum number of concurrent VPN tunnels

Syntax

```
set vpn site-to-site advanced-settings maximum-concurrent-vpn-
tunnels <threshold>
```

Parameters

Parameter	Description
<threshold>	An integer between 1 and 4,294,967,295. The default is 10,000.

Example Command

```
set vpn site-to-site advanced-settings maximum-concurrent-vpn-
tunnels 5000
```

set vpn site-to-site no-local-conns-encrypt

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to exclude the Internet connection's IP address from the local encryption domain.

Packets do not go through a VPN tunnel, if their original source IP address or destination IP address is the local gateway's Internet connection IP address.

This parameter may be useful when all traffic originating from the gateway is hidden behind Hide NAT.

The default is "`false`".

Syntax

```
set vpn site-to-site advanced-settings no-local-conns-encrypt
{true | false}
```

Example Command

```
set vpn site-to-site advanced-settings no-local-conns-encrypt
false
```

set vpn site-to-site no-local-dns-encrypt

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to encrypt DNS requests originating from the appliance.

This applies when a configured DNS server is in a VPN peer's encryption domain.

The default is "`false`".

Syntax

```
set vpn site-to-site advanced-settings no-local-dns-encrypt {true
| false}
```

Example Command

```
set vpn site-to-site advanced-settings no-local-dns-encrypt true
```

set vpn site-to-site outgoing-rulebase-match

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to match traffic to the Internet from VPN peers (that route all their traffic through this gateway) on the Outgoing rulebase.

The default is "`false`".

Syntax

```
set vpn site-to-site advanced-settings outgoing-rulebase-match
{true | false}
```

Example Command

```
set vpn site-to-site advanced-settings outgoing-rulebase-match
false
```

set vpn site-to-site period-after-crl-not-valid

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the time (in seconds), after which a revoked certificate of a remote VPN site remains valid.

This is to allow a wider window for CRL validity in case of mismatch in clock on the VPN sites.

Syntax

```
set vpn site-to-site advanced-settings period-after-crl-not-valid
<threshold>
```

Parameters

Parameter	Description
<threshold>	An integer between 0 and 4,294,967,295. The default is 1800.

Example Command

```
set vpn site-to-site advanced-settings period-after-crl-not-valid
2000
```

set vpn site-to-site period-before-crl-valid

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the time (in seconds), during which a certificate is considered valid prior to the time set by the Certificate Authority.

This is to allow a wider window for CRL validity in case of mismatch in clock on the VPN sites.

Syntax

```
set vpn site-to-site advanced-settings period-before-crl-valid
<threshold>
```

Parameters

Parameter	Description
<threshold>	An integer between 0 and 4,294,967,295. The default is 7200.

Example Command

```
set vpn site-to-site advanced-settings period-before-crl-valid 5
```

set vpn site-to-site perform-ike-using-cluster-ip

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

In a High Availability Cluster, controls whether to perform IKE using a cluster IP address.

The default is "`true`".

Syntax

```
set vpn site-to-site advanced-settings perform-ike-using-cluster-
ip {true | false}
```

Example Command

```
set vpn site-to-site advanced-settings perform-ike-using-cluster-
ip true
```

set vpn site-to-site permanent-tunnel-down-track

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the logging for Permanent VPN Tunnel going down.

Syntax

```
set vpn site-to-site advanced-settings permanent-tunnel-down-track
<permanent-tunnel-down-track>
```

Parameters

Parameter	Description
permanent-tunnel-down-track	Configures the logging: ■ `alert` - Generates only alerts ■ `log` - Generates only logs (this is the default) ■ `none` - Does not generate alerts or logs

Example Command

```
set vpn site-to-site advanced-settings permanent-tunnel-down-track
alert
```

set vpn site-to-site permanent-tunnel-up-track

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the logging for Permanent VPN Tunnel going up.

Syntax

```
set vpn site-to-site advanced-settings permanent-tunnel-up-track
{alert | log | none}
```

Parameters

Parameter	Description
permanent-tunnel-up-track	Configures the logging: ■ `alert` - Generates only alerts ■ `log` - Generates only logs (this is the default) ■ `none` - Does not generate alerts or logs

Example Command

```
set vpn site-to-site advanced-settings permanent-tunnel-up-track
none
```

set vpn site-to-site reply-from-incoming-interface

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to send a reply from the same incoming interface (for IKE and RDP sessions) when remote VPN site starts a VPN tunnel connection.

The default is "`false`".

Syntax

```
set vpn site-to-site advanced-settings reply-from-incoming-
interface {true | false}
```

Example Command

```
set vpn site-to-site advanced-settings reply-from-incoming-
interface true
```

set vpn site-to-site reply-from-same-ip

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls which source IP address to use in IKE sessions when replying to incoming connections.

Syntax

```
set vpn site-to-site advanced-settings reply-from-same-ip {true |
false}
```

Parameters

Parameter	Description
reply-from-same-ip	Controls the source IP address to use in IKE sessions: ■ `true` - Uses the IP address according to destination (this is the default) ■ `false` - Uses the IP address according to the general source IP address configured for Link Selection

Example Command

```
set vpn site-to-site advanced-settings reply-from-same-ip true
```

set vpn site-to-site sync-sa-with-other-cluster-members

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls the number of packets when this Cluster Member must synchronize its VPN SA with other Cluster Members.

Syntax

```
set vpn site-to-site advanced-settings sync-sa-with-other-cluster-
members <threshold>
```

Parameters

Parameter	Description
<threshold>	An integer between -4,503,599,627,370,495 and 4,503,599,627,370,495. The default is 200,000.

Example Command

```
set vpn site-to-site advanced-settings sync-sa-with-other-cluster-
members 200000
```

set vpn site-to-site timeout-for-an-rdp-packet-reply

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the timeout (in seconds) for an RDP packet reply.

Syntax

```
set vpn site-to-site advanced-settings timeout-for-an-rdp-packet-
reply <threshold>
```

Parameters

Parameter	Description
<threshold>	An integer between 0 and 4,294,967,295. The default is 10.

Example Command

```
set vpn site-to-site advanced-settings timeout-for-an-rdp-packet-
reply 20
```

set vpn site-to-site tunnel-test-from-internal

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to perform Tunnel Tests using an internal IP address, which is part of the local encryption domain.

The default is "`false`".

Syntax

```
set vpn site-to-site advanced-settings tunnel-test-from-internal
{true | false}
```

Example Command

```
set vpn site-to-site advanced-settings tunnel-test-from-internal
true
```

set vpn site-to-site udp-encapsulation-for-firewalls-and-proxies

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls whether to enable the industry standard NAT traversal (UDP encapsulation).

When enabled, it is possible to establish a VPN tunnel even when the remote VPN site is behind a NAT device.

The default is "`true`".

Syntax

```
set vpn site-to-site advanced-settings udp-encapsulation-for-
firewalls-and-proxies {true | false}
```

Parameters

Parameter	Description
n/a	

Example Command

```
set vpn site-to-site advanced-settings udp-encapsulation-for-
firewalls-and-proxies true
```

set vpn site-to-site vpn-configuration-and-key-exchange-errors

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the logging of VPN configuration errors and key exchange errors.

Syntax

```
set vpn site-to-site advanced-settings vpn-configuration-and-key-
exchange-errors {alert | log | none}
```

Parameters

Parameter	Description
vpn-configuration-and-key-exchange-errors	Configures the logging: ■ `alert` - Generates only alerts ■ `log` - Generates only logs (this is the default) ■ `none` - Does not generate alerts or logs

Example Command

```
set vpn site-to-site advanced-settings vpn-configuration-and-key-
exchange-errors alert
```

set vpn site-to-site vpn-tunnel-sharing

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the condition for creating new VPN tunnels.

Syntax

```
set vpn site-to-site advanced-settings vpn-tunnel-sharing <vpn-tunnel-sharing>
```

Parameters

Parameter	Description
vpn-tunnel-sharing	Configures the condition for creating new VPN tunnels: ■ `hosts` - Creates a VPN tunnel for each pair of hosts that communicate behind the VPN Gateways ■ `gateways` - Creates a VPN tunnel for each peer VPN Gateway ■ `subnets` - Creates a VPN tunnel for each pair of subnets that communicate behind the VPN Gateways (this is the default)

Example Command

```
set vpn site-to-site advanced-settings vpn-tunnel-sharing gateways
```

TunnelUtil Tool

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Launches the VPN TunnelUtil tool to:

- List IKE and IPsec SAs
- Delete IKE and IPsec SAs

Syntax

```
vpn tunnelutil
```

Example Output

```
HostName> vpn tunnelutil

**********     Select Option     **********

(1)               List all IKE SAs
(2)             * List all IPsec SAs
(3)               List all IKE SAs for a given peer (GW) or user
(Client)
(4)             * List all IPsec SAs for a given peer (GW) or user
(Client)
(5)               Delete all IPsec SAs for a given peer (GW)
(6)               Delete all IPsec SAs for a given User (Client)
(7)               Delete all IPsec+IKE SAs for a given peer (GW)
(8)               Delete all IPsec+IKE SAs for a given User
(Client)
(9)               Delete all IPsec SAs for ALL peers and users
(0)               Delete all IPsec+IKE SAs for ALL peers and users

* To list data for a specific CoreXL instance, append "-i
<instance number>" to your selection.

(Q)               Quit

*****************************************
```

Managing the VPN Driver

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

- Installs the VPN kernel (vpnk) and connects it to the Firewall kernel (fwk).
- Disconnects it from the Firewall kernel (fwk) and uninstall the VPN kernel (vpnk).
- Shows the status of the VPN kernel.

Syntax

```
vpn drv {on | off | reset | stat}
```

Parameters

Parameter	Description
`on`	Starts the VPN kernel.
`off`	Stops the VPN kernel.
`reset`	Resets the VPN kernel.
`stat`	Shows the status of the VPN kernel.

Example Command

```
vpn drv on
```

Debugging VPN

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Instructs the VPN daemon `vpnd` to write debug messages to the `$FWDIR/log/vpnd.elg*` and `$FWDIR/log/ike.elg*` log files.

Debugging of the VPN daemon takes place according to Debug Topics and Debug Levels:

- A Debug Topic is a specific area, on which to perform debugging.

  For example, if the Debug Topic is `LDAP`, all traffic between the VPN daemon and the LDAP server is written to the log file.

  Check Point Support provides the specific Debug Topics when needed.

- Debug Levels range from 1 (least informative) to 5 (most informative - write all debug messages).

For more information, see sk180488 - How to collect a debug for VPN issues.

Syntax

```
vpn debug
      on [<Debug_Topic>=<Debug_Level>]
      off
      ikeon [-s <Size_in_MB>]
      ikeoff
      trunc [<Debug_Topic>=<Debug_Level>]
      truncon [<Debug_Topic>=<Debug_Level>]
      truncoff
      timeon [<Seconds>]
      timeoff
      ikefail [-s <Size_in_MB>]
      mon
      moff
      say ["String"]
      tunnel [<Level>]
```

Parameters

Parameter	Description
No Parameters	Shows the built-in usage.

Parameter	Description
`on`	Turns on high level VPN debug. Information is written in the `$FWDIR/log/vpnd.elg*` files.
<Debug_ Topic >=<Debug_ Level>	Specifies the Debug Topic and the Debug Level. *Check Point Support* provides these. **Best Practice** - Run this command to start the debug: `vpn debug trunc ALL=5`

`off`	Turns off all VPN debug.
	Best Practice - Run one of these commands to stop the VPND debug:
	`vpn debug off`
	`vpn debug truncoff`

`ikeon [-s` *<Size_in_ MB>*`]`	Turns on the IKE debug. Information is written in the `$FWDIR/log/ike.elg*` files. You can specify the size of the `$FWDIR/log/ike.elg` file, when to perform the log rotation (close the current active file, rename it, open a new active file).
`ikeoff`	Turns off IKE debug. Run this command to stop the IKE debug: `vpn debug ikeoff`
`trunc` *or* `truncon`	This command: 1. Rotates the `$FWDIR/log/vpnd.elg` file 2. Truncates the `$FWDIR/log/ike.elg` file 3. Starts the VPND daemon debug 4. Starts the IKE debug Run this command to start the debug: `vpn debug trunc ALL=5`

`truncoff`	Stops the VPND daemon debug.
	Run one of these commands to stop the VPND debug:
	`vpn debug truncoff`
	`vpn debug off`

Parameter	Description
`timeon [<Seconds>]`	Enables the timestamp in the log files. Prints one timestamp after the specified number of seconds. By default, prints the timestamp every 10 seconds.
`timeoff`	Disables the timestamp in the log files every number of seconds.
`ikefail [-s <Size_in_MB>]`	Logs failed IKE negotiations. You can specify the size of the `$FWDIR/log/ike.elg` file, when to perform the log rotation (close the current active file, rename it, open a new active file).
`mon`	Enables the IKE Monitor. Saves the IKE packets in the `$FWDIR/log/ikemonitor.snoop` file. **Warning** - The output file may contain user X-Auth passwords. Make sure the file is protected.
`moff`	Disables the IKE Monitor.
`say "String"`	Saves the specified text string in the `$FWDIR/log/vpnd.elg` file. For example, run: `vpn debug say "BEGIN TEST"` **Notes:** ■ Run this command after you start the VPN debug (with one of these commands: "`vpn debug on`", "`vpn debug trunc`", or "`vpn debug truncon`"). ■ The length of the string is limited to 255 characters.

`tunnel [<Debug_Level>]`	This command:
	1. Rotates the `$FWDIR/log/vpnd.elg` file
	2. Truncates the `$FWDIR/log/ike.elg` file
	3. Starts the VPND daemon debug with these two Debug Topics:
	`tunnel`
	`ikev2`
	If the `<Debug_Level>` is 2,3,4 or 5, then also enables this Debug Topic:
	`CRLCache`
	4. Starts the IKE debug

Configuring Remote Access VPN

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure Remote Access VPN settings.

set remote-access users radius-auth

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures VPN remote access privileges to users defined on the 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 A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '_' (underscore) ■ '@' (at) ■ ' ' (space)
use-radius-groups	Use RADIUS groups for authentication Type: Boolean (true/false)

Example Command

```
set remote-access users radius-auth true use-radius-groups true
radius-groups My group
```

set vpn remote-access default-access-to-lan

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
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 Command

```
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 MySharedKey
```

set vpn remote-access advanced

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
dns-secondary	Configure manually office mode second DNS
dns-tertiary	Configure manually office mode third DNS
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

Parameter	Description
om-network-ip	Office Mode - Allocate IP addresses from the following network Type: Network address
om-subnet-mask	Subnet for allocating IP addresses of incoming remote access connections (Office Mode)
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 Command

```
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
```

set vpn remote-access advanced enc-dom-obj manual remove

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set vpn remote-access advanced enc-dom-obj manual remove name
MyEncDom
```

set vpn remote-access advanced enc-dom-obj manual add

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set vpn remote-access advanced enc-dom-obj manual add name
MyEncDom
```

set vpn remote-access advanced-settings allow-caching-passwords-on-client

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings allow-caching-passwords-
on-client {true | false}
```

Example Command

```
set vpn remote-access advanced-settings allow-caching-passwords-
on-client true
```

set vpn remote-access advanced-settings allow-clear-traffic-while-disconnected

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings allow-clear-traffic-while-disconnected {true | false}
```

Example Command

```
set vpn remote-access advanced-settings allow-clear-traffic-while-disconnected true
```

set vpn remote-access advanced-settings allow-simultaneous-login

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings allow-simultaneous-login
{true | false}
```

Example Command

```
set vpn remote-access advanced-settings allow-simultaneous-login
true
```

set vpn remote-access advanced-settings allow-update-topo

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings allow-update-topo {true |
false}
```

Example Command

```
set vpn remote-access advanced-settings allow-update-topo true
```

set vpn remote-access advanced-settings auth-timeout-limi

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings auth-timeout-limit <auth-timeout-limit>
```

Parameters

Parameter	Description
auth-timeout-limit	

Example Command

```
set vpn remote-access advanced-settings auth-timeout-limit 15
```

set vpn remote-access advanced-settings disable-office-mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings disable-office-mode {true
| false}
```

Example Command

```
set vpn remote-access advanced-settings disable-office-mode true
```

set vpn remote-access advanced-settings disconnect-enc-domain

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings disconnect-enc-domain
{true | false}
```

Example Command

```
set vpn remote-access advanced-settings disconnect-enc-domain true
```

set vpn remote-access advanced-settings enable-back-conn

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings enable-back-conn {true |
false}
```

Example Command

```
set vpn remote-access advanced-settings enable-back-conn true
```

set vpn remote-access advanced-settings enc-dns-traffic

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings enc-dns-traffic {true |
false}
```

Example Command

```
set vpn remote-access advanced-settings enc-dns-traffic true
```

set vpn remote-access advanced-settings enc-method

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings enc-method <enc-method>
```

Parameters

Parameter	Description
enc-method	

Example Command

```
set vpn remote-access advanced-settings enc-method ike-v1
```

set vpn remote-access advanced-settings endpoint-vpn-user-re-auth-timeout

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
endpoint-vpn-user-re-auth-timeout	

Example Command

```
set vpn remote-access advanced-settings endpoint-vpn-user-re-auth-
timeout 15
```

set vpn remote-access advanced-settings ike-ip-comp-support

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings ike-ip-comp-support {true
| false}
```

Example Command

```
set vpn remote-access advanced-settings ike-ip-comp-support true
```

set vpn remote-access advanced-settings ike-support-crash-recovery

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings ike-support-crash-recovery
{true | false}
```

Example Command

```
set vpn remote-access advanced-settings ike-support-crash-recovery
true
```

set vpn remote-access advanced-settings ike-over-tcp

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings ike-over-tcp {true |
false}
```

Example Command

```
set vpn remote-access advanced-settings ike-over-tcp true
```

set vpn remote-access advanced-settings is-udp-enc-active

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings is-udp-enc-active {true |
false}
```

Example Command

```
set vpn remote-access advanced-settings is-udp-enc-active true
```

set vpn remote-access advanced-settings keep-alive-time

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings keep-alive-time <keep-alive-time>
```

Parameters

Parameter	Description
keep-alive-time	

Example Command

```
set vpn remote-access advanced-settings keep-alive-time 15
```

set vpn remote-access advanced-settings office-mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings office-mode [ om-perform-
antispoofing {true | false} ] [ single-om-per-site {true | false}
]
```

Parameters

Parameter	Description
om-perform-antispoofing	
single-om-per-site	

Example Command

```
set vpn remote-access advanced-settings office-mode om-perform-
antispoofing true single-om-per-site true
```

set vpn remote-access advanced-settings om-enable-with-multiple-if

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings om-enable-with-multiple-if
{true | false}
```

Example Command

```
set vpn remote-access advanced-settings om-enable-with-multiple-if
true
```

set vpn remote-access advanced-settings om-method-radius

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings om-method-radius {true |
false}
```

Example Command

```
set vpn remote-access advanced-settings om-method-radius true
```

set vpn remote-access advanced-settings port

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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> ]
{true | false}
```

Parameters

Parameter	Description
visitor-mode-port	
reserve-port-443	

Example Command

```
set vpn remote-access advanced-settings port visitor-mode-port
8080 reserve-port-443 true
```

set vpn remote-access advanced-settings prevent-ip-pool-nat

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings prevent-ip-pool-nat {true
| false}
```

Example Command

```
set vpn remote-access advanced-settings prevent-ip-pool-nat true
```

set vpn remote-access advanced-settings radius-retransmit-timeout

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings radius-retransmit-timeout
<radius-retransmit-timeout>
```

Parameters

Parameter	Description
radius-retransmit-timeou	

Example Command

```
set vpn remote-access advanced-settings radius-retransmit-timeout
15
```

set vpn remote-access advanced-settings snx-encryption-enable-3des

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings snx-encryption-enable-3des
{true | false}
```

Example Command

```
set vpn remote-access advanced-settings snx-encryption-enable-3des
true
```

set vpn remote-access advanced-settings snx-encryption-enable-rc4

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings snx-encryption-enable-rc4
{true | false}
```

Example Command

```
set vpn remote-access advanced-settings snx-encryption-enable-rc4
true
```

set vpn remote-access advanced-settings snx-keep-alive-timeout

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
snx-keep-alive-timeout	

Example Command

```
set vpn remote-access advanced-settings snx-keep-alive-timeout 15
```

set vpn remote-access advanced-settings snx-min-tls

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings snx-min-tls <snx-min-tls>
```

Parameters

Parameter	Description
snx-min-tls	

Example Command

```
set vpn remote-access advanced-settings snx-min-tls tls-1-0
```

set vpn remote-access advanced-settings snx-upgrade

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings snx-upgrade <snx-upgrade>
```

Parameters

Parameter	Description
snx-upgrade	

Example Command

```
set vpn remote-access advanced-settings snx-upgrade ask-user
```

set vpn remote-access advanced-settings snx-user-re-auth-timeout

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
snx-user-re-auth-timeout	

Example Command

```
set vpn remote-access advanced-settings snx-user-re-auth-timeout
15
```

set vpn remote-access advanced-settings snx-uninstall-on-disconnect

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
snx-uninstall-on-disconnect	

Example Command

```
set vpn remote-access advanced-settings snx-uninstall-on-
disconnect ask-user
```

set vpn remote-access advanced-settings update-topo

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings update-topo <update-topo>
```

Parameters

Parameter	Description
update-topo	

Example Command

```
set vpn remote-access advanced-settings update-topo 15
```

set vpn remote-access advanced-settings update-topo-startup

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings update-topo-startup {true
| false}
```

Example Command

```
set vpn remote-access advanced-settings update-topo-startup true
```

set vpn remote-access advanced-settings use-limited-auth-timeout

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings use-limited-auth-timeout
{true | false}
```

Example Command

```
set vpn remote-access advanced-settings use-limited-auth-timeout
true
```

set vpn remote-access advanced-settings verify-gateway-cert

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures advanced settings for VPN remote access.

