QUANTUM

23 October 2024

# GAIA

# R82

Administration 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 R82

For more about this release, see the R82 home page.

### 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 |
|---|---|
| 21 October 2024 | First release of this document |

# Table of Contents

# Gaia Overview

Gaia is the Check Point next generation operating system for security applications. In Greek mythology, Gaia is the mother of all, which represents closely integrated parts to form one efficient system. The Gaia Operating System supports the full portfolio of Check Point Software Blades, Gateway and Security Management products.

Gaia is a unified security Operating System that combines the best of Check Point original operating systems, and IPSO, the operating system from appliance security products. Gaia is available for all Check Point Security Appliances and Open Servers.

Designed from the ground up for modern high-end deployments, Gaia includes support for:

- **IPv4 and IPv6** - fully integrated into the Operating System.
- **High Connection and Virtual Systems Capacity** - 64-bit Linux kernel support.
- **Load Sharing** - ClusterXL and Interface bonding.
- **High Availability** - ClusterXL, VRRP, Interface bonding.
- **Dynamic and Multicast Routing** - BGP, OSPF, RIP, PIM-SM, PIM-DM, IGMP.
- **Easy to use Command Line Interface** - Commands are structured with the same syntactic rules. An enhanced help system and auto-completion simplifies user operation.
- **Role-Based Administration** - Lets Gaia administrators create different roles. Administrators can let users define access to features in the users' role definitions. Each role can include a combination of administrative (read/write) access to some features, monitoring (read-only) access to other features, and no access to other features.

### Gaia CPUSE:

- Get updates for licensed Check Point products directly through the operating system.
- Download and install the updates more quickly. Download automatically, manually, or periodically. Install manually or periodically.
- Get email notifications for newly available updates and for downloads and installations.
- Easy rollback from new update.

### Gaia API:

See sk143612 and *Check Point Gaia API Reference*.

# Introduction to the Gaia Portal

This chapter gives a brief overview of the Gaia Portal interface and procedures for using the interface elements.

## Gaia Portal Overview

- The Gaia Portal is an advanced, web-based interface for Gaia platform configuration.

  You can do almost all system configuration tasks through this Web-based interface.

- Easy Access - Simply connect with a web browser to:

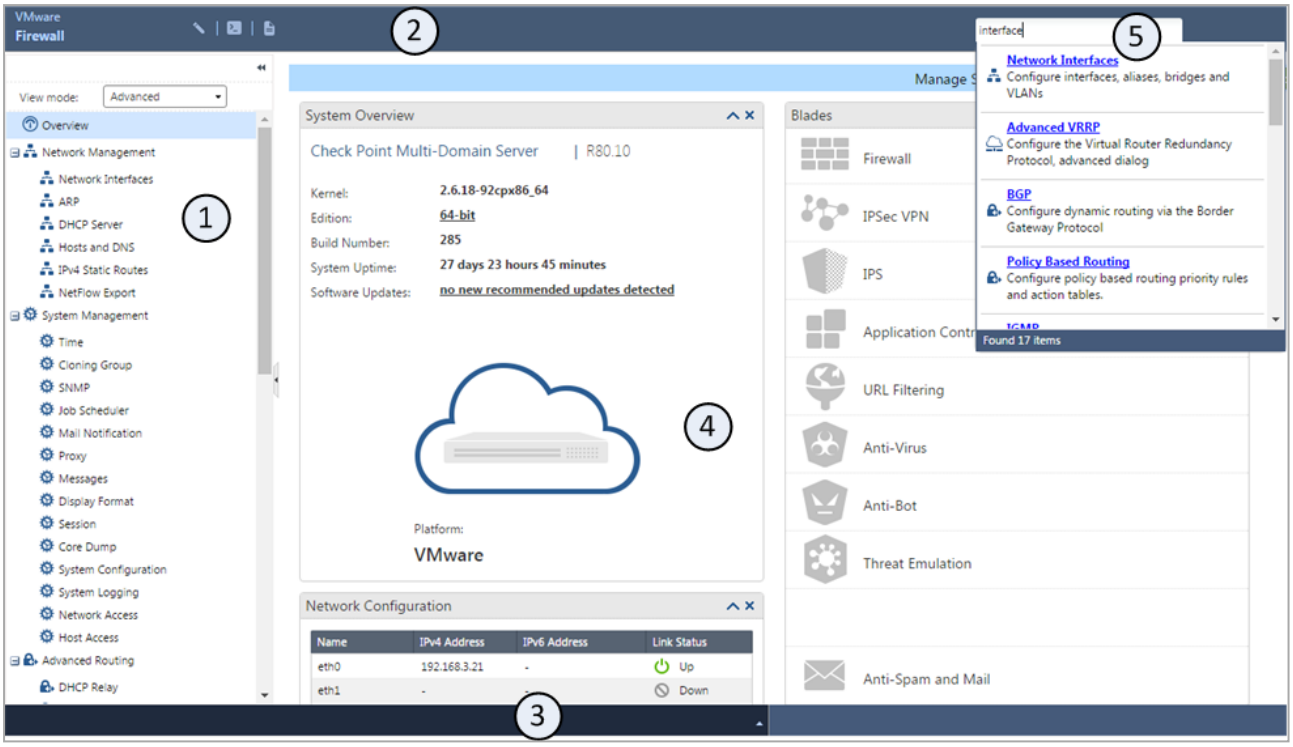
  ```
  https://<IP Address of Gaia Management Interface>
  ```

  **Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

- Browser Support - Microsoft Edge, Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, and Apple Safari.
- Powerful Search Engine - Makes it easy to find features or functionality to configure.
- Easy Operation - Two operating modes:
  - Simplified mode, which shows only basic configuration options.
  - Advanced mode, which shows all configuration options.

  You can easily change these modes.
- Web-Based Access to Command Line - Clientless access to the Gaia Clish directly from your web browser.

## The Gaia Portal interface




| Item | Description |
|---|---|
| 1 | Navigation tree |
| 2 | Toolbar |
| 3 | Status bar |
| 4 | Overview page with widgets that show system information |
| 5 | Search tool |

**Note** - The browser *Back* button is **not** supported. Do **not** use it.

## Logging in to the Gaia Portal

### To log in to the Gaia Portal:

| Step | Instructions |
|---|---|
| 1 | Enter this URL in your browser:<br>`https://<IP Address of Gaia Management Interface>`<br>**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group. |
| 2 | Enter your user name and password. |

**Note** - On a Standalone server (a server which runs both a Security Management Server and a Security Gateway), Gaia Portal stops working when you open SmartView Web Application (`https://<Server IP Address>/smartview`).

**Important:**

**SSL connection ports on Security Management Servers R81 and higher**

- A Security Management Server listens to SSL traffic for *all* services on the TCP port **443** in these cases:
  - If you performed a clean installation of a Security Management Server R82 and enabled the **Endpoint Policy Management** Software Blade.
  - If you upgraded a Security Management Server with disabled **Endpoint Policy Management** Software Blade to R82 and enabled this Software Blade after the upgrade.

  In these cases, when **Endpoint Security** SSL traffic arrives at the TCP port 443, the Security Management Server automatically redirects it (internally) to the TCP port 4434.

| Service | URL and Port |
|---|---|
| Gaia Portal | `https://<IP Address of Gaia Management Interface>` |
| SmartView Web Application | `https://<IP Address of Management Server>/smartview/` |
| Management API Web Services (see *Check Point Management API Reference*) | `https://<IP Address of Management Server>/web_api/<command>` |

- If you upgraded a Security Management Server with enabled **Endpoint Policy Management** Software Blade to R82, then the SSL port configuration *remains* as it was in the previous version, from which you upgraded:

- A Security Management Server listens to Endpoint Security SSL traffic on the TCP port 443
- A Security Management Server listens to SSL traffic for *all other* services on the TCP port 4434:

| Service | URL and Port |
|---|---|
| Gaia Portal | `https://<IP Address of Gaia Management Interface>:4434` |
| SmartView Web Application | `https://<IP Address of Management Server>:4434/smartview/` |
| Management API Web Services (see *Check Point Management API Reference*) | `https://<IP Address of Management Server>:4434/web_api/<command>` |

In R81 and higher, an administrator can manually configure different TCP ports for the Gaia Portal (and other services) and Endpoint Security - **443** or **4434**. For the applicable procedures, see the *R82 Harmony Endpoint Security Server Administration Guide* > Chapter *Endpoint Security Architecture* > Section *Connection Port to Services on an Endpoint Security Management Server*.

**SSL connection ports on Security Management Servers R80.40 and lower**

- When you enable the **Endpoint Policy Management** Software Blade on a Security Management Server, the SSL connection port to these services automatically changes from the default TCP port **443** to the TCP port **4434**:

- **Gaia Portal**

| Configuration | URL and Port |
|---|---|
| Default | `https://<IP Address of Gaia Management Interface>` |
| New | `https://<IP Address of Gaia Management Interface>:4434` |

- **SmartView Web Application**

| Configuration | URL and Port |
|---|---|
| Default | `https://<IP Address of Management Server>/smartview/` |
| New | `https://<IP Address of Management Server>:4434/smartview/` |

- **Management API Web Services** (see *Check Point Management API Reference*)

| Configuration | URL and Port |
|---|---|
| Default | `https://<IP Address of Management Server>/web_api/<command>` |
| New | `https://<IP Address of Management Server>:4434/web_api/<command>` |

- When you disable the **Endpoint Policy Management** Software Blade on a Security Management Server, the SSL connection port automatically changes back to the default TCP port **443**.

### Logging out from the Gaia Portal

Make sure that you always log out from the Gaia Portal (in the top right corner) before you close the web browser. This is because the configuration lock stays in effect even when you close the web browser or terminal window. The lock remains in effect until a different user removes the lock, or the defined inactivity time-out period expires (default is 10 minutes).

# Working with the Configuration Lock

Only one user can have Read/Write access to Gaia configuration settings at a time. All other users can log in with Read-Only access to see configuration settings, as specified by their assigned roles (see *"Roles" on page 480*).

When you log in and no other user has Read/Write access, you get an exclusive configuration lock with Read/Write access. If a different user already has the configuration lock, you have the option to override their lock. If you:

- Override the lock. The other user stays logged in with Read-Only access.
- Do not override the lock. You cannot modify the settings.

**Overriding a configuration lock in the Gaia Portal**

- Click the **Configuration lock**  (above the toolbar). The pencil icon (Read/Write enabled) replaces the lock.
- If you use a configuration settings page, click the **Click here to obtain lock** link. You can see this link if a different user overrides your configuration lock.

**Note** - Only users with Read/Write access privileges can override a configuration lock.

# Using the Gaia Portal Interface Elements

The Gaia Portal contains many elements that make the task of configuring features and system settings easier.

## Toolbar Accessories

You can use these toolbar icons to do these tasks

| Item | Description |
|---|---|
|  | Read/Write mode enabled. |
|  | Configuration locked (Read Only mode). |
|  | Opens the **Console** accessory for CLI commands.<br>Available in the Read/Write mode only. |
|  | Opens the **Scratch Pad** accessory for writing notes or for quick copy and paste operations.<br>Available in the Read/Write mode only. |

## Search Tool

You can use the search bar to find an applicable configuration page by entering a keyword. The keyword can be a feature, a configuration parameter or a word that is related to a configuration page.

The search shows a list of pages related to the entered keyword. To go to a page, click a link in the list.

## Navigation Tree

The navigation three lets you select a page. Pages are arranged in logical feature groups. You can show the navigation tree in one of these view modes:

| Mode | Description |
|---|---|
| **Basic** | Shows some standard pages. |
| **Advanced** | Shows all pages. This is the default mode. |

To change the navigation tree mode, click **View Mode** and select a mode from the list.

To hide the navigation tree, click the **Hide**  icon.

## Status Bar

The status bar, located at the bottom of the window, shows the result of the last configuration operation.

To see a history of the configuration operations during the current session, click the **Expand** icon.

## Configuration Tab

The **Configuration** tab lets you see and configure parameters for Gaia features and settings groups. The parameters are organized into functional settings groups in the navigation tree. You must have Read/Write permissions for a settings group to configure its parameters.

## Monitoring Tab

The **Monitoring** tab lets you see status and detailed operational statistics, in real time, for some routing and high availability settings groups. This information is useful for monitoring dynamic routing and VRRP cluster performance.

To see the **Monitoring** tab, select a routing or high availability feature settings group and then click the **Monitoring** tab. For some settings groups, you can select different types of information from a menu.

# Unsupported Characters and Words

To prevent possible Cross-Site Scripting (XSS) attacks, Gaia Portal does not accept some characters and words when you enter them in various fields.

### Unsupported Characters

| Character | Description |
|---|---|
| < | Less than |
| > | Greater than |
| & | Ampersand |
| ; | Semi-colon |

### Unsupported Words

- `after`
- `apply`
- `catch`
- `eval`
- `subset`

**Note** - Gaia Portal does not support Content Security Policy (CSP).

# System Information Overview

*In This Section:*



This chapter shows you how to see system information in the Gaia Portal and Gaia Clish.

# Showing System Overview Information in Gaia Portal

**Important:**

- If you connected to the Gaia Portal of the applicable Security Group, these actions apply to the entire Security Group.
- If you connected to the Gaia Portal of the applicable Security Group Member, these actions apply only to that Security Group Member.

The **Overview** page shows status widgets.

You can add or remove widgets from the page, move them around the page and minimize or expand them.

**Widgets**

| Widget | Description |
|---|---|
| **System Overview** | System information, including:<br>■ Installed product (for example: Check Point Security Management Server, Check Point Security Gateway)<br>■ Product version number (for example: R82)<br>■ Kernel edition (32-bit, or 64-bit)<br>■ Product build number<br>■ System uptime<br>■ hardware platform, on which Gaia is installed<br>■ Computer serial number (on Check Point appliances) |
| **Blades** | Installed Software Blades.<br>Those that are enabled in SmartConsole, are colored.<br>Those that are disabled in SmartConsole, are grayed out. |

| Widget | Description |
|---|---|
| **Network Configuration** | Interfaces, their IP Addresses and Link Status. |
| **CPU Monitor** | Graphical display of CPU usage. |
| **Memory Monitor** | Graphical display of memory usage. |
| **Packet Rate** | Graphical display of the overall traffic packet rate. |
| **Throughput** | Graphical display of the overall traffic throughput. |

### Adding a widget to the page

| Step | Instructions |
|---|---|
| 1 | Scroll down to the bottom of this page. |
| 2 | Click **Add Widget** and select a widget to show. |

### Moving a widget on the page

| Step | Instructions |
|---|---|
| 1 | Left-click the widget title bar. |
| 2 | Hold the left mouse button. |
| 3 | Drag the widget to the applicable location. |
| 4 | Release the left mouse button. |

# Showing System Overview Information in Gaia Clish

**Important for Scalable Platforms:**

- If you connected to the Gaia gClish of the applicable Security Group, these commands apply to the entire Security Group.
- If you connected to the Gaia Clish of the applicable Security Group Member, these commands apply only to that Security Group Member.

You can use these commands to show system status:

**The "show uptime" command**

**Description**

Shows how long the Gaia system is up and running.

**Syntax**

```
show uptime
```

### The "show version" command

#### Description

Shows the name and versions of the Gaia OS components.

#### Syntax

- To show the full system version information:

```
show version all
```

- To show version information for OS components:

```
show version os
      build
      edition
      kernel
```

- To show name of the installed product:

```
show version product
```

#### Parameters

| Parameter | Description |
|---|---|
| `all` | Shows all Gaia system information. |
| `os build` | Shows the Gaia build number. |
| `os edition` | Shows the Gaia kernel edition. |
| `os kernel` | Shows the Gaia kernel build number. |
| `product` | Shows the Gaia version. |

# Getting Started

1. Install the Gaia OS.

   See the *R82 Installation and Upgrade Guide*.

2. Run the Gaia First Time Configuration Wizard.

   See *"Configuring Gaia for the First Time" on page 59*.

3. Configure the required interfaces:

   A. Enable the required physical interfaces and assign the required IP addresses.

      See *"Physical Interfaces" on page 103*.

   B. Configure the required special interfaces (Bond, VLAN, Bridge, and so on).

      See *"Network Interfaces" on page 102*.

4. Configure the required DNS settings.

   See *"Hosts and DNS" on page 252*.

5. Configure the required IPv4 and IPv6 static routes.

   See:

   - *"IPv4 Static Routes" on page 268*
   - *"IPv6 Static Routes" on page 279*

6. Configure the required Proxy Server.

   See *"Proxy" on page 310*.

7. Configure the required Roles.

   See *"Roles" on page 480*.

8. Configure the required Users.

   See *"Users" on page 469*.

9. Configure the required Password Policy.

   See *"Password Policy" on page 515*.

10. Install the required license.

    See *"License Status" on page 608*.

11. Install the applicable software updates.

    See *"CPUSE - Software Updates" on page 748*.

# Introduction to the Command Line Interface

This chapter introduces the Gaia command line interface.

The default Gaia shell is called `clish`.

### Using the Gaia Clish

| Step | Instructions |
|---|---|
| 1 | Connect to the Gaia platform using one of these options:<br>■ In SmartConsole (see *"Centrally Managing Gaia Device Settings" on page 91*).<br>■ Using a command-line connection (SSH, or a console). |
| 2 | Log in using a user name and password.<br>Immediately after installation, the default user name and password are `admin` and `admin`. |

### Using the Gaia Clish on Security Groups

To configure Security Groups, use the Gaia gClish (Global Clish):

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on the applicable Security Group. |
| 2 | Log in to Gaia Clish. |
| 3 | Type this command and press Enter:<br>`gclish` |

### Notes for Security Groups:

- You use Gaia gClish like Gaia Clish, but the commands are global by default and apply to all the Security Group Members that are part of a Security Group.

- The Gaia gClish commands are **not** applied on Security Group Members that are in status DOWN.

  If a "`set`" command is performed while an Security Group Member was in status DOWN (either administratively or because of a failure), that command is **not** applied on that Security Group Member. The Security Group Member synchronizes its database during its startup process. If the database changed, the Security Group Member reboots itself to apply the changes.

- The *config-lock* is the lock that protects Gaia gClish database. A single Security Group Member can hold the lock for the system.

  When you run the Gaia gClish "`set`" operations from a specific Security Group Member, you must make sure that this Security Group Member holds the config-lock.

  - To see the current config-lock, run:

    ```
    show {config-lock | config-state}
    ```

  - To acquire the config-lock, run:

    ```
    set config-lock on override
    ```

- The Gaia gClish traffic runs in Security Groups on the Sync interface, on the TCP port 1129.