Syntax

```
set vpn remote-access advanced-settings verify-gateway-cert {true
| false}
```

Example Command

```
set vpn remote-access advanced-settings verify-gateway-cert true
```

set vpn remote-access advanced-settings visitor-mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
enable-visitor-mode-all	
visitor-mode-interface	

Example Command

```
set vpn remote-access advanced-settings visitor-mode enable-
visitor-mode-all all visitor-mode-interface 192.168.1.1
```

set vpn remote-access two-factor-authentication

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Configure two-factor authentication for VPN Remote Access.

See *"show vpn remote-access two-factor-authentication" on page 1495*.

Syntax

```
set vpn remote-access two-factor-authentication
      [ use-sms {true | false} [ sms-provider {check-point |
external} ] [ sms-dynamicid-url <sms-dynamicid-url> ] [ sms-
provider-username <sms-provider-username> ] [ sms-provider-
password <sms-provider-password> ] [ sms-api-id <sms-api-id> ] [
sms-message "<sms-message>" ]
      [ use-email {true | false} ] [ email-provider {check-point |
external} ] [ email-dynamicid-path <email-dynamicid-path> ] [
email-api-id <email-api-id> ] [ email-message "<email-message>" ]
[ one-time-password-length <one-time-password-length> ] [ one-
time-password-expiration <one-time-password-expiration> ] [ one-
time-password-retries <one-time-password-retries> ] [ default-
country-code <default-country-code> ]
```

Parameters

Parameter	Description
default-country-code	The default country code for phone numbers that do not include a country code. Type: A number with no fractional part (integer).
email-api-id	The API ID required by the email provider. A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
email-dynamicid-path	The DynamicID path when sending email messages using a user defined email provider.

Parameter	Description
email-message	The email message that will be sent to the user.
email-provider-password	The password required by the email provider.
email-provider-username	The username required by the email provider.
email-provider	Indicates which provider will send the email messages.
one-time-password-expiration	The time users have to enter the one time password before it expires (in minutes).
one-time-password-length	Number of characters used in the one time password. Type: A number with no fractional part (integer).
one-time-password-retries	The number of times users can attempt to enter the one time password before the entire authentication process restarts.
sms-api-id	The API ID required by the SMS provider. A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
sms-dynamicid-url	The DynamicID URL when sending SMS message using a user defined SMS provider.
sms-message	The SMS message that will be sent to the user.
sms-provider	Indicates which provider will send the SMS messages.
sms-provider-password	The password required by the SMS provider.
sms-provider-username	The username required by the SMS provider A string that contains up to 64 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '`.`' (period) ■ '`-`' (minus) ■ '`@`' (at)

Parameter	Description
use-email	Indicates whether sending email messages is enabled (`true`) or disabled (`false`).
use-sms	Indicates whether sending SMS messages is enabled (`true`) or disabled (`false`).

Example Command

```
set vpn remote-access two-factor-authentication use-sms true sms-
provider check-point sms-dynamicid-url urlDynamicId sms-provider-
username admin sms-provider-password extendedPassword sms-api-id
123SmsAPI456 sms-message "Hello" use-email true email-provider
check-point email-dynamicid-path emailDynamicId email-api-id
123EmailAPI456 email-message "Hello" one-time-password-length 8
one-time-password-expiration 5 one-time-password-retries 3
default-country-code 8
```

set vpn remote-access two-factor-authentication advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Two-Factor Authentication sends a One Time Password (OTP) to the end-user to authenticate before connecting to a resource.This command controls whether the target selection screen where to send the passcode (SMS / email) is displayed to the end-user in their Remote Access VPN client.

Syntax

```
set vpn remote-access two-factor-authentication advanced-settings
enable-target-selection-for-passcode { true | false }
```

Parameters

Parameter	Description
enable-target-selection-for-passcode	■ `false` - The passcode (One Time Password) is sent to both SMS and email (default). ■ `true` - After an end-user clicks "Connect" in their Remote Access VPN client, in the next window the end-user must enter a mobile phone number to get the OTP by SMS, or enter an email to get the OTP by Email. **Note** - This setting does not affect the selection screen in the WebUI on the **VPN Remote Access Control** page. On that page the user must still configure to receive the passcode through email, SMS, or both options.

Example Command

```
set vpn remote-access two-factor-authentication advanced-settings
enable-target-selection-for-passcode false
```

set vpn remote-access use-two-factor-authentication

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enable/Disable two-factor authentication for VPN remote access.

Syntax

```
set vpn remote-access use-two-factor-authentication { true | false
}
```

Example Command

```
set vpn remote-access use-two-factor-authentication true
```

delete ssl-network-extender

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Forces a manual deletion of the SSL Network Extender.

This forces the gateway to download the latest version of the SSL Network Extender from the cloud.

Syntax

```
delete ssl-network-extender
```

Example Command

```
delete ssl-network-extender
```

show remote-access users radius-auth

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows VPN remote access configuration for RADIUS users.

Syntax

```
show remote-access users radius-auth
```

Example Command

```
show remote-access users radius-auth
```

show vpn remote-access

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration of remote access VPN.

Syntax

```
show vpn remote-access
```

Example Command

```
show vpn remote-access
```

Example Command

```
> show vpn remote-access
mode: false
default-access-to-lan: accept
track: log
use-two-factor-authentication:true
mobile-client: true
sslvpn-client: false
l2tp-vpn-client: false
l2tp-pre-shared-key:
```

show vpn remote-access advanced

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced settings of remote access VPN.

Syntax

```
show vpn remote-access advanced
```

Example Command

```
show vpn remote-access advanced
```

show vpn remote-access advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced settings of remote access VPN.

Syntax

```
show vpn remote-access advanced-settings
```

Example Command

```
show vpn remote-access advanced-settings
```

show vpn remote-access two-factor-authentication

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Show two-factor authentication for VPN Remote Access settings.

See *"set vpn remote-access two-factor-authentication" on page 1486*.

Syntax

```
show vpn remote-access two-factor-authentication
```

Example Command

```
HostName> show vpn remote-access two-factor-authentication
use-sms:                        false
sms-provider:                   check-point
sms-dynamicid-url:              https:asdf.com
sms-provider-username:          asdf
sms-provider-password:
sms-api-id:                     A3C43B03-874F-9580-BA0D-B7E5EF4E3FAF
sms-message:                    Hello World
use-email:                      true
email-provider:                 check-point
email-dynamicid-path:
email-provider-username:
email-provider-password
email-api-id:
email-message:
one-time-password-length:       6
one-time-password-expiration:   5
one-time-password-retires:      3
default-country-code:
```

Working with Harmony Connect

In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

This section provides commands to work with Harmony Connect.

set harmony harmony-connect-mode

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

To turn on or off the Harmony Connect feature.

See *"set harmony-configuration activation-type" on page 1497*.

Syntax

```
set harmony harmony-connect-mode { on | off }
```

Example Command

```
set harmony harmony-connect-mode on
```

set harmony-configuration activation-type

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

To set the configuration (activation type) of the Harmony Connect feature: manual or orchestration.

Syntax

```
set harmony-configuration activation-type
      manual fqdn <FQDN> shared-secret <Secret> site-A <Address of
Site A> [site-B <Address of Site B>]
      orchestration fqdn <FQDN> shared-secret <Secret> api-key
<API Key> client-id <ID> location <Location>
```

Parameters

Parameter	Status	Description
fqdn	Mandatory	FQDN which is used for authentication purposes
shared-secret	Mandatory	Shared secret
site-A	Mandatory	IP address or URL of site A
site-B	Optional	IP address or URL of site B
api-key	Mandatory	API key which is provided by harmony-connect
client-id	Mandatory	Client ID which is provided by harmony-connect
location	Mandatory	Location of the VPN site

Example for Manual

```
set harmony-configuration activation-type manual fqdn www.fqdn.com
shared-secret mysecret site-A www.siteA.com
```

Example for Orchestration

```
set harmony-configuration activation-type type orchestration api-
key sdvsd client-id dgfwe432 fqdn www.fqdn.com location us-central
shared-secret djdsvgsd
```

Working with OpenSSH Encryption Algorithms

In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

This section provides commands to work with OpenSSH Encryption Algorithms.

add ssh-<encryption-category> algorithm <algorithm>

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Starting in R81.10.x, OpenSSH is used for the SSH server (sshd) instead of Dropbear. OpenSSH enables you to configure which encryption algorithms to use for each stage of the connection, using a config file. Add algorithms from a predefined list.

These are the encryption categories, each with multiple supported algorithms:

- Kex
- Ciphers
- MACs

Syntax

```
add ssh-<encryption-category> algorithm <algorithm>
```

Parameters

Parameter	Description
kex	■ curve25519-sha256 ■ curve25519-sha256@libssh.org ■ ecdh-sha2-nistp521 ■ ecdh-sha2-nistp384 ■ ecdh-sha2-nistp256 ■ diffie-hellman-group14-sha256 ■ diffie-hellman-group14-sha1 ■ diffie-hellman-group16-sha512 ■ diffie-hellman-group18-sha512 ■ diffie-hellman-group-exchange-sha256
cipher	■ aes128-ctr ■ aes256-ctr ■ aes128-cbc ■ aes256-cbc ■ aes192-ctr
hmac	■ hmac-sha1 ■ hmac-sha2-256 ■ hmac-sha2-512

Example Command

```
add ssh-kex algorithm diffie-hellman-group 18-sha512
```

```
add ssh-mac algorithm hmac-sha2-512
```

delete ssh-<encryption-category> algorithm <algorithm>

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Starting in R81.10.x, OpenSSH is used for the SSH server (sshd) instead of Dropbear. OpenSSH enables you to configure which encryption algorithms to use for each stage of the connection, using a config file. Delete algorithms from a predefined list.

These are the encryption categories, each with multiple supported algorithms:

- Kex
- Ciphers
- MACs

Syntax

```
delete ssh-<encryption-category> algorithm <algorithm>
```

Parameters

Parameter	Description
kex	■ curve25519-sha256 ■ curve25519-sha256@libssh.org ■ ecdh-sha2-nistp521 ■ ecdh-sha2-nistp384 ■ ecdh-sha2-nistp256 ■ diffie-hellman-group14-sha256 ■ diffie-hellman-group14-sha1 ■ diffie-hellman-group16-sha512 ■ diffie-hellman-group18-sha512 ■ diffie-hellman-group-exchange-sha256
cipher	■ aes128-ctr ■ aes256-ctr ■ aes128-cbc ■ aes256-cbc ■ aes192-ctr
hmac	■ hmac-sha1 ■ hmac-sha2-256 ■ hmac-sha2-512

Example Command

```
delete ssh-cipher algorithm aes128-cbc
```

show ssh-kex

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Starting in R81.10.x, OpenSSH is used for the SSH server (sshd) instead of Dropbear. OpenSSH enables you to configure which encryption algorithms to use for each stage of the connection, using a config file. Add/delete algorithms from a predefined list.

These are the encryption categories, each with multiple supported algorithms:

- Kex - Key Exchange Algorithms, the key exchange methods that are used to generate per-connection keys.
- Ciphers - The ciphers used to encrypt the connection.
- MACs - Specified the available MAC (message authentication code) algorithms.

Syntax

```
show ssh-kex
```

Parameters

Parameter	Description
kex	■ curve25519-sha256 ■ curve25519-sha256@libssh.org ■ ecdh-sha2-nistp521 ■ ecdh-sha2-nistp384 ■ ecdh-sha2-nistp256 ■ diffie-hellman-group14-sha256 ■ diffie-hellman-group14-sha1 ■ diffie-hellman-group16-sha512 ■ diffie-hellman-group18-sha512 ■ diffie-hellman-group-exchange-sha256

Example Output

```
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp521
ecdh-sha2-nistp384
ecdh-sha2-nistp256
diffie-hellman-group14-sha256
diffie-hellman-group14-sha1
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group-exchange-sha256
```

show ssh-cipher

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Starting in R81.10.x, OpenSSH is used for the SSH server (sshd) instead of Dropbear. OpenSSH enables you to configure which encryption algorithms to use for each stage of the connection, using a config file. Add/delete algorithms from a predefined list.

These are the encryption categories, each with multiple supported algorithms:

- Kex - Key Exchange Algorithms, the key exchange methods that are used to generate per-connection keys.
- Ciphers - The ciphers used to encrypt the connection.
- MACs - Specifies the available MAC (message authentication code) algorithms.

Syntax

```
show ssh-cipher
```

Parameters

Parameter	Description
mac	■ hmac-sha1 ■ hmac-sha2-256 ■ hmac-sha2-512

Example Output

```
aes128-ctr
aes192-ctr
aes256-ctr
```

show ssh-mac

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Starting in R81.10.x, OpenSSH is used for the SSH server (sshd) instead of Dropbear. OpenSSH enables you to configure which encryption algorithms to use for each stage of the connection, using a config file. Add/delete algorithms from a predefined list.

These are the encryption categories, each with multiple supported algorithms:

- Kex - Key Exchange Algorithms, the key exchange methods that are used to generate per connection keys.
- Ciphers - The ciphers used to encrypt the connection
- MACs - Specifies the available MAC (message authentication code) algorithms.

Syntax

```
show ssh-mac
```

Parameters

Parameter	Description
mac	■ hmac-sha1 ■ hmac-sha2-256 ■ hmac-sha2-512

Example Output

```
hmac-sha1
hmac-sha2-256
hmac-sha2-512
```

Configuring SSL VPN Bookmarks on the SSL Network Extender Portal

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure bookmark links that appear in the SSL Network Extender Portal.

add bookmark label

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a new bookmark link that will appear for VPN Remote Access users on 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 A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
password	The password for remote desktop connection A string that contains alphanumeric and special characters.
screen-height	The height of the screen when the bookmark is remote desktop A number with no fractional part (integer)

Parameter	Description
screen-width	The width of the screen when the bookmark is remote desktop A number with no fractional part (integer)
tooltip	Tooltip for the bookmark in the SSL Network Extender portal A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '`(`' (opening round bracket) ■ '`)`' (closing round bracket) ■ ':' (colon) ■ '`@`' (at)
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 A string that contains up to 64 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '`@`' (at)

Example Command

```
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 label

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes an existing bookmark link by label.

This bookmark link appears on the SNX VPN Remote Access landing page.

Syntax

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

Parameters

Parameter	Description
label	Text for the bookmark in the SSL Network Extender portal A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)

Example Command

```
delete bookmark label myLabel
```

delete bookmark all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes all existing bookmark links that appear on the SNX VPN Remote Access landing page.

Syntax

```
delete bookmark all
```

Example Command

```
delete bookmark all
```

set bookmark

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)

Parameter	Description
new-label	Text for the bookmark in the SSL Network Extender portal A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
password	The password for remote desktop connection A string that contains alphanumeric and special characters.
screen-height	The height of the screen when the bookmark is remote desktop A number with no fractional part (integer)
screen-width	The width of the screen when the bookmark is remote desktop A number with no fractional part (integer)
tooltip	Tooltip for the bookmark in the SSL Network Extender portal A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)
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 A string that contains up to 64 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '@' (at)

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that contains less than 257 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '(' (opening round bracket) ■ ')' (closing round bracket) ■ ':' (colon) ■ '@' (at)

Example Command

```
show bookmark label myLabel
```

show bookmarks

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
show bookmarks
```

show used-ad-group bookmarks

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show bookmarks configured to a user group defined in AD in the SNX landing page.

This is relevant only if the user group is defined with VPN remote access privileges.

Syntax

```
show used-ad-group bookmarks name <name>
```

Parameters

Parameter	Description
name	Active Directory group name

Example Command

```
show used-ad-group bookmarks name my AD group
```

set local-group remove bookmark label

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
name	Local group name
bookmark label	Text for the bookmark in the SSL Network Extender portal

Example Command

```
set local-group name myObject_17 remove bookmark label myLabel
```

set local-group add bookmark

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
name	Local group name
bookmark label	Text for the bookmark in the SSL Network Extender portal

Example Command

```
set local-group name myObject_17 add bookmark label myLabel
```

set local-user remove bookmark label

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Removes a bookmark from the SSL Network Extender landing page for an existing locally-defined user.

This is relevant only if the user has remote access VPN privileges. See *"set local-user" on page 115*.

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 Press the TAB key to see the available options.

Example Command

```
set local-user name admin remove bookmark label myLabel
```

set local-user add bookmark label

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Adds a bookmark to the SSL Network Extender landing page for an existing locally-defined user.

This is relevant only if the user has remote access VPN privileges. See *"set local-user" on page 115*.

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 Press the TAB key to see the available options.

Example Command

```
set local-user name admin add bookmark label myLabel
```

set used-ad-group add bookmark label

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
name	Active Directory group name
bookmark label	Text for the bookmark in the SSL Network Extender portal

Example Command

```
set used-ad-group name my AD group add bookmark label myLabel
```

set used-ad-group remove bookmark label

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
name	Active Directory group name
bookmark label	Text for the bookmark in the SSL Network Extender portal

Example Command

```
set used-ad-group name my AD group remove bookmark label myLabel
```

Working with Cluster

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to work with Cluster.

cphaprob

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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.

Parameter	Description
`report`	Reports the status of the <*device*> to the gateway.
`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 Command

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

Example 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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Disables High Availability on the appliance.

Running this command on an appliance that is a cluster member stops the appliance from passing traffic. State synchronization also stops.

Important - This change does **not** survive reboot.

See *"cphastart" below*.

Syntax

```
cphastop
```

Parameters

Parameter	Description
n/a	

Return Value

- 0 - success.
- 1 - failure.

Example Command

```
cphastop
```

Example Output

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

cphastart

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables High Availability on the appliance if:

1. This appliance is configured to be a member of a cluster.
2. High Availability on this appliances was disabled with the "`cphastop`" command (see *"cphastop" on the previous page*).

Syntax

```
cphastart
```

Parameters

Parameter	Description
`n/a`	

Return Value

- 0 - success.
- 1 - failure.

Example Command

```
cphastart
```

Example Output

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

Working with SecureXL SIM

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

SecureXL special commands.

Syntax

```
sim <parameter>
```

Parameters

Parameter	Description
`ver`	Print the SecureXL SIM 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 the interface 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 the template quota feature
`hlqos <options>`	Configure the Heavy-Load CPU QOS feature

Configuring External Log Servers on a Locally Managed Device

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure external Log Servers on a Locally Managed appliance.

set log-servers-configuration

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures external Log Servers for a Locally Managed appliance.

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 {true | false} ]
```

Parameters

Parameter	Description
external-log-server- enable	Determine if an external Log Server is active.
log-server-ip-addr	This IP address is used if the Log Server is not located on the Security Management Server
mgmt-server-ip-addr	This IP address is used for establishing trusted communication between the Check Point Appliance and the Log Server
one-time-password	SIC one time password A string that contains alphanumeric and special characters.
sic-name	Enter the SIC name of the Log Server object that was configured in SmartConsole

Example Command

```
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

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configured external Log Servers on a Locally Managed appliance.

Syntax

```
show log-servers-configuration
```

Example Command

```
show log-servers-configuration
```

Configuring a Remote Security Management Server and Log Server

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure settings to connect to a remote Security Management Server and Log Server.

This applies to Centrally Managed appliances.

connect security-management

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the first connection to the remote Security Management Server.

Syntax

```
connect security-management mgmt-addr <mgmt-addr> use-one-time-
password {true | false} local-override-mgmt-addr { false | true
send-logs-to local-override-log-server-addr addr <ip-addr> }
```

Parameters

Parameter	Description
mgmt-addr	The IP address or hostname of the Security Management Server Type: An IP address or host name
use-one-time-password	Indicates whether to connect to the Security Management Server using a one time password
local-override-mgmt-addr	Indicates if the management address used in the next manual fetch command This IP address is saved and continuously used instead of the IP address downloaded in the policy
ip-addr	IP address of the Log Server, to which the appliance sends the logs
send-logs-to	Indicates from where the address of the log server is taken Press TAB to see available options

Example Command

```
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 mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 { locally-managed | centrally-managed
}
```

Parameters

Parameter	Description
mode	Indicates whether the appliance is managed locally or centrally using a Check Point Security Management Server.

Example Command

```
set security-management mode locally-managed
```

set security-management local-override-mgmt-addr

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures a local override to the IP addresses of the Security Management Server and Log Server.

This is applies to the appliance when it is Centrally Managed (see *"set security-management mode" on page 1536*).

Syntax

```
set security-management local-override-mgmt-addr { false | true
mgmt-address <mgmt-address> send-logs-to local-override-log-
server-addr addr <ip-addr> }
```

Parameters

Parameter	Description
mgmt-address	IP address or hostname of the Security Management Server
send-logs-to	Indicates from where the address of the Log Server is taken Press TAB to see available options
ip-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

Example Command

```
set security-management local-override-mgmt-addr true mgmt-address
myHost.com send-logs-to local-override-log-server-addr addr
myHost.com
```

show security-management

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows settings of the configured remote Security Management Server.

Syntax

```
show security-management
```

Example Command

```
show security-management
```

Configuring the Port-based VLAN (Switch)

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the port-based VLAN (switch) in the appliance.

add switch

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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	A switch name should be LAN[1-8]_Switch

Example Command

```
add switch name LAN2_Switch
```

delete switch

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Deletes a defined port-based VLAN switch object by name.

Syntax

```
delete switch <name>
```

Parameters

Parameter	Description
name	A switch name should be LAN[1-8]_Switch

Example Command

```
delete switch LAN2_Switch
```

set switch add port

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Add a physical port to an existing port-based VLAN (switch).

Syntax

```
set switch <name> add port <port>
```

Parameters

Parameter	Description
name	A switch name should be LAN[1-8]_Switch
port	A name of a LAN interface

Example Command

```
set switch LAN2_Switch add port LAN4
```

set switch remove port

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Removes a physical port from an existing port-based VLAN (switch).

Syntax

```
set switch <name> remove port <port>
```

Parameters

Parameter	Description
name	A switch name should be LAN[1-8]_Switch
port	A name of a LAN interface

Example Command

```
set switch LAN2_Switch remove port LAN4
```

show switch

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows port-based VLAN (switch) configuration.

Syntax

```
show switch <name>
```

Parameters

Parameter	Description
name	A switch name should be LAN[1-8]_Switch

Example Command

```
show switch LAN2_Switch
```

show switch ports

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows ports within a configured port-based VLAN (switch) configuration.

Syntax

```
show switch <name> ports
```

Parameters

Parameter	Description
name	A switch name should be LAN[1-8]_Switch

Example Command

```
show switch LAN2_Switch ports
```

show switches

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows all port-based VLANs (switches).

Syntax

```
show switches
```

Parameters

Parameter	Description
n/a	

Example Command

```
show switches
```

Configuring Advanced Appliance Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure advanced appliance settings.

set os-settings advanced-settings enable-automatic-wifi-channel-change

In the R81.10.X releases, this command is available starting from the R81.10.08 version.

Description

This feature detects and avoid wireless interference by switching to a less "noisy" channel in case of too many interferences. You can enable automatic WiFi channel change.

Syntax

```
set os-settings advanced-settings enable-automatic-wifi-channel-
change { true | false }
```

Parameters

Parameter	Description
enable-automatic-wifi-channel-change	Options: ■ `true` - Enabled ■ `false` - Disabled

Example Command

```
set os-settings advanced-settings enable-automatic-wifi-channel-
change true
```

set os-settings advanced-settings backoff-mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

You can configure how an LTE model behaves when an attempt to register or activate a data session with a cellular service provider fails:

- Continue the attempts (no back-off between the attempts)
- Wait for some time before starting another attempt (there is back-off between the attempts)

Back-off algorithm for handling a registration failure

If a GSM registration fails (for example, a "GPRS Attach" connection fails, or the cellular network is not available), the appliance reboots the cellular modem at these intervals (in minutes): 1, 5, 10, 15, 20, 30, 60, 120, and then every 60 minutes.

Back-off algorithm for handling a data activation failure

If a data session activation fails (for example, a "PDP Context Activation" connection fails), the appliance tries again at these intervals (in minutes): 1, 2, 3, 4, 5, 15, 30, 60, 120, and then every 60 minutes.

Syntax

```
set os-settings advanced-settings backoff-mode <mode>
```

Parameters

Parameter	Description
mode	Specifies the back-off mode: ■ `auto` - Configures the automatic back-off algorithm. By default, there is no back-off. ■ `force-disable` - Disables the back-off algorithm. ■ `force-enable` - Enables the back-off algorithm.

Example Command

```
set os-settings advanced-settings backoff-mode force-enable
```

set os-settings advanced-settings disable-dhcp-options-transfer

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Disable automatic transfer of received Internet DHCP client options to internal DHCP servers on the LAN network .

Syntax

```
set os-settings advanced-settings disable-dhcp-options-transfer
{true | false}
```

Example Command

```
set os-settings advanced-settings disable-dhcp-options-transfer
true
```

set os-settings advanced-settings enable-net-switch-flow-control

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enable net switch flow control.

Syntax

```
set os-settings advanced-settings enable-net-switch-flow-control
{true | false}
```

Example Command

```
set os-settings advanced-settings enable-net-switch-flow-control
true
```

set os-settings advanced-settings enable-jumbo-frames

In the R81.10.X releases, this command is available starting from the R81.10.07 version.

Description

When you enable Jumbo Frames (set to true), you can configure an MTU up to 9000 on both LAN and Internet.

Syntax

```
set os-settings enable-jumbo-frames { true | false }
```

Parameters

Parameter	Description
enable-jumbo-frames	▪ `true` - Enables Jumbo Frames. ▪ `false` - Disables Jumbo Frames.

Example Command

```
set os-settings enable-jumbo-frames true
```

set os-settings advanced-settings force-cellular-4g

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

In Advanced Settings, force cellular module to use 4G network.

Syntax

```
set-os-settings advanced-settings force-cellular-4g {true | false}
```

Example Command

```
set os-settings advanced-settings force-cellular-4g true
```

set os-settings advanced-settings gps-enable

In the R81.10.X releases, this command is available starting from the R81.10.07 version.

Description

Enable to get GPS data from an internal cellular modem.

Syntax

```
set os-settings advanced-settings gps-enable { true | false }
```

Parameters

Parameter	Description
gps-enable	■ `true` - Enable this feature. ■ `false` - Disable this feature

Example Command

```
set os-settings advanced-settings gps-enable true
```

set os-settings advanced-settings ipv6-prefix-selection-mode

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Add support for continuous listening for Router-Advertisements and dynamic update of IPv6-prefix, and provide several methods to select the IPv6-prefix.

Syntax

```
set os-settings advanced-settings ipv6-prefix-selection-mode
<mode>
```

Parameters

Parameter	Description
mode	Router preference: Select the IPv6 prefix with the highest preference. ■ `router-pref-oldest` (default) - If there is more than one prefix with the same preference, select the oldest one unless its remaining lifetime is less than one hour. ■ `router-pref-newest` - If there is more than one prefix with the same preference, select the newest one. Preferred lifetime: Select the IPv6 prefix with the highest preferred lifetime value. ■ `pref-lifetime-oldest` - If there is more than one prefix with the same preferred lifetime, select the oldest one. ■ `pref-lifetime-newest` - If there is more than one prefix with the same preferred lifetime, select the newest one.

Example Command

```
set os-settings advanced-settings ipv6-prefix-selection-mode pref-
lifetime-oldest
```

show os-settings advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the advanced appliance settings.

Syntax

```
show os-settings advanced-settings
```

Example Command

```
show os-settings advanced-settings
```

Sample Output

```
Hostname> show os-settings advanced-setting
gps-enable                        true
enable-pppoe-dst-check:           false
enable-net-switch-flow-control:   false
use-secondary-mccmnc-file:        false
disable-dhcp-options-transfer:    false
use-conn-mon-unique-icmp-id:      false
cellular-reset-modem-after-detect-failed:true
ipv6-prefix-selection-mode:       router-pref-oldest
enable-wifi-monitors:             false
force-cellular-4g:                false
cellular-network:                 auto
enable-lan-on-wan:                false
backoff-mode:                     auto
cellular-connection-establish-timeout:60
cellular-modem-detect-timeout:    120
drop-cellular-mismatched-sourse-ip-packets:false
enable-jumbo-frames:              false
enable-automatic-wifi-channel-change:false
```

show gps-data

In the R81.10.X releases, this command is available starting from the R81.10.07 version.

Description

Show the available GPS data when enabled.

See also:

- *"set os-settings advanced-settings gps-enable" on page 1551*
- *"show os-settings advanced-settings" above*

Syntax

```
show gps-data
```

Sample Output

```
Hostname> show gps-data
tracking angle:.............309.62°
longitude:                  121° 58.3416' W
latitude:                   37° 23.2475' N
geoid_altitude:             2.1
speed:                      0.13
is_valid:                   true
fix_mode:                   3D
horizontal_dilution:        1.0
altitude:                   9.0
magnetic_variation:         3.1 W
satellites_in_view:         16
fix_quality:                GPS
google_earth:               37 23.2475N,121 58.3416W
tracked_satellites:         7
fix_timestamp_utc:          N/A
```

Configuring Monitor Mode

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the Monitor mode.

add monitor-mode-network

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
subnet-mask	Network subnet mask A subnet mask, or 255.255.255.255

Example Command

```
add monitor-mode-network ipv4-address 192.168.1.1 subnet-mask
255.255.255.0
```

set monitor-mode-network

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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
subnet-mask	Network subnet mask A subnet mask, or 255.255.255.255

Example Command

```
set monitor-mode-network ipv4-address 192.168.1.1 ipv4-address
192.168.1.1 subnet-mask 255.255.255.0
```

set monitor-mode-configuration

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set monitor-mode-configuration use-defined-networks true
```

delete monitor-mode-network

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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

Example Command

```
delete monitor-mode-network ipv4-address 192.168.1.1
```

show monitor-mode-networks

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows manually defined local networks for monitor mode configuration.

Syntax

```
show monitor-mode-networks
```

Parameters

Parameter	Description
n/a	

Example Command

```
show monitor-mode-networks
```

show monitor-mode-configuration

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows monitor mode configuration for interfaces.

Syntax

```
show monitor-mode-configuration
```

Parameters

Parameter	Description
n/a	

Example Command

```
show monitor-mode-configuration
```

Configuring Path MTU Discovery

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the Path MTU Discovery mode for a cellular connection.

set-pmtud

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the Path MTU Discovery Mode for a cellular connection.

See also:

- *"show-pmtud" below*

Syntax

```
set pmtud pmtud-mode {daemon | disabled | oneshot}
```

Parameters

Parameter	Description
pmtud-mode	Configures the Path MTU Discovery Mode: ■ `daemon` - Run as a daemon ■ `disabled` - Disabled (default) ■ `oneshot` - Run one time only

Example Command

```
set pmtud pmtud-mode oneshot
```

show-pmtud

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configured Path MTU Discovery Mode for a cellular connection.

See also:

- *"set-pmtud" on the previous page*

Syntax

```
show pmtud
```

Example Command

```
show pmtud
pmtud-mode:                     disabled
```

Working with SD-WAN

In the R81.10.X releases, this feature is available starting from the R81.10.10 version.

This section provides commands to work with SD-WAN in Locally Managed appliances.

With SD-WAN you can configure your Security Gateway to steer traffic dynamically between the configured WAN Links based on the measured ISP link quality. This does not require dynamic routing configuration on your Security Gateway.

The Security Gateway sends different types of traffic through different Internet Service Providers (ISPs) based on application / identity and dynamic measurement of WAN Link characteristics.

The Security Gateway applies the configured SD-WAN rules only if the Security Policy allows this traffic.

After you install the SD-WAN Policy, it becomes the main decision maker for traffic paths, traffic priorities, and so on for WAN connections.

set internet-connection sdwan

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Configures SD-WAN settings on the internet connection.

See:

- *"show internet-connection sdwan-settings" on page 1587*
- *"set internet-connection probe-icmp-servers" on page 359*
- *"set internet-connection probe-icmp6-servers" on page 629*
- *"set internet-connection probe-next-hop" on page 356*

Syntax

```
set internet-connection <Name>
      sdwan
            disabled
            enabled
                  download-speed <1-1000000>
                  override-circuit-id {on | off}
                  upload-speed <1-1000000>
      sdwan-backup {on | off}
      sdwan-ip-address-accessibility
            directly
            via-nat sdwan-nat-ip-address <NAT IPv4 address>
      sdwan-tag <Tag>
```

Parameters

Parameter	Description
internet-connection	Name of the Internet connection. Press the TAB key to see the available options.
sdwan disabled	Disables the SD-WAN in this Internet connection.
sdwan enabled	Enables the SD-WAN in this Internet connection.
download-speed	Configures the SD-WAN interface download speed (Mbps).
override-circuit-id	Enables (`on`) or disables (`off`) the override of the SD-WAN interface Circuit ID. The SD-WAN Policy assigns a Circuit ID automatically (to label the connections). It is possible to override the assigned value. **Note** - This parameter applies only when the appliance works in the Centrally Managed mode. See the *Quantum SD-WAN Administration Guide*.
upload-speed	Configures the SD-WAN interface upload speed (Mbps).
sdwan-backup	Configures this Internet connection as a backup in SD-WAN.
sdwan-ip-address-accessibility	Configures NAT for this Internet connection in SD-WAN: **Note** - This parameter applies only when the appliance works in the Centrally Managed mode. See the *Quantum SD-WAN Administration Guide*. ■ `directly` Specifies that there is no NAT on the IP address of this interface. SD-WAN peers can connect to this IP address directly. ■ `via-nat sdwan-nat-ip-address <NAT IPv4 address>` Specifies that an external device or an ISP applies NAT on the IP address of this interface. Enter the applicable IP address after this external NAT, as the SD-WAN peers receive it.

Parameter	Description
sdwan-tag	Configures a desired interface tag. **Note** - This parameter applies only when the appliance works in the Centrally Managed mode. See the *Quantum SD-WAN Administration Guide*. **Note** - To delete an empty tag, run: `set internet-connection <Name> sdwan enabled sdwan-tag \`

Example Command

```
set internet-connection Internet1 sdwan enabled upload-speed 100
sdwan-tag asd
```

set internet-connection-settings

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Configures the SD-WAN probing settings.

See *"show internet-connection-settings" on page 1588*.

Syntax

```
set internet-connection-settings
      jitter <0-10000>
      latency <0-10000>
      packet-loss <0-100>
      probing-host <IPv4 Address or Hostname>
      second-probing-host <IPv4 Address or Hostname>
      third-probing-host <IPv4 Address or Hostname>
      probing-interval <500-4294967295>
      probing-method {ping | http}
      probing-mode {best | average | worst}
```

Parameters

Parameter	Description
jitter	Configures the jitter threshold (in msec). Default: 80
latency	Configures the latency threshold (in msec). Default: 200
packet-loss	Configures the packet loss threshold (in %). Default: 30
probing-host	Configures the IPv4 Address or Hostname for the first probing destination. Default: `dns.google.com`
second-probing-host	Configures the IPv4 Address or Hostname for the second probing destination. Default: `dns.cloudflare.com`
third-probing-host	Configures the IPv4 Address or Hostname for the third probing destination. Default: `dns.opendns.com`
probing-interval	Configures the interval duration between probes (in msec). Default: 1000
probing-method	Configures the probing method: ■ `ping` - ICMP ping (default) ■ `http` - HTTP

Parameter	Description
probing-mode	Controls which Internet connection the appliance selects in each steering object based on the probing results: ■ `best` - Selects the Internet connection that has the best probing results (the lowest values for the probing characteristics of packet loss, latency, and jitter). This is the default. ■ `average` - Selects the Internet connection that has the average probing results. ■ `worst` - Selects the Internet connection that has the worst probing results (the highest values for the probing characteristics of packet loss, latency, and jitter).

Parameter	Description

Example:
These two Internet connections are configured for SD-WAN - "WAN" and "DMZ".
There are three probing hosts (destinations) - "Host 1", "Host 2", and "Host 3".
The probing results over the configuration probing interval are:

	WAN			DMZ		
Probing Characteristic	Host 1	Host 2	Host 3	Host 1	Host 2	Host 3
Packet Loss (%)	1	1	4	2	3	7
Latency (msec)	1	1	4	2	3	7
Jitter (msec)	1	1	4	2	3	7

Where:

- The best probing result was:
  - For "WAN": Packet Loss = 1, Latency = 1, Jitter = 1
  - For "DMZ": Packet Loss = 2, Latency = 2, Jitter = 2
- The average probing result was:
  - For "WAN": Packet Loss = (1+1+4)/3 = 2, Latency = (1+1+4)/3 = 2, Jitter = (1+1+4)/3 = 2
  - For "DMZ": Packet Loss = (2+3+7)/3 = 4, Latency = (2+3+7)/3 = 4, Jitter = (2+3+7)/3 = 4
- The worst probing result was:
  - For "WAN": Packet Loss = 4, Latency = 4, Jitter = 4
  - For "DMZ": Packet Loss = 7, Latency = 7, Jitter = 7

Therefore:

- If you configure "`best`", the appliance selects the Internet connection "WAN".
- If you configure "`average`", the appliance selects the corresponding Internet connection.
- If you configure "`worst`", the appliance selects the Internet connection "DMZ".

Parameter	Description
Example Command	`set internet-connection-settings latency 200 jitter 80 packet-loss 30 probing-host dns.google.com probing-interval 1000`

add steering-object

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Adds a steering behavior object.

See also:

- *"set steering-object" on page 1579*
- *"show steering-object" on page 1594*
- *"show steering-objects" on page 1595*
- *"delete steering-object" on page 1598*
- *"delete steering-objects" on page 1599*

	WAN			DMZ		
Probing Characteristic	Host 1	Host 2	Host 3	Host 1	Host 2	Host 3
P	11	14	23	27		

Syntax

```
add steering-object
      name "<Name>"
      comment "<Text>"
      candidates-selected
            all
            specific
                  add candidate <Name of Internet Connection>
                        additional-candidate <Name of Internet
Connection>
                        <the same parameters as for 'steering-
object'>
      jitter <0-10000>
      latency <0-10000>
      link-utilization {link-aggregation | prioritize}
      packet-loss <0-100>
      probing-host <IPv4 Address or Hostname>
      second-probing-host <IPv4 Address or Hostname>
      third-probing-host <IPv4 Address or Hostname>
      probing-interval <500-4294967295>
      probing-mode {best | average | worst}
      selection-method <Method>
```

Parameters

Parameter	Description
name	Specifies the name of the SD-WAN steering object. A string that begins with a letter and contain up to 32 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '~' (tilde) ■ ' ' (space)

Parameter	Description
comment	**Optional:** Specifies the comment text for the SD-WAN rule. A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '`(`' (opening round bracket) ■ '`)`' (closing round bracket) ■ ':' (colon) ■ '@' (at)
candidates-selected	Specifies the ISP links: ■ `all` - All relevant links (default) ■ `specific` - Specific links
add candidate	Specifies the name of the Internet connection. Press the TAB key to see the available options.
additional-candidate	Specifies the name of the Internet connection. Press the TAB key to see the available options.
jitter	Configures the jitter threshold (in msec). Default: 30
latency	Configures the latency threshold (in msec). Default: 120
link-utilization	Specifies the ISP link utilization mechanism: ■ `link-aggregation` - Link Aggregation (default). ■ `prioritize` - Prioritize.
packet-loss	Configures the packet loss threshold (in %). Default: 1
probing-host	Configures the IPv4 Address or Hostname for the first probing destination. Default: `dns.google.com`
second-probing-host	Configures the IPv4 Address or Hostname for the second probing destination. Default: `dns.cloudflare.com`

Parameter	Description
third-probing-host	Configures the IPv4 Address or Hostname for the third probing destination. Default: `dns.opendns.com`
probing-interval	Configures the interval duration between probes (in msec). Default: 1000
probing-mode	Controls which Internet connection the appliance selects in each steering object based on the probing results: ■ `best` - Selects the Internet connection that has the best probing results (the lowest values for the probing characteristics of packet loss, latency, and jitter). This is the default. ■ `average` - Selects the Internet connection that has the average probing results. ■ `worst` - Selects the Internet connection that has the worst probing results (the highest values for the probing characteristics of packet loss, latency, and jitter). For more details, see the explanation for this parameter in *"set internet-connection-settings" on page 1567*.
selection-method	Configures the ISP link selection method: ■ `connection-hash` - Connection hash (default) ■ `proportionally-to-download-bandwidth` - Proportionally to download bandwidth ■ `proportionally-to-upload-bandwidth` - Proportionally to upload bandwidth ■ `round-robin` - Round robin

Example Command

```
add steering-object name "Test Steering" comment "My Test
Steering" candidates-selected specific add candidate Internet2
link-utilization prioritize
```

add sdwan-rule

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Adds new SD-WAN manual rules.

Important - Before you add a new SD-WAN rule, make sure to configure the required objects (source, destination, service).

See also:

- *"set sdwan-rule" on page 1583*
- *"show sdwan-rules" on page 1590*
- *"delete sdwan-rule" on page 1597*

SD-WAN Rule Structure

No.	Source	Destination	Applications / Services	Behavior
Rule position	Source objects	Destination objects	Application and Service objects	Steering Behavior object

Syntax

```
add sdwan-rule name <Text without Spaces>
      comment "<Text>"
      disabled {true | false}
      source <Object Name>
      destination <Object Name>
      service <Object Name>
      application-id <Object ID>
      application-name <Object Name>
      behavior <Steering Object>
      position <Number>
      position-above <Number>
      position-below <Number>
```

Parameters

Parameter	Description
name	Specifies the name of the SD-WAN rule. A string of alphanumeric characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits)
comment	**Optional:** Specifies the comment text for the SD-WAN rule. A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '`(`' (opening round bracket) ■ '`)`' (closing round bracket) ■ '`:`' (colon) ■ '`@`' (at)
disabled	Disables (`true`) or enables (`false`) this SD-WAN rule. **Best Practice** - Set the value "`true`" when you add a new rule. Make sure the rule is configured correctly, and only then change set the value "`false`". See *"set sdwan-rule" on page 1583*.
source	Specifies the source object. Press the TAB key to see the available options.
destination	Specifies the destination object. Press the TAB key to see the available options.
service	Specifies the service object. Press the TAB key to see the available options.
application-id	Specifies the application by its ID. Press the TAB key to see the available options.
application-name	Specifies the application by its name. Press the TAB key to see the available options.

Parameter	Description
behavior	Specifies the steering behavior object. Press the TAB key to see the available options.
position	Specifies the rule position.
position-above	Specifies the rule position above the specified rule position.
position-below	Specifies the rule position below the specified rule position.

Example Command

```
add sdwan-rule name MyRule comment "My Test Rule" disabled true
source IP-Phones destination SIP-Provider application-name H.323\
Protocol behavior Business\ Applications
```

set smart-sdwan

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Configures Smart SD-WAN settings - specific default SD-WAN settings.

See:

- *"show smart-sdwan" on page 1592*
- *"show sdwan" on page 1589*

Syntax

```
set smart-sdwan
      link <Name>
            move {up | down}
            position <Number>]
      link-utilization
            link-aggregation
            prioritize
      mode {on | off}
      probing-host <IPv4 Address or Hostname>
      second-probing-host <IPv4 Address or Hostname>
      third-probing-host <IPv4 Address or Hostname>
      probing-mode {best | average | worst}
```

Parameters

Parameter	Description
link-utilization	Specifies the ISP link utilization mechanism: ■ `link-aggregation` - Link Aggregation - use all links equally (default). ■ `prioritize` - Prioritize the Internet connections in a specific order.
link	Specifies the name of the Internet connection. Press the TAB key to see the available options. ■ `move` - Moves the Internet connection above or below its current priority. ■ `position` - Configures the position (priority) of the Internet connection.
mode	Enables (`on`) or disables (`off`) the predefined SD-WAN rules that use the predefined steering behavior objects.
probing-host	Configures the IPv4 Address or Hostname for the first probing destination. Default: `dns.google.com`
second-probing-host	Configures the IPv4 Address or Hostname for the second probing destination. Default: `dns.cloudflare.com`
third-probing-host	Configures the IPv4 Address or Hostname for the third probing destination. Default: `dns.opendns.com`
probing-mode	Controls which Internet connection the appliance selects in each steering object based on the probing results: ■ `best` - Selects the Internet connection that has the best probing results (the lowest values for the probing characteristics of packet loss, latency, and jitter). This is the default. ■ `average` - Selects the Internet connection that has the average probing results. ■ `worst` - Selects the Internet connection that has the worst probing results (the highest values for the probing characteristics of packet loss, latency, and jitter). For more details, see the explanation for this parameter in *"set internet-connection-settings" on page 1567*.

set steering-object

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Configure a specified user-defined steering behavior object.

See also:

- *"add steering-object" on page 1571*
- *"show steering-object" on page 1594*
- *"show steering-objects" on page 1595*
- *"delete steering-object" on page 1598*
- *"delete steering-objects" on page 1599*
- *"set internet-connection-settings" on page 1567*

Syntax