- Similarly to Gaia Clish, Gaia gClish is capable of running extended commands.

  Run this command to see the list of the Gaia gClish extended commands:

  ```
  show commands extended
  ```

- To run a command on specific set of Security Group Members, run the "`set blade-range`" command.

  This runs all the Gaia gClish embedded commands only on the specified subset of Security Group Members.

  **Best Practice** - Because all Security Group Members must have identical configuration, we highly recommend you use the "`set blade-range`" command.

### Saving the configuration changes

When you change the OS configuration with in Gaia Clish, changes are applied immediately to the running system only.

To have the changes survive a reboot, you must run this command:

```
save config
```

# Syntax Legend for CLI Commands

Whenever possible, this guide lists commands, parameters and options in the alphabetical order.

This guide uses this convention in the Command Line Interface (CLI) syntax:

| Character | Description |
|---|---|
| TAB | Shows the available nested subcommands:<br>`main command`<br>`→ nested subcommand 1`<br>`→ → nested subsubcommand 1-1`<br>`→ → nested subsubcommand 1-2`<br>`→ nested subcommand 2`<br>Example:<br>`cpwd_admin`<br>`config`<br>`-a <options>`<br>`-d <options>`<br>`-p`<br>`-r`<br>`del <options>`<br>Meaning, you can run only **one** of these commands:<br>■ This command: `cpwd_admin config -a <options>`<br>■ Or this command: `cpwd_admin config -d <options>`<br>■ Or this command: `cpwd_admin config -p`<br>■ Or this command: `cpwd_admin config -r`<br>■ Or this command: `cpwd_admin del <options>` |
| Curly brackets or braces<br>**{ }** | Enclose a list of available commands or parameters, separated by the vertical bar **|**.<br>User can enter only one of the available commands or parameters. |

| Character | Description |
|---|---|
| Angle brackets<br>**< >** | Enclose a variable.<br>User must explicitly specify a supported value. |
| Square brackets or brackets<br>**[ ]** | Enclose an optional command or parameter, which user can also enter. |

# Command Completion in Gaia Clish

You can automatically complete a command.

This saves time, and can help if you are not sure what to type next.

| Press these keys... | To do this ... |
|---|---|
| <TAB> | Complete or fetch the keyword.<br>Example:<br>`HostName> set in<TAB>`<br>`inactivity-timeout - Set inactivity timeout`<br>`interface - Displays the interface related parameters`<br>`HostName> set in` |
| <SPACE><TAB> | Show the arguments that the command for that feature accepts.<br>Example:<br>`HostName> set interface<SPACE><TAB>`<br>`eth0 eth1 lo`<br>`HostName> set interface` |
| <ESC><ESC> | See possible command completions.<br>Example:<br>`HostName> set inter<ESC><ESC>`<br>`set interface VALUE ipv4-address VALUE mask-length VALUE`<br>`set interface VALUE ipv4-address VALUE subnet-mask VALUE`<br>`set interface VALUE ipv6-address VALUE mask-length VALUE`<br>`set interface VALUE {comments VALUE mac-addr VALUE mtu VALUE state VALUE speed VALUE duplex VALUE auto-negotiation VALUE}`<br>`set interface VALUE {ipv6-autoconfig VALUE}`<br>`HostName> set inter` |

| Press these keys... | To do this ... |
|---|---|
| SHIFT ? | Get help on a feature or keyword.<br>Example:<br>`HostName> set interface<SPACE><SHIFT ?>`<br>`interface: specifies the interface name`<br>`This operation configures an existing interface`<br>`HostName>` |
| UP arrow<br>DOWN arrow | Browse the command history. |
| LEFT arrow<br>RIGHT arrow | Move the cursor inside the current command to edit it. |
| Enter | Run the current command.<br>The cursor does not have to be at the end of the line. |

# Commands and Features in Gaia Clish

Gaia Clish commands are organized into groups of related features, with a basic syntax:

```
<Operation> <Feature> <Parameter>
```

See *"Summary of Gaia Clish Commands" on page 57*.

| Main operations | Description |
|---|---|
| `add` | Adds or creates a new configuration in the system. |
| `set` | Sets a value in the system. |
| `show` | Shows a value or values in the system. |
| `delete` | Deletes a configuration in the system. |

| Other operations | Description |
|---|---|
| `save` | Saves the configuration changes made since the last save operation. |
| `reboot` | Restart the system. |
| `halt` | Turns off the computer. |
| `quit` | Exits from the Gaia Clish. |
| `exit` | Exits from the shell, in which you work. |
| `start` | Starts a transaction. Puts the Gaia Clish into transaction mode.<br>All changes made using commands in transaction mode are either applied at once, or none of the changes is applied, based on the way transaction mode is terminated. |
| `commit` | Ends transaction by committing changes. |
| `rollback` | Ends transaction by discarding changes. |
| `expert` | Enters the Expert shell. Allows low-level access to the system, including the file system. |
| `ver` | Shows the version of the active Gaia image. |
| `restore` | Restores the configuration of the system. |

| Other operations | Description |
|---|---|
| `help` | Shows help on navigating the Gaia Clish and some useful commands. |

- To see the commands, for which you have permissions, run:

  ```
  show commands
  ```

- To see a list of all features, run:

  ```
  show commands feature<SPACE><TAB>
  ```

- To see all commands for a specific feature, run:

  ```
  show commands feature <FeatureName>
  ```

- To see all commands for an operation of a feature, run:

  ```
  show commands [op <Name>] [feature <Name>]
  ```

- To see all operations, run:

  ```
  show commands op<SPACE><TAB>
  ```

**At the *More* prompt:**

To see the next page, press <SPACE>.

To see the next line, press <ENTER>.

To exit from the *More* prompt, press Q.

# Command History in Gaia Clish

You can recall commands you have used before, even in previous sessions.

| Command | Description |
|---|---|
| ? | Recall the previous command. |
| `history` | Show the last 100 executed commands. |
| `!!` | Run the last executed command. |
| `!nn` | Run a specific previous command from the history list.<br>Example: `!14` |
| `!-nn` | Run the `nn`th previous command from the history list - counting from the most recent command.<br>For example, entering `!-3` runs the third from the last command from the history list. |
| `!str` | Run the most recent command that starts with `str`.<br>Example: `!show` |

### Command Reuse

You can combine word designators with history commands to refer to specific words used in previous commands.

Words are numbered from the beginning of the line with the first word being denoted by `0` (digit zero).

Use a colon (`:`) to separate a history command from a word designator.

For example, you could enter `!!:1` to refer to the first argument in the previous command.

In the command "`show interfaces`", the `interfaces` is word 1.

| Word Designator | Meaning |
|---|---|
| `0` | The operation word. |
| `n` | The `n`th word. |
| `^` | The first argument (that is, word 1). |
| `$` | The last argument. |
| `%` | The word matched by the most recent `\?str\?` search. |

Immediately after word designators, you can add a sequence of one or more of these modifiers, each preceded by a colon:

| Modifier | Meaning |
|---|---|
| `p` | Print the new command, but do not execute. |
| `s/str1/str2` | Replace `str1` with `str2` in the first occurrence of the word, to which you refer. |
| `g` | Apply changes over the entire command.<br>Use this modified in conjunction with `s`, as in `gs/str1/str2`. |

# Moving and Editing in Gaia Clish

This table shows the keyboard keys you can use to move within the syntax and edit the syntax:

| Keys | Action |
|---|---|
| **CTRL L** | Clears the screen and shows the current typed command at the top of the screen. |
| **Home**, **CTRL A** | Moves to the beginning of the command line. |
| **End**, **CTRL E** | Moves to the end of the command line. |
| **Left-Arrow**, **CTRL B** | Moves to the previous character to the left of the cursor. |
| **Right-Arrow**, **CTRL F** | Moves to the next character to the right of the cursor. |
| **CTRL Right-Arrow**, **ALT F** | Jumps to the next word to the right of the cursor. |
| **Backspace**, **CTRL H** | Deletes the character to the left of the cursor. |
| **ALT D** | Deletes the word to the right of the cursor (if the cursor is located at the word start). |
| **CTRL ALT H** | Deletes the word to the left of the cursor (if the cursor is located at the word end). |
| **CTRL U** | Deletes the current syntax completely. |
| **CTRL N** | Shows the commands in the history list - from the current position down the list (to the most recent command).<br>Each time you press these keys, it shows another previous command down the list. |
| **CTRL P** | Shows the commands in the history list - from the current position up the list (to the oldest command).<br>Each time you press these keys, it shows another previous command up the list. |

| Keys | Action |
|---|---|
| **CTRL R** | Searches in the history list for the string you enter and shows the matching command. |

# Configuration Lock in Gaia Clish

Only one user can have Read/Write access to Gaia configuration database at a time. All other users can log in with Read-Only access to see configuration settings, as specified by their assigned roles in Gaia OS (see *"Roles" on page 480*).

When you log in and no other user has Read/Write access, you get an exclusive configuration lock with Read/Write access. If a different user already has the configuration lock, you have the option to override their lock.

If you:

- Override the lock, then the other user stays logged in with Read-Only access.
- Do not override the lock, then you cannot modify the settings.

**The "lock database" and "lock database" commands**

### Description

Use the "`lock database override`" and "`unlock database`" commands to get exclusive read-write access to the Gaia database by taking write privileges away from other administrators logged into the system.

### Syntax

| |
|---|
| `lock database override` |
| `unlock database` |

### Comments

- Use these commands with caution.

  The administrator, whose write access is revoked, does not receive a notification.
- The "`lock database override`" command is identical to the "`set config-lock on override`" command.
- The "`unlock database`" command is identical to the "`set config-lock off`" command.

### The "config-lock" commands

#### Description

Configures and shows the state of the configuration lock on Gaia configuration database.

#### Syntax

```
set config-lock
      off
      on [timeout <5-900>] override
```

```
show
      config-lock
      config-state
```

#### Parameters

| Parameter | Description |
|---|---|
| `off` | Turns off the configuration lock. |
| `on` | Turns on the configuration lock.<br>The default timeout value is 300 seconds. |
| `timeout <5-900>` | Optional parameter.<br>Turns on the configuration lock for the specified interval in seconds. |

#### Comments

- The "`set config-lock on override`" command is identical to the "`lock database override`" command.
- The "`set config-lock off`" command is identical to the "`unlock database`" command.

# Environment Commands

### Description

Use these commands to set the Gaia Clish environment for a user for a particular session, or permanently.

### Syntax

#### Viewing the client environment

```
show clienv
      all
      config-lock
      debug
      echo-cmd
      on-failure
      output
      prompt
      rows
      syntax-check
```

#### Configuring the client environment

```
set clienv
      config-lock {on | off}
      debug {0-6}
      echo-cmd {on | off}
      on-failure {continue | stop}
      output {pretty | structured | xml}
      prompt <Prompt String>
      rows <Number of Rows>
      syntax-check {on | off}
```

#### Saving the client environment configuration permanently

```
save clienv
```

**Parameters**

| Parameter | Description |
|---|---|
| `config-lock {on \| off}` | Default value of the Clish `config-lock` parameter.<br>If set to `on`, Gaia Clish locks the configuration when invoked. Otherwise, it continues without a configuration lock.<br>When the configuration is locked by Gaia Clish, no configuration changes are possible in Gaia Portal, until the lock is released. |
| `debug {0-6}` | Debug level.<br>Predefined levels are:<br>■ `0` - (Default) Do not debug, display error messages only<br>■ `5` - Show the `confd` daemon requests and responses<br>■ `6` - Show handler invocation parameters and results |
| `echo-cmd {on \| off}` | If set to `on`, echoes all commands before executing them, when the command execution is done through the "`load configuration`" command.<br>The default is `off`. |
| `on-failure {continue \| stop}` | Action performed on failure:<br>■ `continue` - Show error messages, but continue running commands from a file or a script<br>■ `stop` - (Default) Stop running commands from a file or a script |
| `output {pretty \| structured \| xml}` | Command line output format.<br>The default is `pretty`.<br>See *"Client Environment Output Format" on page 51*. |
| `prompt <Prompt String>` | Command prompt string.<br>A valid prompt string can consist of any printable characters and a combination of these variables:<br>■ `%H` - Replaced with the Command number<br>■ `%I` - Replaced with the User ID<br>■ `%M` - Replaced with the Hostname<br>■ `%P` - Replaced with the Product ID<br>■ `%U` - Replaced with the Username<br>To set the prompt back to the default, use the keyword `default`. |
| `rows <Number of Rows>` | Number of rows to show in your terminal window.<br>If the window size is changed, the number of rows also changes, unless the value is set to 0 (zero). |

| Parameter | Description |
|---|---|
| `syntax-check {on \| off}` | Put the shell into syntax-check mode.<br>Commands you enter are checked syntactically and are not executed, but values are validated.<br>The default is `off`. |

# Client Environment Output Format

Gaia Clish supports these output formats:

**Pretty**

Output is formatted to be clear.

For example, output of the command "`show user admin`" in pretty mode would look like this:

```
gaia> set clienv output pretty

gaia> show user admin
Uid Gid Home Dir. Shell Real Name Privileges
0 0 /home/admin /bin/cli.sh Admin Admin-like shell
gaia>
```

**Structured**

Output is delimited by semi-colons.

For example, output of the command "`show user admin`" in structured mode would look like this:

```
gaia> set clienv output structured

gaia> show user admin
Uid;Gid;Home Dir.;Shell;Real Name;Privileges;
0;0;/home/admin;/bin/bash;Admin;Admin-like shell;
gaia>
```

### XML

Adds XML tags to the output.

For example, output of the command "`show user admin`" in XML mode would look like this:

```
gaia> set clienv output xml

gaia> show user admin
<?xml version="1.0"?>
  <CMDRESPONSE>
  <CMDTEXT>show user admin</CMDTEXT>
  <RESPONSE><System_User>
    <Row>
      <Uid>0</Uid>
      <Gid>0</Gid>
      <Home_Dir.>/home/admin</Home_Dir.>
      <Shell>/bin/bash</Shell>
      <Real_Name>Admin</Real_Name>
      <Privileges>Admin-like shell</Privileges>
    </Row>
    </System_User>
  </RESPONSE>
  </CMDRESPONSE>
gaia>
```

# Expert Mode

**Important** - On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in the Expert mode on the applicable Security Group.

The default Gaia shell is called `clish`.

Gaia Clish is a restrictive shell (role-based administration controls the number of commands available in the shell).

While the use of Gaia Clish is encouraged for security reasons, Gaia Clish does not give access to low level system functions.

For low-level configuration, use the more permissive Expert mode shell. In addition, see sk144112.

- To enter the Expert shell, run in Gaia Clish: `expert`
- To exit from the Expert shell and go back to Gaia Clish, run: `exit`

For instructions to configure the Expert mode password, see *"System Passwords" on page 300*.

**Notes**:

- If a command is supported in Gaia Clish, it is **not** supported to run the corresponding command in Expert mode.
  For example, to work with interfaces, Gaia Clish provides the commands "`show interface`" and "`set interface`".
  Therefore, it is **not** supported to run the `ifconfig` command in the Expert mode.
- Expert mode does not provide more privileges, only more configuration abilities.
- Expert mode is not a security feature. Rather, it offers protection against mistakes.
- Refer to sk181230 to receive audit logs for the Expert mode login on Gaia servers.
- Gaia writes a log message about the Expert mode login to the `/var/log/messages` file:
  - For a local login:

    ```
    Console connection by <username> user to Expert Shell at <Time Date>
    ```

  - For an SSH login:

    ```
    SSH connection by <username> user to Expert Shell with client IP <IP Address> at <Time Date>
    ```

  These Gaia Clish commands are available to work with this feature:
  - To see the current state of this feature:

    ```
    show audit login-notifier
    ```

  - To enable this feature (this is the default):

    ```
    set audit login-notifier on
    ```

  - To disable this feature:

    ```
    set audit login-notifier off
    ```

# User Defined (Extended) Commands

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

### Description

Manage user defined (extended) commands in Gaia Clish.

Extended commands include:

1. Built in extended commands.

   These are mostly intended to configure and troubleshoot Gaia and Check Point products.

2. User defined commands.

You can do role-based administration (RBA) with extended commands:

1. Assign extended commands to roles.
2. Assign the roles to users or user groups.

### Syntax

- To show all extended commands:

  ```
  show extended commands
  ```

- To show the path and description of a specified extended command:

  ```
  show command <Command>
  ```

- To add an extended command:

  ```
  add command <Command> path <Path> description "<Text>"
  ```

- To delete an extended command:

  ```
  delete command <Command>
  ```

**Parameters**

| Parameter | Description |
|---|---|
| *<Command>* | Name of the extended command |
| *<Path>* | Path of the extended command |
| "*<Text>*" | Description of the extended command (must enclose in double quotes) |

See *"List of Available Extended Commands in Roles" on page 511*.

**Example**

To add the *free* command to the *systemDiagnosis* role and assign that role to the user *john*:

| Step | Instructions |
|---|---|
| 1 | To add the *free* command:<br>`gaia> add command free path /usr/bin/free description "Display amount of free and used memory in the system"` |
| 2 | Save the configuration:<br>`gaia> save config` |
| 3 | Log out of Gaia. |
| 4 | Log in to Gaia again. |
| 5 | To add the *free* command to the *systemDiagnosis* role:<br>`gaia> add rba role systemDiagnosis domain-type System readwrite-features ext_free` |
| 6 | To assign the *systemDiagnosis* role to the user *john*:<br>`gaia> add rba user john roles systemDiagnosis` |
| 7 | Save the configuration:<br>`gaia> save config` |

# Summary of Gaia Clish Commands

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

This section shows the list of commands available in Gaia Clish.

**To show the list of all available Gaia Clish commands:**

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on your Gaia system. |
| 2 | Log in to Gaia Clish. |
| 3 | Press the <TAB> key on the keyboard. |

**To show the list of available Gaia Clish '`show`' commands:**

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on your Gaia system. |
| 2 | Log in to Gaia Clish. |
| 3 | Type:<br>`show` |
| 4 | Press the <SPACE> key and then the <TAB> key on the keyboard. |

**To show the list of available Gaia Clish '`add`' commands:**

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on your Gaia system. |
| 2 | Log in to Gaia Clish. |
| 3 | Type:<br>`add` |
| 4 | Press the <SPACE> key and then the <TAB> key on the keyboard. |

**To show the list of available Gaia Clish '`set`' commands:**

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on your Gaia system. |
| 2 | Log in to Gaia Clish. |
| 3 | Type:<br>`set` |
| 4 | Press the <SPACE> key and then the <TAB> key on the keyboard. |

**To show the list of available Gaia Clish '`delete`' commands:**

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on your Gaia system. |
| 2 | Log in to Gaia Clish. |
| 3 | Type:<br>`delete` |
| 4 | Press the <SPACE> key and then the <TAB> key on the keyboard. |

# Configuring Gaia for the First Time

After you install Gaia for the first time, use the First Time Configuration Wizard to configure the system and the Check Point products on it.