```
set steering-object <Name>
      new-name "<Name>"
      comment "<Text>"
      add
            candidate <Name of Internet Connection>
      candidates-selected {all | specific}
      jitter <0-10000>
      latency <0-10000>
      link-utilization {link-aggregation | prioritize}
      packet-loss <0-100>
      probing-host <IPv4 Address or Hostname>
      second-probing-host <IPv4 Address or Hostname>
      third-probing-host <IPv4 Address or Hostname>
      probing-interval <500-4294967295>
      probing-mode {best | average | worst}
      remove
            all-candidates
            candidate <Name of Internet Connection>
      selection-method <Method>
      set
            candidate <Name of Internet Connection>
                  move {down | up}
                  position <Number>
```

Parameters

Parameter	Description
name	Specifies the name of the SD-WAN steering object. A string that begins with a letter and contain up to 32 characters, of this set: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '.' (period) ■ '-' (minus) ■ '~' (tilde) ■ ' ' (space)

Parameter	Description
comment	**Optional:** Specifies the comment text for the SD-WAN rule. A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '`(`' (opening round bracket) ■ '`)`' (closing round bracket) ■ ':' (colon) ■ '@' (at)
add	Adds the specified Internet connection to the steering behavior object. Press the TAB key to see the available options.
candidates-selected	Specifies the ISP links: ■ `all` - All relevant links (default) ■ `specific` - Specific links
add candidate	Specifies the name of the Internet connection. Press the TAB key to see the available options.
jitter	Configures the jitter threshold (in msec). Default: 30
latency	Configures the latency threshold (in msec). Default: 120
link-utilization	Specifies the ISP link utilization mechanism: ■ `link-aggregation` - Link Aggregation - use all links equally (default). ■ `prioritize` - Prioritize the Internet connections in the specified order.
packet-loss	Configures the packet loss threshold (in %). Default: 1
probing-host	Configures the IPv4 Address or Hostname for the first probing destination. Default: `dns.google.com`

Parameter	Description
second-probing-host	Configures the IPv4 Address or Hostname for the second probing destination. Default: `dns.cloudflare.com`
third-probing-host	Configures the IPv4 Address or Hostname for the third probing destination. Default: `dns.opendns.com`
probing-interval	Configures the interval duration between probes (in msec). Default: 1000
probing-mode	Controls which Internet connection the appliance selects in each steering object based on the probing results: ■ `best` - Selects the Internet connection that has the best probing results (the lowest values for the probing characteristics of packet loss, latency, and jitter). This is the default. ■ `average` - Selects the Internet connection that has the average probing results. ■ `worst` - Selects the Internet connection that has the worst probing results (the highest values for the probing characteristics of packet loss, latency, and jitter). For more details, see the explanation for this parameter in *"set internet-connection-settings" on page 1567*.
remove	Removes the specified Internet connection from the steering behavior object. Press the TAB key to see the available options.
selection-method	Configures the ISP link selection method: ■ `connection-hash` - Connection hash. This is the default. ■ `proportionally-to-download-bandwidth` - Proportionally to download bandwidth. ■ `proportionally-to-upload-bandwidth` - Proportionally to upload bandwidth. ■ `round-robin` - Round robin.
set	Configures settings for the specified Internet connection in the steering behavior object. Press the TAB key to see the available options.
move	Moves the Internet connection in the steering behavior object above or below its current priority.
position	Configures the position (priority) of the Internet connection in the steering behavior object.

Example Command

```
set steering-object Test\ Steering latency 100 jitter 20
```

set sdwan mode

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Enables or disables SD-WAN blade on the appliance.

See *"show sdwan" on page 1589*.

Syntax

```
set sdwan mode {on | off}
```

set sdwan-rule

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Configures existing SD-WAN manual rules - you specify the rule by its name or by its position number.

Important - Before you change an existing SD-WAN rule, make sure to configure the required objects (source, destination, service).

See also:

- *"add sdwan-rule" on page 1575*
- *"show sdwan-rules" on page 1590*
- *"delete sdwan-rule" on page 1597*

SD-WAN Rule Structure

No.	Source	Destination	Applications / Services	Behavior
Rule position	Source objects	Destination objects	Application and Service objects	Steering Behavior object

Syntax

```
set sdwan-rule name <Rule Name>
            add
                  application-id <Object ID>
                  application-name <Object Name>
                  destination <Object Name>
                  service <Object Name>
                  source <Object Name>
            behavior <Steering Object>
            comment "<Text>"
            disabled {true | false}
            new-name <Rule Name>
            new-position <Number>
            position-above <Number>
            position-below <Number>
            remove
                  application-id <Object ID>
                  application-name <Object Name>
                  destination <Object Name>
                  service <Object Name>
                  source <Object Name>
            set
                  application-or-service any
                  destination any
                  source any
```

```
set sdwan-rule position <Number>
            add
                  application-id <Object ID>
                  application-name <Object Name>
                  destination <Object Name>
                  service <Object Name>
                  source <Object Name>
            behavior <Steering Object>
            comment "<Text>"
            disabled {true | false}
            new-name <Rule Name>
            new-position <Number>
            position-above <Number>
            position-below <Number>
            remove
                  application-id <Object ID>
                  application-name <Object Name>
                  destination <Object Name>
                  service <Object Name>
                  source <Object Name>
            set
                  application-or-service any
                  destination any
                  source any
```

Parameters

Parameter	Description
set sdwan-rule name	Specifies the existing SD-WAN rule by its name. Press the TAB key to see the available options.
set sdwan-rule position	Specifies the existing SD-WAN rule by its position. Press the TAB key to see the available options.
{name | position} add	Adds objects to the existing rule.
{name | position} behavior	Specifies the steering behavior object. Press the TAB key to see the available options.
{name | position} comment	**Optional:** Specifies the comment text for the SD-WAN rule. A string that contains less than 257 characters, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '`(`' (opening round bracket) ■ '`)`' (closing round bracket) ■ ':' (colon) ■ '`@`' (at)
{name | position} disabled	Disables (`true`) or enables (`false`) this SD-WAN rule. **Best Practice** - Set the value "`true`" when you add a new rule (see *"add sdwan-rule" on page 1575*). Make sure the rule is configured correctly, and only then change set the value "`false`".
{name | position} new-name	Specifies the new name for the rule.
{name | position} new-position	Specifies the new position number for the rule.
{name | position} position-above	Specifies the rule position above the specified rule position.
{name | position} position-below	Specifies the rule position below the specified rule position.
{name | position} remove	Removes objects from the existing rule.

Parameter	Description
{name | position} set	Configures the value in the specified rule column to "any": ■ `application-or-service any` Configures the service / application in the existing rule to "any". ■ `destination any` Configures the destination in the existing rule to "any". ■ `source any` Configures the source in the existing rule to "any".
application-id	Specifies the application by its ID. Press the TAB key to see the available options.
application-name	Specifies the application by its name. Press the TAB key to see the available options.
destination	Specifies the destination object. Press the TAB key to see the available options.
service	Specifies the service object. Press the TAB key to see the available options.
source	Specifies the source object. Press the TAB key to see the available options.

Example Command

```
add sdwan-rule name MyRule disabled true source IP-Phones
destination SIP-Provider application-name H.323\ Protocol behavior
Business\ Applications
set sdwan-rule name MyRule add service SIP
set sdwan-rule name MyRule disabled false
```

show internet-connection sdwan-settings

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows the SD-WAN settings on the internet connection.

See *"set internet-connection sdwan" on page 1564*.

Syntax

```
show internet-connection <Name> sdwan-settings
```

Parameters

Parameter	Description
internet-connection	Name of the Internet connection. Press the TAB key to see the available options.

Example Output

```
MyGW> show internet-connection Internet2 sdwan-settings
link-type:                      public
override-circuit-id:            false
download-speed:                 1
upload-speed:                   1
circuit-id:                     0
sdwan-tag:
sdwan:                          true
sdwan-backup:                   true
sdwan-nat-ip-address:
sdwan-ip-address-accessibility:directly

MyGW>
```

show internet-connection-settings

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows the SD-WAN probing settings.

See *"set internet-connection-settings" on page 1567*.

Syntax

```
show internet-connection-settings
```

Example Output

```
latency:                        200
jitter:                         80
packet-loss:                    30

probing-mode:                   best
probing-host:                   dns.google.com
second-probing-host:            dns.cloudflare.com
third-probing-host:             dns.opendns.com
probing-interval:               1000
```

show sdwan

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows the SD-WAN mode.

See:

- *"set smart-sdwan" on page 1577*
- *"show smart-sdwan" on page 1592*

Syntax

```
show sdwan
```

Example Output

- When SD-WAN is enabled:

```
mode:                           activated
lock-by-smp:                    false
```

- When SD-WAN is disabled:

```
mode:                           deactivated
lock-by-smp:                    false
```

show sdwan-rules

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows SD-WAN manual rules.

See also:

- *"add sdwan-rule" on page 1575*
- *"set sdwan-rule" on page 1583*
- *"delete sdwan-rule" on page 1597*
- *"set smart-sdwan" on page 1577*
- *"show smart-sdwan" on page 1592*
- *"show smart-sdwan-rules" on the next page*

Syntax

```
show sdwan-rules
```

Example Output

```
MyGW> add sdwan-rule name MyRule comment "My Test Rule" disabled
true source IP-Phones destination SIP-Provider application-name
H.323\ Protocol behavior Business\ Applications
MyGW>
MyGW> show sdwan-rules
position    name             source
    applications-services                    destination
                     behavior              disabled    comment
1           MyRule           IP-Phones
    SIP                                      SIP-Provider
                     Business Applicat...  true        My Test
Rule
MyGW>
```

show smart-sdwan-rules

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows the Smart SD-WAN settings - the predefined rules.

See:

- *"show smart-sdwan" on the next page*
- *"show sdwan-rules" on the previous page*
- *"set smart-sdwan" on page 1577*

Syntax

```
show smart-sdwan-rules
```

Example Output

```
priority    name                          source
              applications-services
              destination                                  behavior
            comment
1           Smart_Web_Conference          Any
              Skype, Facetime, Zoom, Slack, Cisco Webex Teams,
Microsoft Tea...  Any                                        Web
Conferencing
2           Smart_File_Sharing            Any
              FTP, Box, Dropbox, Google Drive-web, Google Drive-
mobile           Any                                       File
Sharing
3           Smart_Remote_Access           Any
              LogMeIn, TeamViewer, Microsoft Remote Desktop
Connection, GoTo...  Any
Remote Access
4           Smart_Gaming                  Any
              Battle.Net, Steam, Xbox Live, Origin, PlayStation
Now              Any                                       Gaming
5           Smart_Business_Applica...  Any
              Salesforce, Gmail, Evernote, Office365, iCloud-
email, GitHub, ...  Any
Business Applicat...
6           Smart_Default_Breakout        Any
              Any
              Any                                          Default
Breakout
```

show smart-sdwan

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows the Smart SD-WAN settings - the default settings.

See *"set smart-sdwan" on page 1577*.

Syntax

```
show smart-sdwan [links]
```

Parameters

Parameter	Description
No parameters	Shows the: ■ Configured Smart SD-WAN mode ■ Configured Smart SD-WAN link utilization mechanism
links	Shows the default ISP link prioritization.

Example Output

```
MyGW> show smart-sdwan
smart-sdwan-mode:              on
smart-link-utilization:        link-aggregation

MyGW>
```

```
MyGW> show smart-sdwan links
-------------------------------------------------------------------
----
| priority  |  connection-name      |  interface       |  backup
  |
-------------------------------------------------------------------
----
| 1         |  Internet1            |  WAN             |  false
  |
| 2         |  Internet2            |  DMZ             |  true
  |
-------------------------------------------------------------------
----
MyGW>
```

show steering-object

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows the configuration of a specified steering behavior object.

See also:

- *"show steering-objects" on the next page*
- *"add steering-object" on page 1571*
- *"set steering-object" on page 1579*
- *"delete steering-object" on page 1598*
- *"delete steering-objects" on page 1599*

Syntax

```
show steering-object <Name>
```

Parameters

Parameter	Description
steering-object-name	Name of the steering behavior object. Press the TAB key to see the available options.

Example Output

```
MyGW> show steering-object Upload\ Intensive
name:                          Upload Intensive
comment:
predefined:                    true
latency:                       120
jitter:                        70
packet-loss:                   3
probing-mode:                  best
probing-host:                  dns.google.com
second-probing-host:           dns.cloudflare.com
third-probing-host:            dns.opendns.com
probing-interval:              1000
candidates-selected:           all
link-utilization:              link-aggregation
candidates:                    Internet1 (WAN), Internet2 (DMZ)
MyGW>
```

show steering-objects

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows all steering behavior objects.

See also:

- *"show steering-object" on the previous page*
- *"add steering-object" on page 1571*
- *"set steering-object" on page 1579*
- *"delete steering-object" on page 1598*
- *"delete steering-objects" on page 1599*

Syntax

```
show steering-objects
```

Example Output

```
name                          comment                          predefined
    latency          jitter           packet-loss      first-
probing-hostprobing-interval candidates-selected   link-
utilization      candidates
Upload Intensive                                                true
    120              40               3
dns.google.com   1000             all                    link-
aggregation      Internet1 (WAN), Internet2 (DMZ)
Download Intensive                                              true
    120              40               3
dns.google.com   1000             all                    link-
aggregation      Internet1 (WAN), Internet2 (DMZ)
Web Conferencing                                                true
    100              40               3
dns.google.com   1000             all                    link-
aggregation      Internet2 (DMZ), Internet1 (WAN)
File Sharing                                                    true
    120              40               3
dns.google.com   1000             all                    link-
aggregation      Internet2 (DMZ), Internet1 (WAN)
Remote Access                                                   true
    100              40               3
dns.google.com   1000             all                    link-
aggregation      Internet2 (DMZ), Internet1 (WAN)
Gaming                                                          true
    70               40               3
dns.google.com   1000             all                    link-
aggregation      Internet2 (DMZ), Internet1 (WAN)
Business Applications                                           true
    100              40               3
dns.google.com   1000             all                    link-
aggregation      Internet2 (DMZ), Internet1 (WAN)
Default Breakout                                                true
    150              40               3
dns.google.com   1000             all                    link-
aggregation      Internet1 (WAN), Internet2 (DMZ)
```

delete sdwan-rule

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Deletes an existing SD-WAN manual rule.

See also:

- *"add sdwan-rule" on page 1575*
- *"set sdwan-rule" on page 1583*
- *"show sdwan-rules" on page 1590*

Syntax

```
delete sdwan-rule
       name <Name>
       position <Number)>
```

Parameters

Parameter	Description
name	Specifies the SD-WAN rule by its name. Press the TAB key to see the available options.
position	Specifies the SD-WAN rule by its position. Press the TAB key to see the available options.

Example Command

```
delete sdwan-rule name MyRule
```

delete steering-object

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Deletes a specified user-defined steering behavior object.

Important - There is no prompt to confirm.

See also:

- *"delete steering-objects" on the next page*
- *"add steering-object" on page 1571*
- *"set steering-object" on page 1579*
- *"show steering-object" on page 1594*
- *"show steering-objects" on page 1595*

Syntax

```
delete steering-object name <Name>
```

Parameters

Parameter	Description
steering-object-name	Name of the steering behavior object. Press the TAB key to see the available options.

Example Command

```
delete steering-object MySteeringObject
```

delete steering-objects

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Deletes all user-defined steering behavior objects.

Important - There is no prompt to confirm.

See also:

- *"delete steering-object" on the previous page*
- *"add steering-object" on page 1571*
- *"set steering-object" on page 1579*
- *"show steering-object" on page 1594*
- *"show steering-objects" on page 1595*

Syntax

```
delete steering-objects
```

Working with Hardware Components

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to work with various hardware components on the appliance.

reboot

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Reboots the appliance.

Syntax

```
reboot
```

Example Command

```
reboot
```

set property

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables and disables the first time configuration (from the USB autoplay configuration or the WebUI).

If you enable the first time configuration, then after the reboot the appliance starts the First Time Configuration Wizard.

Syntax

```
set property USB_auto_configuration {always | once | off}
set property first-time-wizard {always | once}
```

Parameters

Parameter	Description
n/a	

show diag

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows information about your appliance:

- Firmware version
- Serial number
- MAC Addresses
- Hardware capabilities (1 - SD card, 2 - Wireless, 3 - DSL, 4 - POE, 5 - Cellular)
- Voltages
- Temperatures for CPU and RAM (DDR)

Syntax

```
show diag
```

Example Output

```
HostName> show diag


Current system info
-----------------------------------
Current image name: R80_XXXXXXXXX_20_35
Current image version: XXX
Previous image name: R80_XXXXXXXXX_20_35
Previous image version: XXXX
Default image name: R80_XXXXXXXXX_20_35
Default image version: XXX
Bootloader version: XXXXXXXX
HW version : XXX
Serial number : XXXXXXXXXX
HW MAC Address: 00:1C:XX:XX:XX:YY
LAN MAC Address: 00:1C:XX:XX:XX:ZZ
Unit version: 1
Unit model: V0
Marketing capabilities: 0
Management opaque: XXX=:XXX/XXX=:XXX
Hardware capabilities: 2 - Wireless
RTC status: OK
Voltage 3V3:            3.3484V - OK (valid: 3.1500V ~ 3.4500V)
Voltage 12V:            12.3000V - OK (valid: 11.4000V ~ 12.6000V)
Voltage 1V8:            1.8240V - OK (valid: 1.7000V ~ 1.9000V)
Voltage 0V9:            0.9570V - OK (valid: 0.8100V ~ 1.1000V)
Voltage 1V2:            1.2050V - OK (valid: 1.1600V ~ 1.2400V)
Voltage 1V2_SRM:                1.2122V - OK (valid: 1.1600V ~ 1.2400V)
CPU Temperature:                47.0000C - OK (valid: 0.0000C ~ 82.0000C)
CPU Temperature(internal):              52.2650C - OK (valid: 0.0000C ~ 100.0000C)
DDR Temperature:                47.0000C - OK (valid: 0.0000C ~ 80.0000C)
EMMC % of device lifetime used:         0-10% - OK (valid: 0 ~ 90%)
EMMC EOL status:                Normal - OK
Branding file: N/A
Preset File installed: no
-----------------------------------


HostName>
```

show disk usage

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the file system space - used and available.

Syntax

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

Parameters

Parameter	Description
-h	Shows a human readable output with units: ■ K - kilobytes ■ M - megabytes ■ G - gigabytes
-m	Shows an output in 1024*1024 (1 megabyte) blocks
-k	Shows an output in 1024 (1 kiloabyte) blocks

Example Output

```
HostName> show disk-usage -h
Filesystem                Size      Used Available Use% Mounted on
tmpfs                    20.0M      3.6M     16.4M  18% /tmp
tmpfs                    60.0M     11.9M     48.1M  20% /fwtmp
/dev/mmcblk1p8          623.8M      1.8M    576.4M   0% /logs
/dev/mmcblk1p11           1.2G    852.4M    291.8M  74% /storage
/dev/mmcblk1p3          692.7M    427.3M    214.9M  67% /pfrm2.0
tmpfs                    20.0M     12.7M      7.3M  64%
/tmp/log/local
tmpfs                   500.0M         0    500.0M   0% /tetmp
/dev/sda1                14.3G     16.0K     14.3G   0% /mnt/usb1
HostName>
```

show memory usage

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the amount of memory that is being used.

Note - To see the total installed memory, run the "`free`" command in the Expert mode.

Syntax

```
show memory-usage
```

Example Output

```
HostName> show memory-usage
Memory usage is: 1078 MB
HostName>
```

sfp-dsl version

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the SFP DSL modem firmware version.

Syntax

```
sfp-dsl version
```

Example Command

```
> sfp-dsl version
DSP Firmware: 052120_153029_1_62_8463
Local Firmware: 052120_153029_1_62_8463
```

Configuring the USB Modem

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure the USB modem settings.

add usb-modem-advanced

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '_' (underscore)
field-value	Value A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '+' (plus) ■ '=' (equal) ■ '_' (underscore) ■ ':' (colon) ■ '/' (slash) ■ '@' (at)
is-any-device	Does paramter apply to all devices Type: Boolean (true/false)

Parameter	Description
product-id	Product ID Type: A hexadecimal string
vendor-id	Vendor ID Type: A hexadecimal string

Example Command

```
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
```

set usb-modem-advanced

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure a USB modem advanced entry.

Syntax

```
set usb-modem-advanced <id> [ field-name <field-name> ] [ field-
value <field-value> ] [ is-any-device {true | false} ] [ vendor-id
<vendor-id> ] [ product-id <product-id>
```

Parameters

Parameter	Description
field-name	Name A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ '_' (underscore)
field-value	Value A string that contains these characters: ■ a-z (lower-case letters) ■ A-Z (upper-case letters) ■ 0-9 (digits) ■ ',' (comma) ■ '.' (period) ■ '-' (minus) ■ '+' (plus) ■ '=' (equal) ■ '_' (underscore) ■ ':' (colon) ■ '/' (slash) ■ '@' (at)
id	USB modem ID Press the TAB key to see the available options.

Parameter	Description
is-any-device	Controls whether the parameter applies (`true`) or not (`false`) to all devices
product-id	Product ID (a hexadecimal string)
vendor-id	Vendor ID (a hexadecimal string)

Example Command

```
set usb-modem-advanced 1 field-name usb_advanced_config_name
field-value usb_advanced_config_value is-any-device true vendor-id
7AA1 product-id 7AA1
```

set usb-modem-watchdog advanced-settings interval

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set usb-modem-watchdog advanced-settings interval 10
```

set usb-modem-watchdog advanced-settings mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 off
```

Parameters

Parameter	Description
n/a	

Example Command

```
set usb-modem-watchdog advanced-settings mode off
```

delete usb-modem-advanced

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete an advanced entry for an existing USB modem.

Syntax

```
delete usb-modem-advanced <id>
```

Parameters

Parameter	Description
id	USB modem ID Press the TAB key to see the available options.

Example Command

```
delete usb-modem-advanced 1 is-any-device
```

delete usb-modem-advanced-all

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Delete all existing USB modem advanced entries.

Syntax

```
delete usb-modem-advanced-all
```

Parameters

Parameter	Description
n/a	

Example Command

```
delete usb-modem-advanced-all
```

show usb-modem-advanced

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show existing USB modem advanced entries.

Syntax

```
show usb-modem-advanced
```

Parameters

Parameter	Description
n/a	

Example Command

```
show usb-modem-advanced
```

show usb-modem-advanced table

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the existing USB modem advanced entries in a table.

Syntax

```
show usb-modem-advanced table
```

Parameters

Parameter	Description
n/a	

Example Command

```
show usb-modem-advanced table
```

show usb-modem-info

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show existing USB modem information.

Syntax

```
show usb-modem-info
```

Parameters

Parameter	Description
n/a	

Example Command

```
show usb-modem-info
```

show usb-modem-info-table

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show existing USB modem information in a table.

Syntax

```
show usb-modem-info table
```

Parameters

Parameter	Description
n/a	

Example Command

```
show usb-modem-info table
```

show usb-modem-watchdog advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration for additional health monitoring functionality to USB modems.

Syntax

```
show usb-modem-watchdog advanced-settings
```

Example Command

```
show usb-modem-watchdog advanced-settings
```

Configuring the Serial Port

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to work with the Serial Port.

set serial-port

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set serial-port port-speed 9600 flow-control rts-cts disabled on mode console
```

set serial-port passive-mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set serial-port passive-mode tcp-port 8080 allow-implicitly true
```

set serial-port active-mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set serial-port active-mode tcp-port 8080 primary-server-address
myHost.com secondary-server-address myHost.com
```

set serial-port-nine-pin

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the settings for the 9 PIN serial port.