You can run the First Time Configuration Wizard in:

- Gaia Portal
- CLI Expert mode

# Running the First Time Configuration Wizard in Gaia Portal

**To start the Gaia First Time Configuration Wizard:**

| Step | Instructions |
|---|---|
| 1 | Connect a computer to the Gaia computer.<br>On Scalable Platforms, connect a computer to the Gaia Management Interface of the Security Group.<br>You must connect to the interface you configured during the Gaia installation (for example, **eth0**). |
| 2 | On your connected computer, configure a static IPv4 address in the same subnet as the IPv4 address you configured during the Gaia installation. |
| 3 | On your connected computer, in a web browser, connect to the IPv4 address you configured during the Gaia installation:<br>`https://<IP address of Gaia Management Interface>` |
| 4 | Enter the default username and password: `admin` and `admin`. |
| 5 | Click **Login**.<br>The Check Point **First Time Configuration Wizard** opens. |
| 6 | Follow the instructions on the First Time Configuration Wizard windows.<br>See the applicable chapters below for installing specific Check Point products. |

Below you can find the description of the First Time Configuration Wizard windows and their fields.

**Note** - Different windows and fields appear for different products and hardware.

### "Deployment Options" window

In this window, you select how to deploy Gaia Operating System.

| Section | Options | Description |
|---|---|---|
| **Setup** | **Continue with R82 configuration** | Use this option to configure the installed Gaia and Check Point products. |
| **Installation** | **Install from Check Point Cloud**<br>**Install from USB device** | Use these options to install a Gaia version. |
| **Recovery** | **Import existing snapshot** | Use this option to import an existing Gaia snapshot. |

If in the **Deployment Options** window, you selected **Install from Check Point Cloud**, the First Time Configuration Wizard asks you to configure the connection to Check Point Cloud. These options appear (applies only to Check Point appliances that you configured as a Security Gateway):

- **Install major version** - This option chooses and installs major versions available on Check Point Cloud. The Gaia CPUSE performs the installation.
- **Pull appliance configuration** - This option applies the initial deployment configuration that includes different OS version on the appliance. You must prepare the initial deployment configuration with the Zero Touch Cloud Service. For more information, see sk116375.

  **Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature.

### "Authentication Details" window

In this window, you configure the main passwords for the Gaia OS.

| Section | Description |
|---|---|
| **Change the default administrator password** | Configures the password for the Expert mode. |
| **Change the default password for Gaia maintenance mode** | Configures the password for the Maintenance Mode (GRUB).<br>This GRUB password protects the GRUB menu and GRUB terminal.<br>Gaia asks for this password when you boot into the Maintenance Mode and when you revert Gaia snapshots. |

**Note** - You can change each password after you complete the Gaia First Time Configuration Wizard. See *"System Passwords" on page 300*.

**Best Practice** - For security reasons, we recommend to configure a different passwords for the Expert mode and for the Maintenance Mode.

### "Management Connection" window

In this window, you select and configure the main Gaia Management Interface.

You connect to this IP address to open the Gaia Portal or CLI session.

| Field | Description |
|---|---|
| **Interface** | By default, First Time Configuration Wizard selects the interface you configured during the Gaia installation (for example, **eth0**).<br>**Note** - After you complete the First Time Configuration Wizard and reboot, you can select another interface as the main Gaia Management Interface and configure its IP settings. |
| **Configure IPv4** | Select how the Gaia Management Interface gets its IPv4 address:<br>■ **Manually** - You configure the IPv4 settings in the next fields.<br>■ **Off** - None. |
| **IPv4 address** | Enter the applicable IPv4 address. |
| **Subnet mask** | Enter the applicable IPv4 subnet mask. |
| **Default Gateway** | Enter the IPv4 address of the applicable default gateway. |
| **Configure IPv6** | Select how the Gaia Management Interface gets its IPv6 address:<br>■ **Manually** - You configure the IPv6 settings in the next fields.<br>■ **Off** - None. |
| **IPv6 Address** | Enter the applicable IPv6 address.<br>**Important** - R82 does **not** support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313). |
| **Mask Length** | Enter the applicable IPv6 mask length. |
| **Default Gateway** | Enter the IPv6 address of the applicable default gateway. |

"Internet Connection" window

**Optional:** In this window, you can configure the interface that connects the Gaia server to the Internet.

| Field | Description |
|---|---|
| **Interface** | Select the applicable interface. |
| **Configure IPv4** | Select how the applicable interface gets its IPv4 address:<br>■ **Manually** - You configure the IPv4 settings in the next fields.<br>■ **Off** - None. |
| **IPv4 address** | Enter the applicable IPv4 address. |
| **Subnet mask** | Enter the applicable IPv4 subnet mask. |
| **Default Gateway** | Enter the IPv4 address of the applicable default gateway. |
| **Configure IPv6** | **Optional:** Select how the applicable interface gets its IPv6 address:<br>■ **Manually** - You configure the IPv6 settings in the next fields.<br>■ **Off** - None. |
| **IPv6 Address** | Enter the applicable IPv6 address. |
| **Mask Length** | Enter the applicable IPv6 mask length. |
| **Default Gateway** | Enter the IPv6 address of the applicable default gateway. |

### "Device Information" window

In this window, you configure the Host name, the DNS servers, and the Proxy server for Gaia.

| Field | Description |
|---|---|
| **Host Name** | Enter the applicable distinct host name. |
| **Domain Name** | Optional: Enter the applicable domain name. |
| **Primary DNS Server** | Enter the applicable IPv4 address of the primary DNS server. |
| **Secondary DNS Server** | Optional: Enter the applicable IPv4 address of the secondary DNS server. |
| **Tertiary DNS Server** | Optional: Enter the applicable IPv4 address of the tertiary DNS server. |
| **Use a Proxy server** | Optional: Select this option to configure the applicable Proxy server. |
| **Address** | Enter the applicable IPv4 address or resolvable hostname of the Proxy server. |
| **Port** | Enter the port number for the Proxy server. |

### "Date and Time Settings" window

In this window, you configure the date and time settings for Gaia.

| Field | Description |
|---|---|
| **Set time manually** | Select this option to configure the date and time settings manually. |
| **Date** | Select the correct date. |
| **Time** | Select the correct time. |
| **Time Zone** | Select the correct time zone. |
| **Use Network Time Protocol (NTP)** | Select this option to configure the date and time settings automatically with NTP. |
| **Primary NTP server** | Enter the applicable IPv4 address or resolvable hostname of the primary NTP server. |
| **Version** | Select the version of the NTP for the primary NTP server. |
| **Secondary NTP server** | Optional: Enter the applicable IPv4 address or resolvable hostname of the secondary NTP server. |
| **Version** | Select the version of the NTP for the secondary NTP server. |
| **Time Zone** | Select the correct time zone. |

**"Installation Type" window**

In this window, you select which type of Check Point products you wish to install on the Gaia computer.

| Field | Description |
|---|---|
| **Security Gateway and/or Security Management** | Select this option to install:<br>■ A Single Security Gateway.<br>**Important** - Scalable Platforms (ElasticXL, Maestro, and Scalable Chassis) support **only** this option.<br>■ A Cluster Member.<br>■ A Security Management Server, including Management High Availability.<br>■ An Endpoint Security Management Server.<br>■ An Endpoint Policy Server.<br>■ CloudGuard Controller.<br>■ A dedicated single Log Server.<br>■ A dedicated single SmartEvent Server.<br>■ A Standalone. |
| **Multi-Domain Server** | Select this option to install:<br>■ A Multi-Domain Server, including Management High Availability.<br>■ A dedicated single Multi-Domain Log Server.<br>**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature. |

**"Products" window**

In this window, you continue to select which type of Check Point products you wish to install on the Gaia computer.