Syntax

```
set serial-port-nine-pin [ port-speed <port-speed> ] [ flow-
control <flow-control> ] [ disabled <disabled> ] [ mode <mode> ]
```

Parameters

Parameter	Description
disabled	Indicates if the 9-PIN serial port is disabled
flow-control	Indicates the method of data flow control to and from the 9 PIN serial port
mode	Indicates if the 9 PIN serial port can be used by a remote telnet server or allow a remote telnet connection to the device connected to the serial port.
port-speed	Indicates the 9 PIN port speed (Baud Rate) of the serial connection

Example Command

```
set serial-port-nine-pin port-speed 9600 flow-control rts-cts
disabled on mode active
```

set serial-port-nine-pin passive-mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the settings for the 9 PIN serial port.

Syntax

```
set serial-port-nine-pin passive-mode [ tcp-port <tcp-port> ] [
allow-implicitly <allow-implicitly> ]
```

Parameters

Parameter	Description
n/a	

Example Command

```
set serial-port-nine-pin passive-mode tcp-port 8080 allow-
implicitly true
```

set serial-port-nine-pin active-mode

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure the settings for the 9 PIN serial port.

Syntax

```
set serial-port-nine-pin active-mode [ tcp-port <tcp-port> ]
[primary-server-address <primary-server-address> ] [ secondary-
server-address <secondary-server-address> ]
```

Example Command

```
set serial-port-nine-pin active-mode tcp-port 8080 primary-server-
address myHost.com secondary-server-address myHost.com
```

show serial-port

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows configuration for the serial port.

Syntax

```
show serial-port
```

Parameters

Parameter	Description
n/a	

Example Command

```
show serial-port
```

show serial-port-nine-pin

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the settings for the 9 PIN serial port.

Syntax

```
show serial-port-nine-pin
```

Example Command

```
show serial-port-nine-pin
```

Additional Hardware Settings

This section provides commands to configure additional hardware settings.

set additional-hw-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 A number with no fractional part (integer)

Example Command

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

show additional-hw-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows advanced hardware related setings.

Syntax

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

Example Command

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

Working with Fonic Bypass

In the R81.10.X releases, this feature is available starting from the R81.10.08 version.

This section provides commands to work with the FONIC (Fail Open Network Interface Card) bypass mechanism implemented between the DMZ and LAN4 ports in the 1595R Wired model.

set fonic-settings advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.08 version.

Description

The 1595R wired model has a FONIC (Fail Open Network Interface Card) bypass mechanism implemented between the DMZ and LAN4 ports.

Use this command to switch FONIC between Active and Bypass mode.

The Bypass mechanism is activated when one of these occurs:

- Power to the appliance is down.
- There is a critical software failure (using watchdog logic).

These are the two Bypass mechanism modes:

- **Active** - The connection between DMZ and LAN4 ports work as a normal system interface and drive data through the appliance, as long as the power is on and the software is valid. If the appliance power is off or the software has a critical problem that prevents it from maintaining a keep-alive mechanism, the Bypass circumvents the DMZ and LAN4 port connection and traffic bypasses the appliance. After power is restored or after a reset, the appliance reboots and the system maintains the bypass between the DMZ/LAN4 ports until the Security Policy is activated. Once the Security Policy is activated, the system will set the Bypass to the mode configured by UI.
- **Force bypass** - The connection between the DMZ and LAN4 port is forcibly bypassed and the traffic bypasses the appliance regardless of the software status. After power is restored or a hardware/software reset, the DMZ-LAN4 port connection is still bypassed until you reconfigure the mode and the software system is valid.

See also:

- *"show fonic-settings advanced-settings" on the next page*

Syntax

```
set fonic-settings advanced-settings mode
```

show fonic-settings advanced-settings

In the R81.10.X releases, this command is available starting from the R81.10.08 version.

Description

The 1595R wired model has a FONIC (Fail Open Network Interface Card) bypass mechanism implemented between the DMZ and LAN4 ports when power to the appliance is down or there is a critical software failure.

Use this command to show the current (FONIC) Bypass configured mode:

See also:

- *"set fonic-settings advanced-settings" on the previous page*

Syntax

```
show fonic-settings advanced-settings
```

Working with Firmware Images

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to work with the appliance firmware images.

show software-version

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the version and the build of the current software.

Syntax

```
show software-version
```

show saved image

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows information about the saved backup image.

Syntax

```
show saved-image
```

show upgrade log

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows upgrade log file content.

Important - To exit the log file view, press the **Q** key.

Syntax

```
show upgrade-log
```

Example Output

```
HostName> show upgrade-log
2021-Sep-01-11:36:45: Executing command: '/opt/fw1/bin/cp_write_
syslog.sh [System Operations] Starting Image upgrade process...'
2021-Sep-01-11:36:45: Checking for active partitions...
2021-Sep-01-11:36:45: Active Kernel is /dev/mmcblk1p1, active root
FS is /dev/mmcblk1p3
2021-Sep-01-11:36:45: Board UID is 00:1C:XX:XX:XX:XX
2021-Sep-01-11:36:45: Board model is V0
... (truncated for brevity) ...
2021-Sep-26-11:36:47: Executing command: '/opt/fw1/bin/cp_write_
syslog.sh [System Operations] Upgrading the appliance software
version'
2021-Sep-26-11:36:47: Current version is R80_XXXXXXXXX_20_30, new
image version is R80_XXXXXXXXX_20_35
2021-Sep-26-11:36:47: Comparing 80 80 20 20 35 35
2021-Sep-26-11:36:47: Preparing storage for image...
2021-Sep-26-11:36:48: Copying data from the image file...
... (truncated for brevity) ...
2021-Sep-26-11:38:25: Entered the upgrade preboot script.
... (truncated for brevity) ...
2021-Sep-26-11:38:25: Current image version is R80_XXXXXXXXX_20_35
2021-Sep-26-11:38:25: Build number is XXXXXXXXX
... (truncated for brevity) ...
HostName>
```

show revert-log

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the log file of previous revert operations.

See *"revert to previous-image" on page 1641*.

Syntax

```
show revert-log
```

upgrade from usb or tftp server

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Upgrades the software image from a file located 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 Command

```
upgrade from tftp server my-tftp-server filename my-new-
software.img
```

update default-image from current-image

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Update default image from currently running image.

Syntax

```
update default-image from current-image preserve-settings {yes |
no} [force {yes | no}]
```

Parameters

Parameter	Description
preserve-settings	Yes - Preserve your current settings No - Do not preserve your current settings
force	Yes - Execute immediately No - Confirm before rebooting

Example Command

```
update default-image from current-image preserve-settings yes
force yes
```

Example Output

```
The system will now reboot.
During this boot, default image will be updated from current
image.
Save settings as part of the image: yes
Save license as part of the image: yes
Save SIC as part of the image: yes
Are you sure you want to continue(yes/no)?
```

revert to previous-image

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Reverts the appliance to the previous software image.

See *"show revert-log" on page 1638*.

Syntax

```
revert to previous-image
```

revert to factory-defaults

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Revert the appliance to the original factory defaults.

Important - This command deletes all data and software images from the appliance.

Syntax

```
revert to factory-defaults
```

Enter `yes` to continue.

Configuring Backup

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to collect backup.

backup settings (TFTP, SFTP, USB)

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Back up settings immediately to TFTP, SFTP, or USB.

Added SCP and FLASH periodic backup methods.

See also:

- *"set periodic-backup (FTP)" on page 1646*
- *"set periodic-backup (TFTP or SFTP)" on page 1647*

Notes:

- While using flash backup in both methods "`set periodic backup`" and "`backup settings`", there cannot be more than 3 backup files in the `/backup/logs/` directory. The oldest backup file will be deleted to free the space for the new backup file.
- While using flash, there is no need to enter username, password, and server.

Syntax

```
backup settings to {usb | tftp server <Server Address> | sftp
server <Server Address> | scp <Server Address> | flash} [filename
<Backup Filename>] [file-encryption {off | on password <Encryption
Password>}] [backup-policy {on | off}] [add-comment "Comment"]
[username <Server Username> password <Server Password>]
```

Parameters

Parameter	Description
to	Specifies the backup destination: ■ USB storage device ■ TFTP server ■ SFTP server ■ SCP ■ Flash
filename	Specifies the name of the backup file
file-encryption	Enables (`on`) or disables (`off`) the encryption of the backup file
backup-policy	Enables (`on`) or disables (`off`) the backup policy
username	Specifies the username on the remote server See *"Special Characters in Gaia Clish" on page 59*
password	Specifies the password on the remote server See *"Special Characters in Gaia Clish" on page 59*

Example Command

```
backup settings to sftp server 192.168.1.1 filename my_backup_file
file-encryption on pass MyEncPassword backup-policy off username
MyServerUsername password MyServerPassword
```

show backup-settings-info

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the information for the previous backup of the appliance's settings.

Syntax

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

The "`show backup-settings-log`" command shows the log file for the previous backup settings operations.

Parameters

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

Example Command

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

set periodic-backup (FTP)

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures periodic backup to a remote FTP server.

See also:

"set periodic-backup (TFTP or SFTP)" on the next page

Syntax

```
set periodic-backup [ mode {on | off} ] [ 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 hh ]
```

Parameters

Parameter	Description
day-of-month	Day of the month to backup 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 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 A number with no fractional part (integer)
schedule	Schedule the frequency of the periodic backup Press TAB to see available options

Parameter	Description
server-address	Backup server name or IPv4 address (FTP) Type: backupUrl
server-password	Backup server password A string that contains alphanumeric and special characters.
server-username	Backup server username A string that contains up to 64 characters **without** spaces, of this set: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '.' (period) ■ '-' (minus) ■ '@' (at)

Example Command

```
set periodic-backup mode true server-address 192.168.1.1 server-
username admin server-password 12345 file-encryption true
encryption-password 67890 schedule monthly day-of-month 2 hour 2
```

set periodic-backup (TFTP or SFTP)

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configure a periodic backup to TFTP or SFTP server.

Added SCP and FLASH periodic backup methods.

See also:

- *"set periodic-backup (FTP)" on the previous page*
- *"backup settings (TFTP, SFTP, USB)" on page 1643*

Notes:

- While using flash backup in both methods “set periodic backup” and “backup settings” there cannot be more than 3 backup files in the /backup/logs folder. The oldest file will be deleted to create room for the new backup file.
- While using flash, there is no need to enter server-username, server-password, or server-address.

Syntax

```
set periodic-backup [ mode {on | off} ] [ server-address <server-ip-address>] [ protocol {ftp | sftp | scp | flash}] [ 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 <hh>]
```

Parameters

Parameter	Description
server-address	IP address of destination
protocol	Valid values: ■ `ftp` ■ `sftp` (default) ■ `scp` ■ `flash`
server-username	User name to authenticate
server-password	Password to authenticate
file-encryption	File encryption is turned on or off
encryption-password	Password to encrypt/decrypt file
schedule	Periodicity of the backup: monthly/weekly/daily
day-of-month	Day of the month on which to backup settings (in case of monthly backup)
day-of-week	Day of the week on which to backup settings (in case of weekly backup)
hour	Hour on which to backup settings

Example Command

```
set periodic-backup mode on server-address 192.168.1.1 protocol
sftp server-username admin server-password 12345 file-encryption
true encryption-password 67890 schedule daily hour 1:00
```

```
set periodic-backup mode on protocol scp server-username <username
> server-password <password> server-address <server> schedule
daily file-encryption false hour 11
```

```
set periodic-backup mode on protocol flash mode true schedule
daily file-encryption false hour 11
```

show periodic-backup

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows periodic backup configuration.

Syntax

```
show periodic-backup
```

Parameters

Parameter	Description
n/a	

Example Command

```
show periodic-backup
```

Restoring Settings

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to restore settings.

restore settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Restores the appliance settings from a backup file.

The backup file can be located on a USB device or on a TFTP / SFTP server.

Important - The appliance automatically reboots after the settings are restored.

Syntax

```
restore settings from { usb | tftp server <serverIP> | sftp server
<serverIP> username <username> password <password> } filename
<file_name>
```

Parameters

Parameter	Description
`file_name`	Name of the backup file.
`serverIP`	IPv4 address of the TFTP / SFTP server.
`username`	Username for authentication on the SFTP server
`password`	Password for authentication on the SFTP server

Example Command

```
restore settings from tftp server 1.1.1.1 filename sg80
```

```
restore settings from sftp server 192.168.1.100 username johnsmith
password verysecretpassword filename
/backups/backupsettingsfile.txt
```

show restore-settings-log / restore-default-settings-log

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the log file content of previous restoring of settings.

Syntax

```
show {restore-settings-log | restore-default-settings-log}
```

Parameters

Parameter	Description
`restore-settings-log`	Shows the log file content for previous restoring of saved settings.
`restore-default-settings-log`	Shows the log file content for previous restoring of the default settings.

Example Command

```
show restore-settings-log
```

restore default-settings

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

Important - The appliance automatically reboots after the default settings are restored.

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 - success.
- 1 - failure.

Example Command

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

Configuring RESTful API

In the R81.10.X releases, this feature is available starting from the R81.10.00 version.

This section provides commands to configure RESTful API.

set rest-api

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enable or disable REST API.

Syntax

```
set rest-api mode {true | false}
```

Parameters

Parameter	Description
n/a	

Example Command

```
set rest-api mode true
```

show rest-api

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Show the REST API status (on or off).

Syntax

```
show rest-api
```

Example Command

```
show rest-api
```

Example Output

```
HostName> show rest-api
mode: on
```

Miscellaneous Commands

This section provides miscellaneous commands.

cpinfo

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Collect a Check Point Support Information (CPinfo) file.

Check Point Support uses this file to understand the appliance configuration.

Syntax

```
cpinfo -h
cpinfo -v
cpinfo [ [-p] [-z] [-o /<path>/<filename> ]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help
`-v`	Shows the CPinfo tool version
`-p`	Includes the policy files in the output
`-z`	Compresses the output file (GZip) Applies only when you use the "`-o`" parameter
`-o /<`*`path`*`>/<`*`filename`*`>`	Specifies the path and the name for the output file If you do not specify the path, the command creates the output file in the current working directory

Example Command

```
[Expert@HostName]# cpinfo -p -z -o /storage/myAppliance.cpinfo

cpinfo (I:0110):        Beginning ...

cpinfo (I:0116):        Latest cpinfo version: http://www.checkpoint.com/downloads/

cpinfo (I:0123):        Getting components list...

cpinfo (I:0124):        Getting CP status...

cpinfo (I:0125):        Getting CP products keys...

cpinfo (I:0126):        Getting CP products version information...

cpinfo (I:0127):        Getting system information...

cpinfo (I:0128):        Getting IP Interfaces information...

cpinfo (I:0129):        Running netstat...

cpinfo (I:0133):        Getting FW-1 data...

cpinfo (I:0136):        Getting license information...

cpinfo (I:0138):        Getting other CP products information...

cpinfo (I:0139):        Getting CPWD (Watch Dog) information...

cpinfo (I:0140):        Getting directory listing...

cpinfo (I:0142):        Getting kernel information...

cpinfo (I:0112):        Embedding files ...

cpinfo (I:0143):        Embedding appliance-specific information...

cpinfo (I:0117):        Zipping output file ...

cpinfo (I:0118):        Zipping output file - done (/storage/myAppliance.cpinfo.gz)

cpinfo (I:0111):        Done
[Expert@HostName]#

[Expert@HostName]# ls -l /storage/myAppliance.cpinfo*
-rw-r--r--    1 root     root      11571353 Sep 17 17:59 /storage/myAppliance.cpinfo.gz
[Expert@HostName]#
```

cpstat

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the status and statistics information of Check Point applications.

Syntax

```
cpstat [-d] [-p <Port>] [-s <SICname>] [-f <Flavor>] [-o <Polling
Interval> [-c <Count>] [-e <Period>]] [-x] [-j] <Application Flag>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. The output shows the SNMP queries and SNMP responses for the applicable SNMP OIDs.
`-p <Port>`	Optional. Port number of the Application Monitoring (AMON) server. The default port is 18192.
`-s <SICname>`	Optional. Secure Internal Communication (SIC) name of the Application Monitoring (AMON) server.
`-f <Flavor>`	Optional. Specifies the type of the information to collect. If you do not specify a flavor explicitly, the command uses the first flavor in the `<Application Flag>`. To see all flavors, run the `cpstat` command without any parameters.

Parameter	Description
`-o <Polling Interval>`	Optional. Specifies the polling interval (in seconds) - how frequently the command collects and shows the information. Examples: ■ 0 - The command shows the results only once and the stops (this is the default value). ■ 5 - The command shows the results every 5 seconds in the loop. ■ 30 - The command shows the results every 30 seconds in the loop. ■ N - The command shows the results every N seconds in the loop. Use this parameter together with the "`-c <Count>`" parameter and the "`-e <Period>`" parameter. Example: `cpstat os -f perf -o 2`
`-c <Count>`	Optional. Specifies how many times the command runs and shows the results before it stops. You must use this parameter together with the "`-o <Polling Interval>`" parameter. Examples: ■ 0 - The command shows the results repeatedly every <*Polling Interval*> (this is the default value). ■ 10 - The command shows the results 10 times every <*Polling Interval*> and then stops. ■ 20 - The command shows the results 20 times every <*Polling Interval*> and then stops. ■ N - The command shows the results N times every <*Polling Interval*> and then stops. Example: `cpstat os -f perf -o 2 -c 2`

Parameter	Description
`-e <Period>`	Optional. Specifies the time (in seconds), over which the command calculates the statistics. You must use this parameter together with the "`-o <Polling Interval>`" parameter. You can use this parameter together with the "`-c <Count>`" parameter. Example: `cpstat os -f perf -o 2 -c 2 -e 60`
`-x`	Generates the output in the XML format
`-j`	Generates the output in the JSON format
`<Application Flag>`	Mandatory. See the table below with flavors for the application flags.

These flavors are available for the application flags:

Note - The available flags depend on the enabled Software Blades.

Feature or Software Blade	Flag	Flavors
List of enabled Software Blades	`blades`	`ips, fw, av, amw, vpn, vpn, aspm, ia, apcl, default`
Operating System	`os`	`default, ifconfig, routing, routing6, memory, old_memory, cpu, disk, perf, multi_cpu, multi_disk, sensors, power_supply, hw_info, all, average_cpu, average_memory, statistics, updates, licensing, connectivity, vsx`
Firewall	`fw`	`default, interfaces, policy, perf, hmem, kmem, inspect, cookies, chains, fragments, totals, totals64, ufp, http, ftp, telnet, rlogin, smtp, pop3, sync, log_connection, all`

Feature or Software Blade	Flag	Flavors
Application Control	appi	default, subscription_status, update_status, RAD_status, top_last_hour, top_last_day, top_last_week, top_last_month
URL Filtering	urlf	default, subscription_status, update_status, RAD_status, top_last_hour, top_last_day, top_last_week, top_last_month
Anti-Virus	ci	default
Threat Prevention	antimalware	default, scanned_hosts, scanned_mails, subscription_status, update_status, history_av_incidents, history_ab_incidents, history_ab_comp_hosts, history_av_comp_hosts, top_sus_urls, top_countries, ab_prm_contracts, av_prm_contracts, ab_prm_contracts, infected_hosts, ab_prm_contracts, av_prm_contracts
Threat Prevention Statistics	monitoring	all, without_network
Threat Prevention Top Events	topEvents	top_last_hour, top_last_day, top_last_week, top_last_month

Feature or Software Blade	Flag	Flavors
Threat Emulation	`threat-emulation`	`default, general_statuses, update_status, scanned_files, malware_detected, scanned_on_cloud, malware_on_cloud, average_process_time, emulated_file_size, queue_size, peak_size, file_type_stat_file_scanned, file_type_stat_malware_detected, file_type_stat_cloud_scanned, file_type_stat_cloud_malware_scanned, file_type_stat_filter_by_analysis, file_type_stat_cache_hit_rate, file_type_stat_error_count, file_type_stat_no_resource_count, contract, downloads_information_current, downloading_file_information, queue_table, history_te_incidents, history_te_comp_hosts`
Statistics for some IPS protections	`asm`	`default, WS`
IPsec VPN	`vpn`	`default, product, IKE, ipsec, traffic, compression, accelerator, nic, statistics, watermarks, all`
QoS	`fg`	`all`
High Availability	`ha`	`default, all`
Certificate Authority	`ca`	`default, crl, cert, user, all`
Anti-Virus	`ci`	`default`
Provisioning Agent	`PA`	`default`
Provisioning Agent	`PAHB`	`default`
Basic Security Gateway Statistics	`web_ui`	`fw, accepted_data, service_count, ips, av, urlf, vpn, aspm`

Feature or Software Blade	Flag	Flavors
Historical status values	`persistency`	`product, TableConfig, SourceConfig`

Return Value

- 0 - success.
- 1 - failure.

Example Output

- Success shows the output.
- Failure shows an appropriate error message.

Example 1

```
[Expert@HostName]# cpstat -f cpu os

CPU User Time (%):   1
CPU System Time (%): 6
CPU Idle Time (%):   93
CPU Usage (%):       7
CPU Queue Length:    -
CPU Interrupts/Sec:  1625
CPUs Number:         4

[Expert@HostName]#
```

Example 2

```
[Expert@HostName]# cpstat os -f perf

Total Virtual Memory (Bytes):             2048765952
Active Virtual Memory (Bytes):            770162204
Total Real Memory (Bytes):                2048765952
Active Real Memory (Bytes):               916725760
Free Real Memory (Bytes):                 1132040192
Memory Swaps/Sec:                         -
Memory To Disk Transfers/Sec:             -
CPU User Time (%):                        1
CPU System Time (%):                      6
CPU Idle Time (%):                        93
CPU Usage (%):                            7
CPU Queue Length:                         -
CPU Interrupts/Sec:                       1641
CPUs Number:                              4
Disk Servicing Read\Write Requests Time: -
Disk Requests Queue:                      -
Disk Free Space (%):                      83
Disk Total Free Space (Bytes):            52432896
Disk Available Free Space (Bytes):        52432896
Disk Total Space (Bytes):                 62914560

[Expert@HostName]#
```

Example 3

```
[Expert@HostName]# cpstat -f default fw

Policy name:  local
Install time: Thu Sep 16 15:44:35 2021


Interface table
-------------------------------------------------
|Name    |Dir|Total   |Accept  |Deny    |Log    |
-------------------------------------------------
|WAN     |in | 5211524| 5208364|    3160|3499377|
|WAN     |out| 8388637| 8388336|     301|      0|
|LAN1    |in |       0|       0|       0|      0|
|LAN1    |out|       0|       0|       0|      0|
|LAN3    |in |       0|       0|       0|      0|
|LAN3    |out|       0|       0|       0|      0|
|LAN1.334|in |    1161|    1161|       0|   2386|
|LAN1.334|out|     520|     520|       0|   2534|
|LAN1.348|in | 8323376| 8323344|      32|      0|
|LAN1.348|out|18681816| 5442172|13239644|      1|
-------------------------------------------------
|        |   |40607034|27363897|13243137|3504298|
-------------------------------------------------



Interface table (64-bit)
--------------------------------
|Name|Dir|Total|Accept|Deny|Log|
--------------------------------
--------------------------------



ISP link table
------------------
|Name|Status|Role|
------------------
------------------


[Expert@HostName]#
```

cpstart

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Starts Check Point services after they were stopped with the *"cpstop" on page 1669* command.

Syntax

```
cpstart
```

Return Value

- 0 - success.
- 1 - failure.

cpstop

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

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

See *"cpstart" on page 1668*.

Syntax

```
cpstop
```

Return Value

- 0 - success.
- 1 - failure.

cpwd_admin

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

The Check Point WatchDog (`cpwd`) is a process that invokes and monitors critical processes such as Check Point daemons on the appliance, and attempts to restart them if they fail.

Among the processes monitored by Watchdog are `sfwd`, `dropbear`, and others.

The list of monitored processes depends on the installed and configured Check Point products and Software Blades.

The Check Point WatchDog writes monitoring information to the `$CPDIR/log/cpwd.elg` log file.

The `cpwd_admin` utility shows the status of the monitored processes, and configures the Check Point WatchDog.

There are two types of Check Point WatchDog monitoring

Monitoring	Description
Passive	WatchDog restarts the process only when the process terminates abnormally. In the output of the `cpwd_admin list` command, the `MON` column shows `N` for passively monitored processes.
Active	WatchDog checks the process status every predefined interval. WatchDog makes sure the process is alive, as well as properly functioning (not stuck on deadlocks, frozen, and so on). In the output of the `cpwd_admin list` command, the `MON` column shows `Y` for actively monitored processes. The list of actively monitored processes is predefined by Check Point. Users cannot change or configure it.

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
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

Parameters

Parameter	Description
`config <options>`	Configures the Check Point WatchDog. See *"cpwd_admin config" on page 1673*.
`del <options>`	Temporarily deletes a monitored process from the WatchDog database of monitored processes. See *"cpwd_admin del" on page 1676*.
`detach <options>`	Temporarily detaches a monitored process from the WatchDog monitoring. See *"cpwd_admin detach" on page 1677*.
`exist`	Checks whether the WatchDog process `cpwd` is alive. See *"cpwd_admin exist" on page 1678*.
`flist <options>`	Saves the status of all monitored processes to a `$CPDIR/tmp/cpwd_list_<Epoch Timestamp>.lst` file. See *"cpwd_admin flist" on page 1679*.
`getpid <options>`	Shows the PID of a monitored process. See *"cpwd_admin getpid" on page 1681*.

Parameter	Description
`kill <options>`	Terminates the WatchDog process `cpwd`. See *"cpwd_admin kill" on page 1682*. **Important** - Do **not** run this command unless explicitly instructed by Check Point Support or R&D to do so.
`list`	Prints the status of all monitored processes on the screen. See *"cpwd_admin list" on page 1683*.
`monitor_list`	Prints the status of actively monitored processes on the screen. See *"cpwd_admin monitor_list" on page 1686*.
`start <options>`	Starts a process as monitored by the WatchDog. See *"cpwd_admin start" on page 1687*.
`start_monitor`	Starts the active WatchDog monitoring - WatchDog monitors the predefined processes actively. See *"cpwd_admin start_monitor" on page 1689*.
`stop <options>`	Stops a monitored process. See *"cpwd_admin stop" on page 1690*.
`stop_monitor`	Stops the active WatchDog monitoring - WatchDog monitors all processes only passively. See *"cpwd_admin stop_monitor" on page 1692*.

cpwd_admin config

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the Check Point WatchDog.

Important - After changing the WatchDog configuration parameters, you must restart the WatchDog process with the "`cpstop`" and "`cpstart`" commands (which restart *all* Check Point processes).

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Parameters

Parameter	Description
`-h`	Shows built-in usage.
`-a <Configuration_Parameter_1>=<Value_1> <Configuration_Parameter_2>=<Value_2> ... <Configuration_Parameter_N>=<Value_N>`	Adds the WatchDog configuration parameters. **Note** - Spaces are not allowed between the name of the configuration parameter, the equal sign, and the value.
`-d <Configuration_Parameter_1> <Configuration_Parameter_2> ... <Configuration_Parameter_N>`	Deletes the WatchDog configuration parameters that user added with the "`cpwd_admin config -a`" command.
`-p`	Shows the WatchDog configuration parameters that user added with the "`cpwd_admin config -a`" command.
`-r`	Restores the default WatchDog configuration.

These are the available configuration parameters and the accepted values:

Configuration Parameter	Accepted Values	Description
`no_limit`	■ Range: -1, 0, >0 ■ Default: 5	If `rerun_mode=1`, specifies the maximal number of times the WatchDog tries to restart a process. ■ -1 - Always tries to restart ■ 0 - Never tries to restart ■ >0 - Tries this number of times
`num_of_procs`	■ Range: 30 - 2000 ■ Default: 2000	Configures the maximal number of processes managed by the WatchDog.
`rerun_mode`	■ 0 ■ 1 (default)	Configures whether the WatchDog restarts processes after they fail: ■ 0 - Does not restart a failed process. Monitor and log only. ■ 1 - Restarts a failed process (this is the default).
`reset_ startups`	■ Range: > 0 ■ Default: 3600	Configures the time (in seconds) the WatchDog waits after the process starts and before the WatchDog resets the process's `startup_counter` to 0. To see the process's startup counter, in the output of the `cpwd_admin list` command, refer to the `#START` column.
`sleep_mode`	■ 0 ■ 1 (default)	Configures how the WatchDog restarts the process: ■ 0 - Ignores timeout and restarts the process immediately ■ 1 - Waits for the duration of `sleep_timeout`
`sleep_ timeout`	■ Range: 0 - 3600 ■ Default: 60	If `rerun_mode=1`, specifies how much time (in seconds) passes from a process failure until WatchDog tries to restart it.
`stop_timeout`	■ Range: > 0 ■ Default: 60	Configures the time (in seconds) the WatchDog waits for a process stop command to complete.

Configuration Parameter	Accepted Values	Description
`zero_timeout`	■ Range: > 0 ■ Default: 7200	After failing `no_limit` times to restart a process, the WatchDog waits `zero_timeout` seconds before it tries again. The value of the `zero_timeout` must be greater than the value of the `timeout`.

The WatchDog saves the user defined configuration parameters in the `$CPDIR/registry/HKLM_registry.data` file in the "`: (Wd_Config`" section:

```
("CheckPoint Repository Set"
  : (SOFTWARE
    : (CheckPoint
      : (CPshared
        :CurrentVersion (6.0)
        : (6.0
        ... ...
          : (reserved
          ... ...
            : (Wd
                : (Wd_Config
                    :Configuration_Parameter_1 ("[4]Value_1")
                    :Configuration_Parameter_2 ("[4]Value_2")
                )
            )
          ... ...
```

Example Command

```
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -a sleep_timeout=120 no_limit=12
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog Configuration parameters are:
sleep_timeout : 120
no_limit : 12
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#

[Expert@HostName:0]# cpwd_admin config -r
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
```

cpwd_admin del

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Temporarily deletes a monitored process from the WatchDog database of monitored processes.

Notes:

- WatchDog stops monitoring the detached process, but the process stays alive.
- The *"cpwd_admin list" on page 1683* command does not show the deleted process anymore.
- This change applies until all Check Point services restart during boot, or with the *"cpstart" on page 1668* command.

Syntax

```
cpwd_admin del -name <Application Name>
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 1683* command in the leftmost column `APP`. Example - `SFWD`

Example Command

```
[Expert@HostName:0]# cpwd_admin del -name SFWD
cpwd_admin:
successful Del operation
[Expert@HostName:0]#
```

cpwd_admin detach

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Temporarily detaches a monitored process from the WatchDog monitoring.

Notes:

- WatchDog stops monitoring the detached process, but the process stays alive.
- The *"cpwd_admin list" on page 1683* command does not show the detached process anymore.
- This change applies until all Check Point services restart during boot, or with the *"cpstart" on page 1668* command.

Syntax

```
cpwd_admin detach -name <Application Name>
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 1683* command in the leftmost column `APP`. Example - `SFWD`

Example Command

```
[Expert@HostName:0]# cpwd_admin detach-name SFWD
cpwd_admin:
successful Detach operation
[Expert@HostName:0]#
```

cpwd_admin exist

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Checks whether the WatchDog process `cpwd` is alive.

Syntax

```
cpwd_admin exist
```

Example Command

```
[Expert@HostName:0]# cpwd_admin exist
 cpwd_admin: cpWatchDog is running
[Expert@HostName:0]#
```

cpwd_admin flist

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Saves the status of all WatchDog monitored processes to a file.

Syntax

```
cpwd_admin flist [-full]
```

Parameters

Parameter	Description
`-full`	Shows the verbose output.

Example Output

Column	Description
APP	Shows the WatchDog name of the monitored process.
PID	Shows the PID of the monitored process.
STAT	Shows the status of the monitored process: ■ E - executing ■ T - terminated
#START	Shows how many times the WatchDog started the monitored process.
START_TIME	Shows the time when the WatchDog started the monitored process for the last time.
SLP/LIMIT	In verbose output, shows the values of the sleep_timeout and no_limit configuration parameters (see *"cpwd_admin config" on page 1673*).
MON	Shows how the WatchDog monitors this process (see the explanation for the *"cpwd_admin" on page 1670*): ■ Y - Active monitoring ■ N - Passive monitoring
COMMAND	Shows the command the WatchDog run to start this process.

Example Command

```
[Expert@HostName:0]# cpwd_admin flist
/opt/fw1/tmp/cpwd_list_3346530290.lst
[Expert@HostName:0]#
```

cpwd_admin getpid

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the PID of a WatchDog monitored process.

Syntax

```
cpwd_admin getpid -name <Application Name>
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 1683* command in the leftmost column `APP`. Example - `SFWD`

Example Command

```
[Expert@HostName:0]# cpwd_admin getpid -name SFWD
10983
[Expert@HostName:0]#
```

cpwd_admin kill

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Terminates the WatchDog process `cpwd`.

Important - Do **not** run this command unless explicitly instructed by Check Point Support or R&D to do so.
To restart the WatchDog process, you must restart all Check Point services with the *"cpstop" on page 1669* and *"cpstart" on page 1668* commands.

Syntax

```
cpwd_admin kill
```

cpwd_admin list

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Prints the status of all WatchDog monitored processes on the screen.

Syntax

```
cpwd_admin list [-full]
```

Parameters

Parameter	Description
`-full`	Shows the verbose output.

Example Output

Column	Description
APP	Shows the WatchDog name of the monitored process.
PID	Shows the PID of the monitored process.
STAT	Shows the status of the monitored process: ■ E - executing ■ T - terminated
#START	Shows how many times the WatchDog started the monitored process.
START_TIME	Shows the time when the WatchDog started the monitored process for the last time.
SLP/LIMIT	In verbose output, shows the values of the sleep_timeout and no_limit configuration parameters (see *"cpwd_admin config" on page 1673*).
MON	Shows how the WatchDog monitors this process (see the explanation for the *"cpwd_admin" on page 1670*): ■ Y - Active monitoring ■ N - Passive monitoring
COMMAND	Shows the command the WatchDog run to start this process.

Example 1 - Standard output

```
[Expert@HostName]# cpwd_admin list
APP         PID    STAT   #START   START_TIME              MON
COMMAND
RNGD        3076   E      1        [16:03:47] 14/9/2021    N
/pfrm2.0/bin/jitterentropy_rngd -v
DROPBEAR    11318  E      1        [16:03:51] 16/9/2021    N
dropbear -F -j -k -p 22 -r /pfrm2.0/etc/dropbear_rsa_host_key -b
/opt/fw1/conf/sshd_banner.txt
cposd       3834   E      1        [16:03:53] 14/9/2021    N    cposd
RTDB        3868   E      1        [16:03:54] 14/9/2021    N    rtdbd
SFWD        10983  E      1        [16:04:55] 14/9/2021    N    fw
sfwd
[Expert@HostName]#
```

Example 2 - Verbose output

```
[Expert@HostName]# cpwd_admin list -full
APP         PID    STAT  #START  START_TIME              SLP/LIMIT
MON
-------------------------------------------------------------------
--------------
RNGD        3076   E     1       [16:03:47] 14/9/2021    60/5
N
            PATH = /pfrm2.0/bin/jitterentropy_rngd
            COMMAND = /pfrm2.0/bin/jitterentropy_rngd -v
-------------------------------------------------------------------
--------------
DROPBEAR    11318  E     1       [16:03:51] 16/9/2021    60/5
N
            PATH = /pfrm2.0/bin/dropbear
            COMMAND = dropbear -F -j -k -p 22 -r
/pfrm2.0/etc/dropbear_rsa_host_key -b /opt/fw1/conf/sshd_
banner.txt
-------------------------------------------------------------------
--------------
cposd       3834   E     1       [16:03:53] 14/9/2021    60/5
N
            PATH = /pfrm2.0/bin/cposd
            COMMAND = cposd
            ENV = SECORM_SKIP_ATTACHED_DBS=1
-------------------------------------------------------------------
--------------
RTDB        3868   E     1       [16:03:54] 14/9/2021    60/5
N
            PATH = /pfrm2.0/bin/rtdbd
            COMMAND = rtdbd
-------------------------------------------------------------------
--------------
SFWD        10983  E     1       [16:04:55] 14/9/2021    60/5
N
            PATH = /opt/fw1/bin/fw
            COMMAND = fw sfwd
[Expert@HostName]#
```

cpwd_admin monitor_list

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Prints the status of actively monitored processes on the screen.

See the explanation about the active monitoring in *"cpwd_admin" on page 1670*.

Syntax

```
cpwd_admin monitor_list
```

Example Command

```
[Expert@HostName:0]# cpwd_admin monitor_list
cpwd_admin:
Server (path=$CPDIR/monitor/cpwd_monitor) does not monitor any process
[Expert@HostName:0]#
```

cpwd_admin start

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Starts a process as monitored by the WatchDog.

Syntax

```
cpwd_admin start -name <Application Name> -path "<Full Path to
Executable>" -command "<Command Syntax>" [-env {inherit | <Env_
Var>=<Value>] [-slp_timeout <Timeout>] [-retry_limit {<Limit> |
u}]
```

Parameters

Parameter	Description
`-name <Application Name>`	Name, under which the `cpwd_admin list` command shows the monitored process in the leftmost column `APP`. Example: `SFWD`
`-path "<Full Path to Executable>"`	The full path (with or without Check Point environment variables) to the executable including the executable name. Must enclose in double-quotes. Example for the DropBear: "`dropbear -F -j -k -p 22 -r /pfrm2.0/etc/dropbear_rsa_host_key -b /opt/fw1/conf/sshd_banner.txt`"
`-command "<Command Syntax>"`	The command and its arguments to run. Must enclose in double-quotes. Example for the SFWD: "`sfwd`"
`-env {inherit | <Env_ Var>=<Value>}`	Configures whether to inherit the environment variables from the shell. ■ `inherit` - Inherits all the environment variables (WatchDog supports up to 80 environment variables) ■ *<Env_Var>=<Value>* - Assigns the specified value to the specified environment variable

Parameter	Description
`-slp_timeout <Timeout>`	Configures the specified value of the "`sleep_timeout`" configuration parameter. See *"cpwd_admin config" on page 1673*.
`-retry_limit {<Limit> | u}`	Configures the value of the "`retry_limit`" configuration parameter. See *"cpwd_admin config" on page 1673*. ■ `<Limit>` - Tries to restart the process the specified number of times ■ `u` - Tries to restart the process unlimited number of times

Example Command

For the list of process and the applicable syntax, see sk97638.

cpwd_admin start_monitor

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Starts the active WatchDog monitoring. WatchDog monitors the predefined processes actively.

See the explanation for the *"cpwd_admin" on page 1670* command.

Syntax

```
cpwd_admin start_monitor
```

Example Command

```
[Expert@HostName:0]# cpwd_admin start_monitor
cpwd_admin:
CPWD has started to perform active monitoring on Check Point services/processes
[Expert@HostName:0]#
```

cpwd_admin stop

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Stops a WatchDog monitored process.

Important - This change does **not** survive reboot.

Syntax

```
cpwd_admin stop -name <Application Name> [-path "<Full Path to Executable>" -command "<Command Syntax>" [-env {inherit | <Env_Var>=<Value>]
```

Parameters

Parameter	Description
`-name <Application Name>`	Name under which the `cpwd_admin list` command shows the monitored process in the leftmost column `APP`. Example - `SFWD`
`-path "<Full Path to Executable>"`	The full path (with or without Check Point environment variables) to the executable including the executable name. Must enclose in double-quotes. Example for the DropBear: `"dropbear -F -j -k -p 22 -r /pfrm2.0/etc/dropbear_rsa_host_key -b /opt/fw1/conf/sshd_banner.txt"`
`-command "<Command Syntax>"`	The command and its arguments to run. Must enclose in double-quotes. Example for the SFWD: `"sfwd"`
`-env {inherit | <Env_Var>=<Value>}`	Configures whether to inherit the environment variables from the shell. ■ `inherit` - Inherits all the environment variables (WatchDog supports up to 80 environment variables) ■ `<Env_Var>=<Value>` - Assigns the specified value to the specified environment variable

Example Command

For the list of process and the applicable syntax, see sk97638.

cpwd_admin stop_monitor

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Stops the active WatchDog monitoring. WatchDog monitors all processes only passively.

See the explanation for the *"cpwd_admin" on page 1670* command.

Syntax

```
cpwd_admin stop_monitor
```

Example Command

```
[Expert@HostName:0]# cpwd_admin stop_monitor
cpwd_admin:
CPWD has stopped performing active monitoring on Check Point services/processes
[Expert@HostName:0]#
```

fwaccel

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Controls the acceleration (SecureXL) for IPv4 traffic.

Important:

- You must run this command in the Expert mode.
- For information about this command, see the:
  R80.20 Performance Tuning Administration Guide >
  Chapter *SecureXL and Falcon Acceleration Cards in R80.20* >
  Section *SecureXL Commands and Debug* >
  Section *'fwaccel' and 'fwaccel6'*.

Syntax

Command	Description
`fwaccel {-h | help}`	Shows the built-in help.
`fwaccel [-i <SecureXL ID>] off <options>`	Stops the acceleration on-the-fly for all SecureXL instances or for the specified instance. This does not survive reboot.
`fwaccel conns <options>`	Shows all connections that pass through SecureXL.
`fwaccel dbg <options>`	Controls the SecureXL Debug.
`fwaccel dos`	Controls the Rate Limiting for DoS Mitigation in SecureXL.
`fwaccel feature <Feature-Name> {on | off}`	Controls the specified SecureXL features.
`fwaccel identities <options>`	This command is deprecated. Do **not** use it.
`fwaccel on <options>`	Starts the acceleration on-the-fly, if it was previously stopped.
`fwaccel ranges <options>`	Shows the loaded ranges.
`fwaccel revoked_ips <options>`	This command is deprecated. Do **not** use it.
`fwaccel stat [-a] [-t] [-v]`	Shows the SecureXL status.
`fwaccel stats <options>`	Shows the acceleration statistics.
`fwaccel synatk <options>`	Controls the Accelerated SYN Defender.
`fwaccel tab -t <Table-Name>`	Shows the contents of the specified SecureXL table.
`fwaccel templates <options>`	Shows the SecureXL templates.
`fwaccel ver`	Shows the SecureXL and FireWall version.

Example Output - fwaccel stat