- If in the **Installation Type** window, you selected **Security Gateway and/or Security Management**, these options appear:

| Field | Description |
|---|---|
| **Security Gateway** | Select this option to install:<br>• A single Security Gateway.<br>**Important** - Scalable Platforms (ElasticXL, Maestro, and Scalable Chassis) support **only** this option.<br>• A Cluster Member.<br>• A Standalone. |
| **Security Management** | Select this option to install:<br>• A Security Management Server, including Management High Availability.<br>• An Endpoint Security Management Server.<br>• An Endpoint Policy Server.<br>• A CloudGuard Controller.<br>• A dedicated single Log Server.<br>• A dedicated single SmartEvent Server.<br>• A Standalone.<br>**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature |
| **Unit is a part of a cluster** | This option is available only if you selected **Security Gateway**.<br>Select this option to install a cluster of dedicated Security Gateways, or a Full High Availability Cluster.<br>Select the cluster type:<br>• **ElasticXL** - For a cluster of dedicated Security Gateways based on the HyperScale technology.<br>• **ClusterXL** - For a cluster of dedicated Security Gateways, or a Full High Availability Cluster.<br>• **VRRP Cluster** - For a VRRP Cluster on Gaia.<br>**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature. |

| Field | Description |
|---|---|
| **Define Security Management as** | Select **Primary** to install:<br>• A Security Management Server.<br>• An Endpoint Security Management Server.<br>• An Endpoint Policy Server.<br>• A CloudGuard Controller.<br>Select **Secondary** to install:<br>• A Secondary Management Server in Management High Availability.<br>Select **Log Server / SmartEvent only** to install:<br>• A dedicated single Log Server.<br>• A dedicated single SmartEvent Server.<br>**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature. |
| **Install as VSNext** | Select to configure this ElasticXL Cluster in the VSNext mode.<br>You **cannot** convert to the VSNext mode after the installation.<br>See the *R82 VSX Administration Guide*.<br>**Important:**<br>• Only ElasticXL supports this option.<br>• To install a Security Gateway in the Legacy VSX mode:<br>1. Do **not** select this checkbox.<br>2. In SmartConsole, configure a VSX Gateway and the required Virtual System and Virtual Switch objects. |

- If in the **Installation Type** window, you selected **Multi-Domain Server**, these options appear:

| Field | Description |
|---|---|
| **Primary Multi-Domain Server** | Select this option to install a Primary Multi-Domain Server in Management High Availability. |
| **Secondary Multi-Domain Server** | Select this option to install a Secondary Multi-Domain Server in Management High Availability. |
| **Multi-Domain Log Server** | Select this option to install a dedicated single Multi-Domain Log Server. |

**Note** - By default, the option **Automatically download Blade Contracts, new software, and other important data** is enabled. See sk111080.

### "Dynamically Assigned IP" window

This window appears if in the **Products** window, you selected only the **Security Gateway** option.

In this window, you select if this Security Gateway gets its IP address dynamically (DAIP gateway).

| Field | Description |
|---|---|
| **Yes** | Select this option, if this Security Gateway gets its IP address dynamically (DAIP gateway).<br>**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246). |
| **No** | Select this option, if you wish to configure this Security Gateway with a static IP address. |

### "Secure Communication to Management Server" window

This window appears only if:

- In the **Installation Type** window, you selected the **Security Gateway and/or Security Management** option and in the **Products** window, you selected only the **Security Gateway** option (and optionally, **Unit is a part of a cluster** option)
- In the **Installation Type** window, you selected the **Multi-Domain Server** option and the **Secondary Multi-Domain Server** or the **Multi-Domain Log Server** option.

In this window, you configure a one-time Activation Key.

You must enter this key later in SmartConsole when you create the corresponding object and initialize SIC.

| Field | Description |
|---|---|
| **Activation Key** | Enter one-time activation key (between 4 and 127 characters long). |
| **Confirm Activation Key** | Enter the same one-time activation key again. |
| **Connect to your Management as a Service** | This option is available only if in the **Products** window you selected the **Security Gateway** option.<br>Select this option if you wish to manage this Security Gateway from the Quantum Smart-1 Cloud service in Infinity Portal. |
| **Authentication token** | Enter the token you generated in the Quantum Smart-1 Cloud service.<br>See the *Quantum Smart-1 Cloud Administration Guide*. |

### "Security Management Administrator" window

This window appears only if in the **Installation Type** window, you selected the **Security Gateway and/or Security Management** option and in the **Products** window, you selected only the **Security Management** option (and optionally, other options).

In this window, you configure the main Security Management Administrator to log in to SmartConsole.

| Field | Description |
|---|---|
| **Use Gaia administrator: admin** | Configures the username **admin**. |
| **Define a new administrator** | Configures the user-defined username. |

### "Security Management GUI Clients" window

In this window, you configure which computers are allowed to connect with SmartConsole to this Security Management Server.

| Field | Description |
|---|---|
| **Any IP Address** | Select this option to allow all computers to connect. |
| **This machine** | Select this option to allow only a specific computer to connect.<br>By default, the First Time Configuration Wizard uses the IPv4 address of your computer.<br>You can change it to another IP address. |
| **Network** | Select this option to allow an entire IPv4 subnet of computers to connect.<br>Enter the applicable subnet IPv4 address and subnet mask. |
| **Range of IPv4 addresses** | Select this option to allow a specific range of IPv4 addresses to connect.<br>Enter the applicable start and end IPv4 addresses. |

### "Leading VIP Interfaces Configuration" window

This window appears only if in the **Installation Type** window, you selected the **Multi-Domain Server** option.

In this window, you select the main Leading VIP Interface on this Multi-Domain Server or Multi-Domain Log Server.

| Field | Description |
|---|---|
| **Select leading interface** | Select the applicable interface. |

### "Multi-Domain Server GUI Clients" window

This window appears only if in the **Installation Type** window, you selected the **Multi-Domain Server** option and the **Primary Multi-Domain Server** option.

In this window, you configure which computers are allowed to connect with SmartConsole to this Multi-Domain Server.

| Field | Description |
|---|---|
| **Any host** | Select this option to allow all computers to connect. |
| **IP address** | Select this option to allow only a specific computer to connect.<br>By default, the First Time Configuration Wizard uses the IPv4 address of your computer.<br>You can change it to another IP address. |

### "First Time Configuration Wizard Summary" window

In this window, you can see the installation options you selected.

The links at the bottom of this window:

- **End-user License Agreement and Privacy Policy**
- **Update and Data Sharing Settings**

  For information about these settings, see sk175504.

| Field | Description |
|---|---|
| **Automatically download and install Software Blade Contracts, security updates and other important data (highly recommended)** | Controls the download of "Security" data from online Check Point servers:<br>• Allows to update the installed Check Point products that are defined as "Security". For example, CPUSE Deployment Agent, Threat Emulation Engine.<br>• Allows to download data that is defined as "Security". For example, signatures for the IPS Software Blade. |
| **Automatically download software updates and new features (highly recommended)** | Controls the download of "Non-Security" data from online Check Point servers:<br>• Allows to update the installed Check Point products that are defined as "Non-Security". For example, updates for the CPinfo tool.<br>• Allows to download data that is defined as "Non-Security". |

| Field | Description |
|---|---|
| **Help Check Point improve the product by sending anonymous information** | Controls the upload of anonymous data to online Check Point servers:<br>• Allows to upload anonymous logs.<br>For example, the upload of logs from the CPUSE tool.<br>• Allows to upload anonymous diagnostics information.<br>For example, the upload of data from the CPinfo and CPUSE tools.<br>Check Point uses this data internally for bug analysis and to improve the products.<br>All data is subject to the European privacy policy (GDPR). |
| **I approve sharing core dump files and other relevant crash data which might contain personal information** | If you enable this option, Gaia operating system uploads the detected core dump files to Check Point Cloud.<br>Check Point R&D can analyze the crashes and issue fixes for them.<br>See *"Crash Data" on page 394*.<br>**Warning** - Because core dump files contain a snapshot of the memory, they can contain personal and sensitive information. |

**Notes:**

- At the end of the First Time Configuration Wizard, the Gaia computer reboots and the initialization process is performed in the background for several minutes.
- If you installed the Gaia computer as a Security Management Server or Multi-Domain Server, only read-only access is possible with SmartConsole during this initialization time.
- To make sure the configuration is finished:

1. Connect to the command line on the Gaia computer.
2. Log in to the Expert mode.
3. Check that the bottom section of the `/var/log/ftw_install.log` file contains one of these sentences:

   - `installation succeeded`
   - `FTW: Complete`

   Run:

   ```
   cat /var/log/ftw_install.log | egrep --color
   "installation succeeded|FTW: Complete"
   ```

Example outputs:

- From a Security Gateway or Cluster Member:

```
[Expert@GW:0]# cat /var/log/ftw_install.log | egrep
--color "installation succeeded|FTW: Complete"
Dec 06, 19 19:19:51 FTW: Complete
[Expert@GW:0]#
```

- From a Security Management Server or a Standalone:

```
[Expert@SA:0]# cat /var/log/ftw_install.log | egrep
--color "installation succeeded|FTW: Complete"
Dec 06, 2019 03:48:38 PM installation succeeded.
06/12/19 15:48:39 FTW: Complete
[Expert@SA:0]#
```

- From a Multi-Domain Server:

```
[Expert@MDS:0]# cat /var/log/ftw_install.log |
egrep --color "installation succeeded|FTW:
Complete"
Dec 06, 2019 07:43:15 PM installation succeeded.
[Expert@MDS:0]#
```

- From a Scalable Platform Security Group:

```
[Expert@HostName-ch0x-0x:0]# g_cat /var/log/ftw_
install.log | egrep --color "installation
succeeded|FTW: Complete"
Dec 06, 19 19:19:51 FTW: Complete
[Expert@HostName-ch0x-0x:0]#
```

# Running the First Time Configuration Wizard in CLI Expert mode

### Description

Use this command in the Expert mode to test and to run the First Time Configuration Wizard on a Gaia system for the first time after the system installation.

**Notes:**

- The `config_system` utility is **not** an interactive configuration tool. It helps automate the first time configuration process.
- The `config_system` utility is only for the first time configuration, and **not** for ongoing system configurations.

**Important** - On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in the Expert mode on the applicable Security Group.