```
[Expert@HostName]# fwaccel stat
+-------------------------------------------------------------------
------------+
|Id|Name |Status     |Interfaces               |Features
          |
+-------------------------------------------------------------------
------------+
|0 |SND  |enabled    |WAN,LAN1,LAN3
|Acceleration,Cryptography     |
|  |     |           |                         |Crypto:
Tunnel,UDPEncap,MD5,  |
|  |     |           |
|SHA1,NULL,3DES,DES,CAST,      |
|  |     |           |                         |CAST-40,AES-
128,AES-256,ESP,  |
|  |     |           |
|LinkSelection,DynamicVPN,     |
|  |     |           |                         |NatTraversal,AES-
XCBC,SHA256  |
+-------------------------------------------------------------------
------------+

Accept Templates : enabled
Drop Templates   : disabled
NAT Templates    : enabled
[Expert@HostName]#
```

Example Output - fwaccel conns

```
[Expert@HostName]# fwaccel conns
Source          SPort Destination     DPort PR Flags           C2S
i/f S2C i/f Inst PPAK ID Policy ID  CPU Held Pkts TTL/Timeout
--------------- ----- --------------- ----- -- --------------- ---
---- ------- ---- ------- ---------- --- --------- -----------
    192.168.1.1   443   172.30.129.96 52122  6 ...A..S..L.....
5/1     1/5    3       0 935426077   2         0   16/23
  172.30.129.96 52121     192.168.1.1   443  6 ...A..S........
5/1     1/5    1       0 935426077   0         0    6/11
  172.30.129.96 52122     192.168.1.1   443  6 ...A..S........
5/1     1/5    3       0 935426077   2         0   16/23
    192.168.1.1   443   172.30.129.96 52121  6 ...A..S..L.....
5/1     1/5    1       0 935426077   0         0    6/11

Idx Interface
--- ---------
  0 lo
  1 WAN
  3 LAN1
  4 LAN3

Total number of connections: 2
Total number of links: 2
[Expert@HostName]#
```

Example Output - fwaccel stats

```
[Expert@HostName]# fwaccel stats
Name                          Value         Name
       Value
---------------------------  ------------  ----------------------
------  ------------

Accelerated Path
-------------------------------------------------------------------
--------------------
accel packets                          64363    accel bytes
              3261056
outbound packets                      120267    outbound bytes
              9857792
conns created                          21455    conns deleted
                21454
C total conns                              1    C TCP conns
                    1
C non TCP conns                            0    nat conns
                    0
dropped packets                            0    dropped bytes
                    0
fragments received                         3    fragments transmit
                    0
fragments dropped                          0    fragments expired
                    0
IP options stripped                        0    IP options restored
                    0
IP options dropped                         0    corrs created
                    0
corrs deleted                              0    C corrections
                    0
corrected packets                          0    corrected bytes
                    0

Accelerated VPN Path
-------------------------------------------------------------------
--------------------
C crypt conns                              0    enc bytes
              2683456
dec bytes                            2683472    ESP enc pkts
                55904
```

```
ESP enc err                                0    ESP dec pkts
                55903
ESP dec err                                0    ESP other err
                    0
espudp enc pkts                            0    espudp enc err
                    0
espudp dec pkts                            0    espudp dec err
                    0
espudp other err                           0

Medium Streaming Path
------------------------------------------------------------------
--------------------
CPASXL packets                             0    PSLXL packets
                64363
CPASXL async packets                       0    PSLXL async packets
                64363
CPASXL bytes                               0    PSLXL bytes
              3261056
C CPASXL conns                             0    C PSLXL conns
                    1
CPASXL conns created                       0    PSLXL conns created
                21455
PXL FF conns                               0    PXL FF packets
                    0
PXL FF bytes                               0    PXL FF acks
                    0
PXL no conn drops                          0

Inline Streaming Path
------------------------------------------------------------------
--------------------
PSL Inline packets                         0    PSL Inline bytes
                    0
CPAS Inline packets                        0    CPAS Inline bytes
                    0

QoS Paths
------------------------------------------------------------------
--------------------
QoS General Information:
------------------------
Total QoS Conns                            0    QoS Classify Conns
                    0
```

```
 gtp tcpopt pkts                              0
gtp apn err pkts                             0

General
-------------------------------------------------------------------
--------------------
memory used                                1976    C tcp handshake
conns                     1
C tcp established conns                       0    C tcp closed conns
                      0
C tcp pxl handshake conns                     1    C tcp pxl
established conns                0
C tcp pxl closed conns                        0    outbound cpasxl
packets                     0
outbound pslxl packets                        0    outbound cpasxl
bytes                       0
outbound pslxl bytes                          0    DNS DoR stats
                      0

(*) Statistics marked with C refer to current value, others refer
to total value

[Expert@HostName]#
```

fw commands

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

The "`fw`" commands control various aspects of the Check Point Security Gateway.

To see the available "`fw`" commands, on the command line enter `fw` and press the TAB key.

For some of the CLI commands, you can enter the "`-h`" parameter to the available parameters.

For more information about the `fw`commands, see the *R81.10 CLI Reference Guide*.

Important:

- You must run these commands in the Expert mode.
- You can run these commands in the debug mode: `fw -d ...`
- For more information, see the:
  R81.10 CLI Reference Guide >
  Chapter *Security Gateway Commands* >
  Section *fw*.

Command	Description
`fw activation [-h]`	Activates the license.
`fw agbn_tunnel_mode [-h]`	Tests the tunnel mode for the Reach My Device service (Permanent or On-Demand). See *"Configuring the "Reach My Device" Service" on page 1308*.
`fw avload [-h]`	Loads the Anti-Virus signatures to kernel.
`fw check_available_firmware [-h]`	Checks for firmware updates and activates them if needed.
`fw cloud_activate [-h]`	Connects the appliance to the Cloud Management
`fw cloud_reset_key [-h]`	Resets the Cloud Management registration key to the original or specific value.

Command	Description
`fw ctl [-h]`	Controls the Security Gateway kernel: ■ `arp` ■ `block` ■ `chain` ■ `conn` ■ `debug` ■ `dos` ■ `failmem` ■ `get` ■ `iflist` ■ `install` ■ `kdebug` ■ `leak` ■ `pstat` ■ `resetifn` ■ `sdstat` ■ `set` ■ `setsync` ■ `tcpstrstat` ■ `uninstall` ■ `zdebug`
`fw debug [-h]`	Controls the debug of the SFWD daemon. See sk113090.
`fw fetch <options>`	Fetches the policy from the Management Server (on Centrally Managed), or local directory (on Centrally Managed and Locally Managed).
`fw fetchdefault [-h]`	Fetches the default policy (on Centrally Managed and Locally Managed).
`fw fetchlocal [-h]`	Fetches the last policy from local directory (on Centrally Managed and Locally Managed).
`fw gen_initial_policy [-h]`	Compiles the initial policy (on Centrally Managed and Locally Managed).
`fw log_server_activate [-h]`	On Centrally Managed, configures a Log Server, to which the Security Gateway sends its logs.
`fw monitor [-h]`	Captures the traffic inspected by Software Blades (on Centrally Managed and Locally Managed).

Command	Description
`fw notify_firmware_update [-h]`	Sends a firmware update notification to the Cloud Management.
`fw pull_cert [-h]`	On Centrally Managed, pulls a certificate from the Management Server's Internal Certificate Authority (ICA).
`fw sfwd <options>`	Controls the SFWD daemon.
`fw sic_init [-h]`	On Centrally Managed, initializes the Secure Internal Communication (SIC).
`fw sic_reset [-h]`	On Centrally Managed, resets the Secure Internal Communication (SIC) configuration.
`fw sic_test`	On Centrally Managed, shows status of the Secure Internal Communication (SIC) communication with a Management Server.
`fw smbcloud_report_pdf <options>`	Generates a report PDF file in Cloud Management. Full syntax: `fw smbcloud_report_pdf -d <report-data> -n <report-name> -v {true | false}` In addition, see *"generate report cloud-report" on page 1298*.
`fw stat [-h]`	Shows the installed policy. This command is deprecated - use the "`cpstat fw -f policy`" command (see *"cpstat" on page 1660*).
`fw tab [-h]`	Shows and deletes the contents of the specified kernel tables.
`fw unloadlocal`	Uninstalls all local policies. **Warning:** ■ This command prevents all traffic from passing through the Security Gateway, because it disables the IP Forwarding in the Linux kernel on the Security Gateway. ■ This command removes all policies from the Security Gateway. This means that the Security Gateway accepts all incoming connections destined to all active interfaces without any filtering or protection enabled.
`fw ver [-k]`	Shows the Firewall version.

fetch policy

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 - success.
- 1 - failure.

Example Command

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

fetch certificate

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
fetch certificate mgmt-ipv4-address 192.168.1.100 gateway-name
SMB_Appliance
```

kernel-parameter

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

These Gaia Clish commands configure kernel parameters in the `/opt/fw1/boot/modules/fwkern.conf` file to control the advanced Security Gateway behavior.

Syntax

```
kernel-parameter
      delete name <Parameter Name>
      set
            int name <Parameter Name> value <Integer Value> [read_
only]
            string name <Parameter Name> value "<String Value>"
[read_only]
      show
```

Commands

- To configure a specified value for a specified kernel parameter and save it in the `/opt/fw1/boot/modules/fwkern.conf` file:

  These are available scenarios and commands:

  - For integer parameters whose value can be changed on-the-fly in the current session:

    ```
    kernel-parameter set type int name <Parameter Name> value
    <Integer Value>
    ```

  - For integer parameters whose value can be changed only during boot:

    ```
    kernel-parameter set type int name <Parameter Name> value
    <Integer Value> read_only
    ```

  - For string parameters whose value can be changed on-the-fly in the current session:

    ```
    kernel-parameter set type string name <Parameter Name>
    value "<String Value>"
    ```

  - For string parameters whose value can be changed only during boot:

    ```
    kernel-parameter set type string name <Parameter Name>
    value "<String Value>" read_only
    ```

- To see all configured kernel parameters in the `/opt/fw1/boot/modules/fwkern.conf` file:

  ```
  kernel-parameter show
  ```

- To remove a specified kernel parameter from the `/opt/fw1/boot/modules/fwkern.conf` file:

  ```
  kernel-parameter delete name <Parameter Name>
  ```

set advanced-settings ipip-enabled

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables or disables the IPIP feature.

IPIP, a variation of DS-Lite, is used to tunnel IPv4 traffic over IPv6-only networks. As in DS-Lite, the IPv4 traffic is tunneled over an existing IPv6 connection. The DS-Lite/IPIP tunnel is created between the client (gateway) and a peer (AFTR which resides on the ISP and is configured statically or acquired via DHCPv6).

Note - Before you can configure the IPIP feature on a specific internet connection, you must enable the IPIP feature in the Advanced Settings.

Syntax

```
set advanced-settings ipip-enabled { on | off }
```

Parameters

Parameter	Description
ipip-enabled	Enables (`on`) or disables (`off`) the IPIP feature.

Example Command

```
set advanced-settings ipip-enabled on
```

set device-details auth-cert

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the authentication certificate for WebUI on this device.

You can see and install the certificates in WebUI > **VPN** view > **Certificates** > **Installed Certificates**.

See:

- *"show device-details" on page 1716*
- *"add internal-certificate" on page 1313*

Syntax

```
set device-details auth-cert { defaultCert | <Installed
Certificate> }
```

Parameters

Parameter	Description
auth-cert	The authentication certificate. Press the TAB key to see the available options.

Example Command

```
set device-details auth-cert defaultCert
```

set device-details country

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the device's country for the WLAN.

Syntax

```
set device-details country <country>
```

Parameters

Parameter	Description
country	The country where you are located. Press the TAB key to see the available options.

Example Command

```
set device-details country united-states
```

set device-details hostname

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the device's hostname.

Syntax

```
set device-details hostname <hostname>
```

Parameters

Parameter	Description
hostname	The appliance name used to identify the gateway. A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '-' (minus)

Example Command

```
set device-details hostname My-appliance
```

set device-details hostname-prefix

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Configures the prefix in the device's default hostname.

During the image installation, Gaia Embedded assigns a hostname in this format:

```
<Prefix>-<ID>
```

Example:

```
Gateway-ID-7F95E42D
```

Item	Description
Prefix	Gateway-ID
ID	7F95E42D

See:

- *"set device-details hostname" on page 1711*
- *"show device-details" on page 1716*

Syntax

```
set device-details hostname-prefix <prefix>
```

Parameters

Parameter	Description
prefix	The prefix part of the appliance hostname. A string that contains these characters: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '-' (minus)

Example Command

```
set device-details hostname-prefix My-appliance
```

set misp-refresh-route

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Indicates whether acceleration will refresh routes in a multiple ISP configuration.

Syntax

```
set misp-refresh-route mode {true | false}
```

Parameters

Parameter	Description
na	

Example Command

```
set misp-refresh-route mode true
```

set sic_init

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

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 Command

```
set sic_init password verySecurePassword
```

show device-details

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the configuration of basic device details - hostname, country, default certificate.

See:

- *"set device-details auth-cert" on page 1709*
- *"set device-details country" on page 1710*
- *"set device-details hostname" on page 1711*

Syntax

```
show device-details
```

Example 1

```
Gateway-ID-7F95E42D> show device-details
hostname:                       Gateway-ID-7F95E42D
country:                        united-states
auth-cert:                      Default Web Portal Certificate

Gateway-ID-7F95E42D>
```

Example 2

```
Gateway-ID-7F95E42D> show device-details
hostname:                       Gateway-ID-7F95E42D
country:                        united-states
auth-cert:                      Default VPN and Cluster certificate

Gateway-ID-7F95E42D>
```

show internet probe-stats

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Enables the user to get statistics about the internet connection quality (latency, packet loss, etc.) from the last 24 hours with a resolution of 1 minute for the last hour and 1 hour resolution for the rest of the period.

Syntax

```
show internet probe-stats
```

Parameters

Parameter	Description
n/a	

Example Command

```
HostName> show internet probe-stats
wan1:
wan2:
server: dns.google.com:
time        avg[ms] min[ms] max[ms] packet loss[%]
17:00       62.94 52 1205 0.24
18:00       57.63 52 134 0.00
19:00       57.06 52 123 0.08
20:00       57.22 52 1100 0.00
21:00       56.49 52 124 0.00
22:00       57.08 52 88 0.00
23:00       57.49 52 96 0.08
00:00       57.95 53 145 0.00
01:00       59.02 53 1176 0.00
02:00       57.78 53 120 0.00
03:00       57.65 53 105 0.00
04:00       57.39 52 295 0.00
05:00       57.32 53 94 0.00
06:00       57.27 53 222 0.00
06:31       55.33 53 62 0.00
06:32       57.48 53 70 0.00
06:33       55.24 53 63 0.00
06:34       56.76 53 71 0.00
06:35       57.76 53 73 0.00
06:36       56.29 53 64 0.00
06:37       55.90 53 66 0.00
06:38       59.62 53 84 0.00
06:39       55.38 53 64 0.00
06:40       57.95 53 71 0.00
06:41       56.76 53 64 0.00
06:42       56.48 53 69 0.00
06:43       56.45 53 65 0.00
06:44       57.19 53 65 0.00
06:45       56.05 53 66 0.00
06:46       57.52 53 81 0.00
06:47       58.10 53 85 0.00
06:48       58.10 53 74 0.00
06:49       64.81 53 222 0.00
06:50       56.80 53 62 0.00
06:51       58.33 53 76 0.00
06:52       55.81 53 61 0.00
06:53       59.76 53 110 0.00
06:54       57.00 53 77 0.00
06:55       56.76 53 73 0.00
06:56       57.05 53 71 0.00
```

```
06:57       57.86 53 93 0.00
06:58       56.52 53 62 0.00
06:59       55.71 53 62 0.00
07:00       56.90 53 65 0.00
07:01       58.71 53 82 0.00
07:02       57.10 53 79 0.00
07:03       58.81 53 71 0.00
07:04       57.86 53 73 0.00
07:05       55.86 54 64 0.00
07:06       57.15 53 74 0.00
07:07       55.62 53 67 0.00
07:08       56.62 53 73 0.00
07:09       56.95 53 72 0.00
07:10       56.29 53 69 0.00
07:11       57.71 53 84 0.00
07:12       57.71 53 67 0.00
07:13       58.10 53 93 0.00
07:14       58.71 54 81 0.00
07:15       57.24 53 74 0.00
07:16       56.52 53 68 0.00
07:17       61.00 53 93 0.00
07:18       57.60 53 82 0.00
07:19       55.48 53 60 0.00
07:20       58.62 53 76 0.00
07:21       56.76 53 72 0.00
07:22       57.05 53 65 0.00
07:23       57.55 53 71 0.00
07:24       56.62 53 82 0.00
07:25       56.48 53 78 0.00
07:26       56.10 53 64 0.00
07:27       59.10 54 83 0.00
07:28       57.10 53 86 0.00
07:29       60.43 53 97 0.00
07:30       60.00 54 73 0.00
```

show logs

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows Gaia Embedded system and kernel logs.

Syntax

```
show logs {system | kernel}
```

Parameters

Parameter	Description
system	Shows the Gaia Embedded system logs (content of the `/var/log/messages` file).
kernel	Shows the Gaia Embedded kernel logs (the same the `dmesg` command in the Expert mode).

Example Command

```
show logs kernel
```

show rule hits

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Shows the top hits for Firewall policy rules.

Syntax

```
show rule-hits [top <rule>]
```

Parameters

Parameter	Description
rule	Number of rules in the Security Policy for which to show the hits. Minimum value is 1.

Example Output 1

```
HostName> show rule-hits
Top Rule Hits
-------------
Rule Number     Rule Hits
0               3940
0               3247
0               3017
0               2179
HostName>
```

Example Output 2

```
HostName> show rule-hits top 2
Top Rule Hits
-------------
Rule Number     Rule Hits
0               3940
0               3248
HostName>
```

enabled-blades

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

This command allows the user to see a list of the active Software Blades on the appliance. It is available from both Gaia Clish and Expert mode.

Syntax

```
enabled_blades
```

Example Command

```
enabled_blades
```

update security-blades

In the R81.10.X releases, this command is available starting from the R81.10.00 version.

Description

Manually update Software Blades.

Syntax

```
update security-blades [ all ]
```

Example Command

```
update security-blades all
```

Working with VoIP

In the R81.10.X releases, this feature is available starting from the R81.10.10 version.

This section provides commands to work with VoIP.

set voip

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Configures VoIP settings.

See *"show voip" on page 1731*.

Syntax

```
set voip
      allow-pbx-management-from-internet {true | false}
      disable-sip-inspection {true | false}
      external-ip-phones-ipv4-addresses
            add name <Name of Object>
            remove-all name
            remove name <Name of Object>
      external-phones-name <Name of Object>
      external-sip-provider-ipv4-addresses
            add name <Name of Object>
            remove-all name
            remove name <Name of Object>
      ip-Phones-ipv4-addresses
            add name <Name of Object>
            remove-all name
            remove name <Name of Object>
      is-active {true | false}
      log-sip-provider-traffic {true | false}
      pbx-provider-ipv4Address <IPv4 address>
      phones-name <Name of Object>
      sip-provider-name <Name of Object>
      use-pbx {true | false}
      use-public-phones {true | false}
      use-sip-provider {true | false}
      use-vpn-remote-access-phones {true | false}
      use-vpn-site-to-site-phones {true | false}
```

Parameters

Parameter	Description
`allow-pbx-management-from-internet`	Specifies whether to allow access to the PBX management portal from the Internet: ■ `true` - Allow (this is the default) ■ `false` - Block
`disable-sip-inspection`	Specifies whether to disable the inspection of SIP-based traffic: ■ `true` - Disable ■ `false` - Enable (this is the default) Note - RTP services must be configured.
`external-ip-phones-ipv4-addresses`	Performs actions in the table that maps names of network objects to phones' external IPv4 addresses: ■ `add name <Name of Object>` Adds an object with the specified name. ■ `remove-all name` Removes all objects. ■ `remove name <Name of Object>` Removes an object with the specified name. Where "`<Name of Object>`" is - A string that contains these characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '–' (minus)
`external-phones-name`	Specifies the object name that represents the external phones that connect with Internet public IP addresses. Where "`<Name of Object>`" is - A string that contains these characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '–' (minus)

Parameter	Description
`external-sip-provider-ipv4-addresses`	Performs actions in the table that maps names of network objects to SIP service provider: ■ `add name <Name of Object>` Adds an object with the specified name. ■ `remove-all name` Removes all objects. ■ `remove name <Name of Object>` Removes an object with the specified name. Where "`<Name of Object>`" is - A string that contains these characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '–' (minus)
`ip-Phones-ipv4-addresses`	Performs actions in the table that maps names of network objects to phones' internal IPv4 addresses: ■ `add name <Name of Object>` Adds an object with the specified name. ■ `remove-all name` Removes all objects. ■ `remove name <Name of Object>` Removes an object with the specified name. Where "`<Name of Object>`" is - A string that contains these characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '–' (minus)
`is-active`	Specifies whether to enable the VoIP configuration: ■ `true` - Enable ■ `false` - Disable (this is the default)
`log-sip-provider-traffic`	Specifies whether to generate logs for traffic from the external (off premises) SIP provider: ■ `true` - Generate ■ `false` - Do not generate (this is the default)

Parameter	Description
`pbx-provider-ipv4Address`	Specifies the IPv4 address of the on-premises SIP (PBX) server.
`phones-name`	Specifies the object name that represents the phones. Where "*<Name of Object>*" is - A string that contains these characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '–' (minus)
`sip-provider-name`	Specifies the object name that represents the external (off premise) SIP service provider. Where "*<Name of Object>*" is - A string that contains these characters **without** space between them: ■ `a-z` (lower-case letters) ■ `A-Z` (upper-case letters) ■ `0-9` (digits) ■ '–' (minus)
`use-pbx`	Specifies whether to use an on-premises SIP server (PBX): ■ `true` - Use ■ `false` - Do not use (this is the default)
`use-public-phones`	Specifies whether to use phones with Internet public IP addresses: ■ `true` - Use ■ `false` - Do not use (this is the default)
`use-sip-provider`	Specifies whether VoIP service is provided by an external (off premises) SIP service provider: ■ `true` - Yes (this is the default) ■ `false` - No
`use-vpn-remote-access-phones`	Specifies whether phones use Remote Access VPN to connect: ■ `true` - Yes ■ `false` - No (this is the default)

Parameter	Description
`use-vpn-site-to-site-phones`	Specifies whether phones use Site to Site VPN to connect: ■ `true` - Yes ■ `false` - No (this is the default)

Example Command

```
set voip is-active true sip-provider-name SIP-Provider phones-name
IP-Phones external-phones-name External-IP-Phones
```

show voip

In the R81.10.X releases, this command is available starting from the R81.10.10 version.

Description

Shows the configured VoIP settings.

See *"set voip" on page 1725*.

Syntax

```
show voip
```

Example Output

```
MyGW> show voip
is-active:                    false
use-sip-provider:             true
sip-provider-name:            SIP-Provider
log-sip-provider-traffic:     false
disable-sip-inspection:       false
use-pbx:                      false
phones-name:                  IP-Phones
pbx-provider-ipv4Address:
allow-pbx-management-from-internet:true
use-vpn-site-to-site-phones:  false
use-vpn-remote-access-phones: false
use-public-phones:            false
external-phones-name:         External-IP-Phones

MyGW>
```

Working with Dr. Spark

In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

This section provides commands to work with Dr. Spark - a tool that can check the Quantum Spark gateway performance and health status.

Notes:

- If the Quantum Spark gateway is connected to the Internet, then this tool automatically updates itself.
- To see information about using this tool in WebUI and to get the latest offline installation package, see the section "**Logs and Monitoring**" > "**Dr. Spark**" in:
  - *R81.10.X Quantum Spark Centrally Managed Administration Guide for 1500, 1600, 1800, 1900, 2000 Appliances*.
  - *R81.10.X Quantum Spark Locally Managed Administration Guide for 1500, 1600, 1800, 1900, 2000 Appliances*.

Installing the Built-In Tool Package

1. Connect to the command line on the Quantum Spark gateway.
2. If your default shell is Gaia Clish, then go to the Expert mode:

   ```
   expert
   ```

3. Run this command to check if the command is already installed:

   ```
   drSMB
   ```

   If the output shows:

   - "`drSMB: command not found`", then go to the next step to install the built-in tool package.

     Example:

     ```
     [Expert@Hostname]# drSMB
     -bash: drSMB: command not found
     [Expert@Hostname]#
     ```

   - The syntax options, then refer to the **Syntax** and **Parameters** sections below.

     Example:

     ```
     [Expert@Hostname]# drSMB
     Usage:  [opt]
     Option:
       diag                  - Display system diagnostics
     [Expert@Hostname]#
     ```

4. Install the built-in tool package:

   ```
   bash /pfrm2.0/bin/doctor-smb.sh
   ```

5. Run this command to make sure the tool is installed:

   ```
   drSMB
   ```

Syntax

```
drSMB diag last_run {verify | print}
drSMB diag light
drSMB diag list [{[TestId1],[TestId2],... | [SectionName]}]
drSMB diag performance [<Time in Sec>]
drSMB diag print [except] [{[TestId1],[TestId2],... |
[SectionName]}]
drSMB diag verify [except] [{[TestId1],[TestId2],... |
[SectionName]}]
```

Parameters

Parameter	Available From	Description
`drSMB diag last_run {verify | print}`	R81.10.05	Shows the latest generated Dr. Spark report. See *"drSMB diag last_run" on the next page*.
`drSMB diag light`	R81.10.08	Runs only Dr. Spark tests that take a short time to run. See *"drSMB diag light" on page 1738*.
`drSMB diag list [<options>]`	R81.10.05	Shows all available Dr. Spark tests. See *"drSMB diag list" on page 1739*.
`drSMB diag performance [<Time in Sec>]`	R81.10.05	Runs only Dr. Spark performance tests. See *"drSMB diag performance" on page 1747*.
`drSMB diag print [<options>]`	R81.10.05	Runs all Dr. Spark tests and shows a verbose output. See *"drSMB diag print" on page 1749*.
`drSMB diag verify [<options>]`	R81.10.05	Runs all Dr. Spark tests and shows an output. See *"drSMB diag verify" on page 1752*.
`[TestId1], [TestId2],...`	R81.10.05	You can filter the list of Dr. Spark tests by test names. To see the test names, run: `drSMB diag list`

Parameter	Available From	Description
[*SectionName*]	R81.10.05	You can filter the list of Dr. Spark tests by a section name (one section at a time): ■ Cellular ■ Cluster ■ Connectivity ■ Hardware ■ License ■ Memory ■ Misc ■ OS ■ Performance ■ Policy_and_Configuration ■ Reach_My_Device ■ Sizing ■ SMP ■ Status ■ VPN ■ VSX_Configuration

drSMB diag last_run

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Shows the latest Dr. Spark report generated with the "*"drSMB diag verify" on page 1752*" command.

Syntax

```
drSMB diag last_run {verify | print}
```

Parameters

Parameter	Description
`print`	Shows the latest report with one test after another. This output does not show explicitly if a test passed or failed.
`verify`	Shows the latest report in a table format with the column "`Result`" that explicitly show if a test passed or failed.

Example Output

See *"drSMB diag verify" on page 1752*.

drSMB diag light

In the R81.10.X releases, this command is available starting from the R81.10.08 version.

Description

Generates a brief Dr. Spark report (~50 tests) with general information about the gateway.

Run only the Dr. Spark diagnostic tests that take a short time to run.

Tests with the duration of 0 or 1 seconds are defined as light tests.

Dr. Spark light runs in two scenarios:

- In the Expert mode:

  ```
  drSMB diag light
  ```

- Night job:

  In R81.10.10 and higher, you can choose how the job runs: Dr. Spark light or Dr. Spark full.

  In R81.10.08, you can only run Dr. Spark light.

Syntax

```
drSMB diag light
```

Example Output

Output is the same as *"drSMB diag print" on page 1749*, but with fewer tests.

drSMB diag list

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Shows a list of available Dr. Spark tests.

Syntax

```
drSMB diag list [{[TestId1],[TestId2],... | [SectionName]}]
```

Parameters

Parameter	Description
[*TestId1*], [*TestId2*],...	Optional parameter. Specifies the tests by their names or their numbers. To see the test names, run: `drSMB diag list`
[*SectionName*]	Optional parameter. Specifies the tests by their section name (one section name at a time): ■ `Cellular` ■ `Cluster` ■ `Connectivity` ■ `Hardware` ■ `License` ■ `Memory` ■ `Misc` ■ `OS` ■ `Performance` ■ `Policy_and_Configuration` ■ `Reach_My_Device` ■ `Sizing` ■ `SMP` ■ `Status` ■ `VPN` ■ `VSX_Configuration`

Example Output - tests in the section "Performance"

```
[Expert@MyGW]# drSMB diag list Performance
2024-03-17_19-17-59
-------------------------------------------------------------------
---------------------
| ID | Title                           | Command
                    |
-------------------------------------------------------------------
---------------------
| Performance
                    |
-------------------------------------------------------------------
---------------------
| 20 | Acceleration                    | acceleration_verifier
                    |
| 21 | Accept Templates                | accept_templates_verifier
                    |
| 22 | Number Of Connections           | connections_number_
verifier                    |
| 23 | Connection Balance              | connection_balance_
verifier                    |
| 24 | Sfwd Stability                  | sfwd_stability_verifier
                    |
| 25 | Smart Accel                     | smart_accel_verifier
                    |
| 26 | Policy ByPass                   | policy_bypass_verifier
                    |
| 27 | F2F And F2V Packet Percentage   | packet_percentage_
verifier                     |
| 28 | CoreXL and Dispatchers          | corexl_dispachers_
verifier                     |
| 29 | Interface Affinity              | interface_affinity_
verifier                    |
-------------------------------------------------------------------
---------------------
| Run "drSMB diag print <TestNum>" to display test verbose output
                    |
-------------------------------------------------------------------
---------------------

[Expert@MyGW]#
```

Example Output - specific test

```
[Expert@MyGW]# drSMB diag list 20
2024-03-17_19-54-58
------------------------------------------------------------------------
---------------------
| ID | Title                           | Command
                    |
------------------------------------------------------------------------
---------------------
| Performance
                    |
------------------------------------------------------------------------
---------------------
| 20 | Acceleration                    | acceleration_verifier
                    |
------------------------------------------------------------------------
---------------------
| Run "drSMB diag print <TestNum>" to display test verbose output
                    |
------------------------------------------------------------------------
---------------------

[Expert@MyGW]# drSMB diag list Acceleration
2024-03-17_19-55-04
------------------------------------------------------------------------
---------------------
| ID | Title                           | Command
                    |
------------------------------------------------------------------------
---------------------
| Performance
                    |
------------------------------------------------------------------------
---------------------
| 20 | Acceleration                    | acceleration_verifier
                    |
------------------------------------------------------------------------
---------------------
| Run "drSMB diag print <TestNum>" to display test verbose output
                    |
------------------------------------------------------------------------
---------------------

[Expert@MyGW]#
```

Example Output - full list of tests

```
[Expert@MyGW]# drSMB diag list
2024-03-17_19-05-15
-------------------------------------------------------------------
---------------------
| ID | Title                           | Command
                    |
-------------------------------------------------------------------
---------------------
| Misc
                    |
-------------------------------------------------------------------
---------------------
|  1 | Core Dumps                      | core_dump_verifier -v
                    |
|  2 | Kernel Panics                   | kernel_panic_verifier
                    |
-------------------------------------------------------------------
---------------------
| Policy and Configuration
                    |
-------------------------------------------------------------------
---------------------
|  3 | Administrator Security Settings | administrator_security_
setting               |
|  4 | Policy Status                   | configload_status_
verifier                  |
|  5 | Access Rule                     | access_rule_verifier
                    |
|  6 | Certificates                    | certificates_verifier
                    |
|  7 | RAD Daemon Status               | rad_daemon_verifier
                    |
|  8 | MultiWstlsd Check               | multiwstlsd_verifier
                    |
|  9 | Internet Object                 | internet_object_verifier
```

```
                    |
| 10 | Certificates Expiration         | certificates_expiration_
verifi                |
-------------------------------------------------------------------
--------------------
| Status
                    |
-------------------------------------------------------------------
--------------------
| 11 | Password Complexity             | password_complexity_
verifier                 |
| 12 | Partitions                      | partition_status
                    |
| 13 | Blade Update                    | blade_update_verifier
                    |
| 14 | Blade License Status            | blades_license_verifier
                    |
-------------------------------------------------------------------
--------------------
| Sizing
                    |
-------------------------------------------------------------------
--------------------
| 15 | Memory Script                   | peak_connections_verifier
                    |
| 16 | Connected Hosts                 | connected_hosts_verifier
                    |
-------------------------------------------------------------------
--------------------
| Memory
                    |
-------------------------------------------------------------------
--------------------
| 17 | Allocation Failures             | memory_allocation_
failures                   |
| 18 | Flash Usage                     | flash_usage_verifier
```

```
uster SIC Locally Managed     | cluster_sic_locally_verifier
          |
| 31 | Cluster SIC To Management       | cluster_mgmt_sic_verifier
                    |
| 32 | Standby Internet Connection     | cluster_standby_internet_
conne                |
| 33 | Internet Connection Probing     | cluster_internet_
connection_pr               |
| 34 | Cluster VMAC Status             | cluster_vmac_verifier
                    |
| 35 | Cluster Sync Status             | cluster_sync_verifier
                    |
| 36 | SMP Cluster Setup Status        | cluster_smp_setup_
verifier                   |
| 37 | SMP Cluster SIC Status          | cluster_smp_sic_verifier
                    |
| 38 | Cluster State                   | cluster_state_verifier
                    |
-------------------------------------------------------------------
---------------------
| Reach My Device
                    |
-------------------------------------------------------------------
---------------------
| 39 | RMD Info                        | rmd_info_verifier
                    |
| 40 | Tunnel Status                   | rmd_tunnel_status_
verifier                   |
| 41 | SSH Connectivity                | rmd_ssh_connectivity_
verifier                |
| 42 | APP Connectivity                | rmd_app_connectivity_
verifier                |
| 43 | Proxy Configuration             | rmd_proxy_configuration_
verifi                |
-------------------------------------------------------------------
---------------------
| SMP
                    |
-------------------------------------------------------------------
---------------------
```

```
----------------------------
| License
                   |
-------------------------------------------------------------------
---------------------
| 81 | License Status                  | license_status_verifier
                   |
| 82 | License Region                  | license_region_verifier
                   |
-------------------------------------------------------------------
---------------------
| Wireless
                   |
-------------------------------------------------------------------
---------------------
| 83 | Wifi HW Is Up                   | wifi_hw_verifier
                   |
| 84 | Wireless Down Due To Configured | wireless_down_verifier
                   |
| 85 | Wireless Interference           | wireless_interference_
verifier               |
| 86 | Poor Quality Clients            | poor_quality_clients_
verifier                |
-------------------------------------------------------------------
---------------------
| Run "drSMB diag print <TestNum>" to display test verbose output
                   |
-------------------------------------------------------------------
---------------------

[Expert@MyGW]#
```

drSMB diag performance

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Generates a report with general information about the gateway performance.

To get this report in WebUI, click the **Home** view > in the **Troubleshooting** section, click the **Dr. Spark** page > click **Dr. Spark - Load**.

Syntax

```
drSMB diag performance [<Time in Sec>]
```

Parameters

Step	Instructions
<Time in Sec>	You can specify the test duration. The default test duration is 10 seconds.

Example Output

```
[Expert@MyGW]# drSMB diag performance
2024-03-17_19-51-35

Running the performance test, output will be displayed in about 30
sec.

Gateway Performance:

Number of hosts: 0
Number of connections: 12
Connection rate: 11 per second
Throughput:
 Receive: 16458 Kbps
 Transmit: 1343 Kbps
Packet Rate:
 Receive: 206 packets per second
 Transmit: 16 packets per second
SSL is disabled
-----Blade Status-----
Blade IPS is disabled
Blade AV is disabled
Blade AB is disabled
Blade TE is disabled
Blade ASPAM is disabled
VPN-RA is active
VPN-S2S is disabled
NGTP is disabled
----CPU and Memory----
Average available CPU is 98.36%
Available CPU on CPU 1 is 98.37%
Available CPU on CPU 2 is 98.31%
Available CPU on CPU 3 is 98.42%
Available CPU on CPU 4 is 98.34%
Available memory on the gateway: 6325296 KB
Fw1 memory consumption: 6%
SFWD memory consumption: 111784 KB
[Expert@MyGW]#
```

drSMB diag print

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Generates a full report (~80 tests) with information about the gateway.

The report shows one test result after another (not in a table format).

To get this report in WebUI, click the **Home** view > in the **Troubleshooting** section, click the **Dr. Spark** page > click **Generate the Dr. Spark Report**.

Syntax

```
drSMB diag print [except] [{[TestId1],[TestId2],... |
[SectionName]}]
```

Parameters

Parameter	Description
[*TestId1*], [*TestId2*],...	Optional parameter. Specifies the tests by their names or their numbers. To see the test names, run: `drSMB diag list`
[*SectionName*]	Optional parameter. Includes only the tests in the specified section (one section name at a time): ■ `Cellular` ■ `Cluster` ■ `Connectivity` ■ `Hardware` ■ `License` ■ `Memory` ■ `Misc` ■ `OS` ■ `Performance` ■ `Policy_and_Configuration` ■ `Reach_My_Device` ■ `Sizing` ■ `SMP` ■ `Status` ■ `VPN` ■ `VSX_Configuration`
`except`	Optional parameter. Runs all tests, except the specified.

Example Output - specific test

```
[Expert@MyGW]# drSMB diag print 20
2024-03-17_19-57-05
============================
Acceleration:
============================

Checking acceleration status....
Acceleration is enabled.

-------------------------------------------------------------------
-----------------------------
| Tests Status
                            |
-------------------------------------------------------------------
-----------------------------
| ID | Title                          | Result     | Reason
                            |
-------------------------------------------------------------------
-----------------------------
| Performance
                            |
-------------------------------------------------------------------
-----------------------------
| 20 | Acceleration                   | Passed     | Acceleration
is enabled.                 |
-------------------------------------------------------------------
-----------------------------
| Tests Summary
                            |
-------------------------------------------------------------------
-----------------------------
| Passed: 1/1 test, 0 of them info, 0 of them warning, and 0 of
them N/A.                      |
| Setting MOTD...
                            |
| Output file: /storage/doctor_smb/tempfiles/verifier_sum.20.2024-
03-17_19-57-05.txt           |
-------------------------------------------------------------------
-----------------------------
[Expert@MyGW]#
```

drSMB diag verify

In the R81.10.X releases, this command is available starting from the R81.10.05 version.

Description

Shows the latest generated Dr. Spark report.

Syntax

```
drSMB diag verify [except] [{[TestId1],[TestId2],... |
[SectionName]}]
```

Parameters

Parameter	Description
[*TestId1*], [*TestId2*],...	Optional parameter. Specifies the tests by their names or their numbers. To see the test names, run: `drSMB diag list`
[*SectionName*]	Optional parameter. Specifies the tests by their section name (one section name at a time): ■ `Cellular` ■ `Cluster` ■ `Connectivity` ■ `Hardware` ■ `License` ■ `Memory` ■ `Misc` ■ `OS` ■ `Performance` ■ `Policy_and_Configuration` ■ `Reach_My_Device` ■ `Sizing` ■ `SMP` ■ `Status` ■ `VPN` ■ `VSX_Configuration`
`except`	Optional parameter. Runs all tests, except the specified.

Example Output - verify

```
[Expert@MyGW]# drSMB diag verify
2024-03-17_19-24-14
Duration of tests vary and may take a few minutes to complete

-------------------------------------------------------------------
-------------------------------
| Tests Status
                              |
-------------------------------------------------------------------
-------------------------------
| ID | Title                              | Result     | Reason
                              |
-------------------------------------------------------------------
-------------------------------
| Misc
                              |
-------------------------------------------------------------------
-------------------------------
|  1 | Core Dumps                         | Passed     | Userspace
core was not found.             |
|  2 | Kernel Panics                      | Passed     | No kernel
panics on the current software  |
|    |                                    |            | version.
                              |
-------------------------------------------------------------------
-------------------------------
| Policy and Configuration
                              |
-------------------------------------------------------------------
-------------------------------
|  3 | Administrator Security Settings | Warning    |
Administrator password complexity enforce |
|    |                                    |            | ment is
disabled, you can change it by 's |
|    |                                    |            | et
administrator session-settings'.       |
|  4 | Policy Status                      | Passed     | There is no
policy installation issue.    |
|  5 | Access Rule                        | Passed     | Illegal
access rules was not found.       |
|  6 | Certificates                       | Passed     | There is no
issue with the certificates.  |
|  7 | RAD Daemon Status                  | N/A        | This test is
only for appliances with les |
|    |                                    |            | s then 2GB
```

```
RAM.                              |
|  8 | MultiWstlsd Check               | N/A        | This test is
only for appliances with les |
|    |                                 |            | s then 2GB
RAM.                              |
|  9 | Internet Object                 | Passed     | Object
'Internet' is not present in incom |
|    |                                 |            | ing policy
rules.                            |
| 10 | Certificates Expiration         | Info       | Default VPN
and Cluster certificate expir |
|    |                                 |            | ation is on
Tue Feb 27 14:53:54 2029. Def |
|    |                                 |            | ault Web
Portal Certificate expiration is |
|    |                                 |            |  on Sun Feb
26 14:53:40 2034.             |
-------------------------------------------------------------------
------------------------------
| Status
                                |
-------------------------------------------------------------------
------------------------------
| 11 | Password Complexity             | Warning    | Warrning:
password complexity for adminis |
|    |                                 |            | trator
passwords level is low. We recomme |
|    |                                 |            | nd you
enforce password complexity for ad |
|    |                                 |            | ministrator
passwords in Device > System  |
|    |                                 |            | >
Administrators > Security Settings.     |
| 12 | Partitions                      | Passed     | All
partitions are less than 90% full.    |
| 13 | Blade Update                    | Passed     | All blades
installation succeed.          |
| 14 | Blade License Status            | Passed     | All the
blades have valid licenses.       |
-------------------------------------------------------------------
------------------------------

...(truncated)...
[Expert@MyGW]#
```

Example Output - print

```
[Expert@MyGW]# drSMB diag print
2024-03-17_19-30-55
==============================
Core Dumps:
==============================

Checking for userspace core....
Userspace core was not found.

==============================
Kernel Panics:
==============================

Checking for kernel panics....
No kernel panics on the current software version.

==============================
Administrator Security Settings:
==============================

Checking administrator security settings....
Administrator password complexity enforcement is disabled, you can
change it by 'set administrator session-settings'.

==============================
Policy Status:
==============================

Checking for policy installation errors....
There is no policy installation issue.

==============================
Access Rule:
==============================

Checking for illegal access rules....
Illegal access rules was not found.

==============================
Certificates:
==============================

Checking certificates....
There is no issue with the certificates.

==============================
```

```
RAD Daemon Status:
==============================

Checking RAD Daemon....
This test is only for appliances with less then 2GB RAM.

==============================
MultiWstlsd Check:
==============================

Checking multiwstlsd...
This test is only for appliances with less then 2GB RAM.

==============================
Internet Object:
==============================

Checking if object 'Internet' is present in incoming policy
rules....
Object 'Internet' is not present in incoming policy rules.

...(truncated)...
[Expert@MyGW]#
```