### Syntax

#### Viewing the configurable parameters

| Form | Command |
|---|---|
| Short form | `config_system -l` |
| Long form | `config_system --list-params` |

#### Running the First Time Configuration Wizard from a specified configuration file

| Form | Command |
|---|---|
| Short form | `config_system -f <Path and Filename>` |
| Long form | `config_system --config-file <Path and Filename>` |

#### Running the First Time Configuration Wizard from a specified configuration string

| Form | Command |
|---|---|
| Short form | `config_system -s <String>` |
| Long form | `config_system --config-string <String>` |

### Creating a First Time Configuration Wizard configuration file template in a specified path

| Form | Command |
|---|---|
| Short form | `config_system -t <Path>` |
| Long form | `config_system --create-template <Path>` |

### Making sure the First Time Configuration Wizard configuration file is valid

```
config_system --dry-run
```

## Procedure

### Running the First Time Configuration Wizard from a configuration string

| Step | Instructions |
|---|---|
| 1 | Run this command in Expert mode:<br>`config_system --config-string <String of Parameters and Values>`<br>A configuration string must consist of *parameter=value* pairs, separated by the ampersand (&).<br>You must enclose the whole string between quotation marks.<br>For example:<br>`"hostname=myhost&domainname=somedomain.com&timezone='America/Indiana/Indianapolis'&ftw_sic_key=aaaa&install_security_gw=true&gateway_daip=false&install_ppak=true&gateway_cluster_member=true&install_security_managment=false"`<br>For more information on valid parameters and values, run the "`config_system --list-params`" command. |
| 2 | Reboot the system. |

### Creating a configuration file

| Step | Instructions |
|---|---|
| 1 | Run this command in the Expert mode:<br>`config_system -t <File Name>` |

| Step | Instructions |
|---|---|
| 2 | Open the file you created in a text editor. |
| 3 | Edit all parameter values as necessary. |
| 4 | Save the updated configuration file. |

**Making sure the First Time Configuration Wizard configuration file is valid**

Run this command in Expert mode:

```
config_system --config-file <File Name> --dry-run
```

**Running the First Time Configuration Wizard from a configuration file**

| Step | Instructions |
|---|---|
| 1 | Run this command in Expert mode:<br>`config_system -f <File Name>` |
| 2 | Reboot the system. |

If you do not have a configuration file, you can create a configuration template and fill in the parameter values as necessary.

Before you run the First Time Configuration Wizard, you can validate the configuration file you created.

### Parameters

A configuration file contains the "`<parameter>=<value>`" pairs described in the table below.

**Note** - The `config_system` parameters can change from Gaia version to Gaia version. Run the "`config_system --list-params`" command to see the available parameters.

Table: The 'config_system' parameters

| Parameter | Supports Scalable Platforms? | Description | Valid values |
|---|---|---|---|
| `admin_hash` | – | Configures the administrator's password. | A string of alphanumeric characters, enclosed between single quotation marks. |
| `default_gw_v4` | – | Specifies IPv4 address of the default gateway. | Single IPv4 address. |
| `default_gw_v6` | – | Specifies IPv6 address of the default gateway. | Single IPv6 address. |
| `domainname` | – | Configures the domain name (optional). | Fully qualified domain name. Example: `somedomain.com` |
| `download_info` | ✓ | If its value is set to "`true`":<br>■ Downloads and installs Check Point Software Blade contracts.<br>■ Downloads and installs Check Point security updates.<br>■ Downloads other important information.<br>For more information, see sk94508 and sk175504.<br>**Best Practice** - We highly recommended you enable this optional parameter. | ■ `true` (default)<br>■ `false` |

Table: The 'config_system' parameters (continued)

| Parameter | Supports Scalable Platforms? | Description | Valid values |
|---|---|---|---|
| `download_from_checkpoint_non_security` | ✓ | If its value is set to "`true`":<br>■ Downloads Check Point software updates.<br>■ Downloads new Check Point features.<br>For more information, see sk94508 and sk175504.<br>**Best Practice** - We highly recommended you enable this optional parameter. | ■ `true` (default)<br>■ `false` |
| `ftw_sic_key` | ✓ | Configures the Secure Internal Communication key, if the value of the "`install_security_managment`" parameter is set to "`false`". | A string of alphanumeric characters (between 4 and 127 characters long). |
| `gateway_cluster_member` | – | Configures the Security Gateway as member of ClusterXL, if its value is set to "`true`". | ■ `true`<br>■ `false` |
| `gateway_daip` | – | Configures the Security Gateway as Dynamic IP (DAIP) Security Gateway, if its value is set to "`true`". | ■ `true`<br>■ `false` (default)<br>**Note** - Must be set to "`false`", if ClusterXL or Security Management Server is enabled. |
| `hostname` | ✓ | Configures the name of the local host (optional). | A string of alphanumeric characters. |

Table: The 'config_system' parameters (continued)

| Parameter | Supports Scalable Platforms? | Description | Valid values |
|---|---|---|---|
| `iface` | – | Interface name (optional). | Name of the interface exactly as it appears in the device configuration. Examples: `eth0`, `eth1` |
| `install_mds_interface` | – | Specifies Multi-Domain Server management interface. | Name of the interface exactly as it appears in the device configuration. Examples: `eth0`, `eth1` |
| `install_mds_primary` | – | Makes the installed Security Management Server the Primary Multi-Domain Server.<br>**Note** - The value of the "`install_security_managment`" parameter must be set to "`true`". | ▪ `true`<br>▪ `false`<br>**Note** - Can only be set to "`true`", if the value of the "`install_mds_secondary`" parameter is set to "`false`". |
| `install_mds_secondary` | – | Makes the installed Security Management Server a Secondary Multi-Domain Server.<br>**Note** - The value of the "`install_security_managment`" parameter must be set to "`true`". | ▪ `true`<br>▪ `false`<br>**Note** - Can only be set to "`true`", if the value of the "`install_mds_primary`" parameter is set to "`false`". |

Table: The 'config_system' parameters (continued)

| Parameter | Supports Scalable Platforms? | Description | Valid values |
|---|---|---|---|
| `install_mgmt_primary` | – | Makes the installed Security Management Server the Primary one.<br>**Notes**:<br>■ Can only be set to "`true`", if the value of the "`install_mgmt_secondary`" parameter is set to "`false`".<br>■ To install a dedicated Log Server, the value of this parameter must be set to "`false`". | ■ `true`<br>■ `false` |
| `install_mgmt_secondary` | – | Makes the installed Security Management Server a Secondary one.<br>**Notes**:<br>■ Can only be set to "`true`", if the value of the "`install_mgmt_primary`" parameter is set to "`false`".<br>■ To install a dedicated Log Server, the value of this parameter must be set to "`false`". | ■ `true`<br>■ `false` |

Table: The 'config_system' parameters (continued)

| Parameter | Supports Scalable Platforms? | Description | Valid values |
|---|---|---|---|
| `install_mlm` | – | Installs Multi-Domain Log Server, if its value is set to "`true`". | ■ `true`<br>■ `false` |
| `install_security_gw` | – | Installs Security Gateway, if its value is set to "`true`". | ■ `true`<br>■ `false` |
| `install_security_managment` | – | Installs a Security Management Server or a dedicated Log Server, if its value is set to "`true`". | ■ `true`<br>■ `false` |
| `install_security_vsx` | ✓ | Installs VSX Gateway, if its value is set to "`true`". | ■ `true`<br>■ `false` |
| `ipaddr_v4` | – | Configures the IPv4 address of the management interface. | Single IPv4 address. |
| `ipaddr_v6` | – | Configures the IPv6 address of the management interface. | Single IPv6 address. |
| `ipstat_v4` | – | Turns on static IPv4 configuration, if its value is set to "`manually`". | ■ `manually` (default)<br>■ `off` |
| `ipstat_v6` | – | Turns static IPv6 configuration on, if its value is set to "`manually`". | ■ `manually`<br>■ `off` (default) |
| `maas_authentication_key` | – | Configures the authentication key for Management as a Service (MaaS). Applies only to Security Gateways. | A string of alphanumeric characters, enclosed between single quotation marks. |
| `masklen_v4` | – | Configures the IPv4 mask length for the management interface. | A number from 0 to 32. |

Table: The 'config_system' parameters (continued)

| Parameter | Supports Scalable Platforms? | Description | Valid values |
|---|---|---|---|
| `masklen_v6` | – | Configures the IPv6 mask length for the management interface. | A number from 0 to 128. |
| `mgmt_admin_name` | – | Configures the management administrator's username.<br>**Note** - You must specify this parameter, if the value of the "`install_security_managment`" parameter is set to "`true`". | A string of alphanumeric characters. |
| `mgmt_admin_passwd` | – | Configures the management administrator's password.<br>**Note** - You must specify this parameter, if the value of the "`install_security_managment`" parameter is set to "`true`". | A string of alphanumeric characters. |

Table: The 'config_system' parameters (continued)

| Parameter | Supports Scalable Platforms? | Description | Valid values |
|---|---|---|---|
| `mgmt_admin_radio` | – | Configures Management Server administrator.<br>**Note** - You must specify this parameter, if you install a Management Server. | ▪ Set the value to "`gaia_admin`", if you wish to use the Gaia "`admin`" account.<br>▪ Set the value to "`new_admin`", if you wish to configure a new administrator account. |
| `mgmt_gui_clients_first_ip_field` | – | Specifies the first address of the range, if the value of the "`mgmt_gui_clients_radio`" parameter is set to "`range`". | Single IPv4 address of a host.<br>Example: `192.168.0.10` |
| `mgmt_gui_clients_hostname` | – | Specifies the netmask, if value of the "`mgmt_gui_clients_radio`" parameter is set to "`this`". | Single IPv4 address of a host.<br>Example: `192.168.0.15` |
| `mgmt_gui_clients_ip_field` | – | Specifies the network address, if the value of the "`mgmt_gui_clients_radio`" parameter is set to "`network`". | IPv4 address of a network.<br>Example: `192.168.0.0` |
| `mgmt_gui_clients_last_ip_field` | – | Specifies the last address of the range, if the value of the "`mgmt_gui_clients_radio`" parameter is set to "`range`". | Single IPv4 address of a host.<br>Example: `192.168.0.20` |

Table: The 'config_system' parameters (continued)

| Parameter | Supports Scalable Platforms? | Description | Valid values |
|---|---|---|---|
| `mgmt_gui_clients_radio` | – | Specifies SmartConsole clients that can connect to the Security Management Server. | ■ `any`<br>■ `range`<br>■ `network`<br>■ `this` |
| `mgmt_gui_clients_subnet_field` | – | Specifies the netmask, if the value of the "`mgmt_gui_clients_radio`" parameter is set to "`network`". | A number from 1 to 32. |
| `ntp_primary` | – | Configures the IP address of the primary NTP server (optional). | IPv4 address. |
| `ntp_primary_version` | – | Configures the NTP version of the primary NTP server (optional). | ■ `1`<br>■ `2`<br>■ `3`<br>■ `4` |
| `ntp_secondary` | – | Configures the IP address of the secondary NTP server (optional). | IPv4 address. |
| `ntp_secondary_version` | – | Configures the NTP version of the secondary NTP server (optional). | ■ `1`<br>■ `2`<br>■ `3`<br>■ `4` |
| `primary` | – | Configures the IP address of the primary DNS server (optional). | IPv4 address. |
| `proxy_address` | – | Configures the IP address of the proxy server (optional). | IPv4 address, or Hostname. |
| `proxy_port` | – | Configures the port number of the proxy server (optional). | A number from 1 to 65535. |

Table: The 'config_system' parameters (continued)

| Parameter | Supports Scalable Platforms? | Description | Valid values |
|---|---|---|---|
| `reboot_if_required` | – | Reboots the system after the configuration, if its value is set to "`true`" (optional). | ▪ `true`<br>▪ `false` |
| `secondary` | – | Configures the IP address of the secondary DNS server (optional). | IPv4 address. |
| `sg_cluster_id` | ✓ | For Check Point Support use only. | |
| `tertiary` | – | Configures the IP address of the tertiary DNS server (optional). | IPv4 address. |
| `timezone` | ✓ | Configures the Area/Region (optional). | The Area/Region must be enclosed between single quotation marks.<br>Examples:<br>`'America/New_York'`<br>`'Asia/Tokyo'`<br>**Note** - To see the available Areas and Regions, connect to any Gaia computer, log in to Gaia Clish, and run this command (names of Areas and Regions are case-sensitive):<br>`set timezone Area <SPACE><TAB>` |

Table: The 'config_system' parameters (continued)

| Parameter | Supports Scalable Platforms? | Description | Valid values |
|---|---|---|---|
| `upload_crash_data` | ✓ | Uploads core dump files that help Check Point resolve stability issues, if its value is set to "`true`". For more information, see *"Crash Data" on page 394*.  **Warning** - The core dump files may contain personal data. | ▪ `true`<br>▪ `false` (default) |
| `upload_info` | ✓ | Uploads data that helps Check Point provide you with optimal services, if its value is set to "`true`". For more information, see sk94509.  **Best Practice** - We highly recommended you enable this optional parameter. | ▪ `true`<br>▪ `false` (default) |

# Centrally Managing Gaia Device Settings

*In This Section:*



**Important** - Scalable Platform Security Groups do **not** support Central Management of Gaia Device Settings (Known Limitation MBS-4754):

1. Connect with SmartConsole to the Management Server.
2. From the left navigation panel, click **Gateways & Servers**.
3. Right-click on the Security Group object.
4. The **Scripts** and **Actions** menus are **not** supported.

# Introduction of Gaia Central Management

SmartConsole lets you:

- Centrally configure network topology:
  - IPv4 and IPv6 addresses
  - IPv4 and IPv6 static routes
- Centrally configure device settings for these network services:
  - DNS
  - NTP
  - Proxy server
- Do Backup and Restore operation

A compressed `.tgz` backup file captures the Gaia OS configuration and the Security Gateway database.

- Do maintenance operations:
  - By opening the Gaia Portal or command shell from SmartConsole
  - By fetching settings from the device, or by pushing settings to the device
- Examine recent tasks:

  The **Recent Tasks** tab, located in the bottom section of SmartConsole, shows recent Gaia Security Gateway management tasks done using SmartConsole.
- Run command line scripts on the Security Gateway.

  Output from the commands shows in the **Recent Tasks** window.

  Double-click the task to see the complete output.
- Receive notification on local device configuration change

  The **Status** column in the **Gateways** view indicates changes in the device configuration
- Implement configuration changes without a full policy install (**Push Settings to Device** action)
- Automate the configuration of Cloning Groups and synchronization between the members

# Managing Gaia in SmartConsole

After enabling Central management, Gaia Security Gateways can be more effectively managed through SmartConsole.

## Running Command Scripts

### One Time scripts

You can manually enter and run a command line script on the selected Gaia Security Gateways.

This feature is useful for scripts that you do not have to run on a regular basis.

**Running a one-time script**

| Step | Instructions |
|---|---|
| 1 | Right-click the Security Gateway. |
| 2 | Select **Scripts > Run One Time Script**. |
| 3 | The **Run One Time Script** window opens<br>You can:<br>■ Enter the command in the **Script Body** text box and specify script arguments, or<br>■ Load the complete command from a text file<br>**Notes:**<br>• By default, the maximum size of a script is: 8 kilobytes.<br>• This value can be changed in SmartConsole > **Main application menu > Global properties > Advanced > Configure > Central Device Management > device_settings_max_script_length_in_KB**. |
| 4 | Click **Run**.<br>The output from the script shows in the **Tasks** tab > **Results** column.<br>■ Double-clicking the task shows the output in a larger window<br>■ You can also right-click the task, and select **View**, and then **Copy to Clipboard**<br>**Notes:**<br>• The **Run One Time Script** window does not support interactive or continuous scripts. To run interactive or continuous scripts, open a command shell.<br>• If the Security Gateways are not part of a Cloning Group, you can run a script on multiple Security Gateways at the same time. |

### Running a script from the repository

| Step | Instructions |
|---|---|
| 1 | Right-click the Security Gateway. |
| 2 | Select **Scripts > Run Repository Script**. |
| 3 | The **Select Script** window opens.<br>You can:<br>■ Select a script from the drop-down box, or click **New** to create a new script for the repository.<br>■ Enter script arguments.<br>**Note** - The **Select Script** window does not support interactive or continuous scripts. To run interactive or continuous scripts, open a command shell. |
| 4 | Click **Run**.<br>The output from the script shows in the **Tasks** tab > **Results** column.<br>■ Placing the mouse in the **Details** column shows the output in a larger window.<br>■ You can also right-click, and select **View**, or **Copy to Clipboard**. |

## Manage repository scripts

You can create new scripts, edit or delete scripts from the script repository.

### Managing scripts

| Step | Instructions |
|---|---|
| 1 | Right-click the Security Gateway. |
| 2 | Select **Scripts > Manage Script Repository**. |
| 3 | The **Manage Scripts** window opens. |

**Note** - You can also run and manage scripts if you click **Scripts** in the Gateways view.

# Understanding One-Time Scripts

If you specify a script:

- By default, the maximum size of a script is: 8 kB.
- The output from the script shows in the **Tasks** tab at the bottom of the **Gateways & Servers** view.
- The **Run One Time Script** window does not support interactive or continuous scripts. To run interactive or continuous scripts, open a command shell.

# Running Repository Scripts

You can run a predefined script from the script repository.

**Running a script from the repository**

| Step | Instructions |
|---|---|
| 1 | In the **Gateways & Servers** view, right-click the Security Gateways or Security Management Servers, on which you want to run scripts. |
| 2 | Select **Scripts** > **Scripts Repository**.<br>The **Scripts Repository** window opens. |
| 3 | Do one of these steps:<br>■ Select an existing script from the list, click **Run**, enter **Arguments** if needed, and click **Run**.<br>■ Click **New** to create a new script for the repository, or load it from a text file. Click **OK**. |

The output from the script shows in the **Tasks** tab at the bottom of the **Gateways & Servers** view.

**Notes:**

- The **Scripts Repository** window does not support interactive or continuous scripts. To run interactive or continuous scripts, open a command shell.
- You can run the script on multiple Security Gateways or Security Management Servers at the same time.
- For a cluster object, the script will run automatically on all cluster members.

# Backup and Restore

These options let you:

- Back up the Gaia OS configuration and the Firewall database to a compressed file
- Restore the Gaia OS configuration and the Firewall database from a compressed file

**Best Practice** - We recommended using System Backup to back up your system regularly. Schedule system backups on a regular basis, daily or weekly, to preserve the Gaia OS configuration and Firewall database.

## Backing up the System

**Note** - After you install the Security Gateway for the first time, you must publish the SmartConsole session before you perform a system backup operation.

**Backing up the system**

| Step | Instructions |
|---|---|
| 1 | In the **Gateways & Servers** view, right-click the Security Gateway object you want to back up. |
| 2 | Select **Actions** > **System Backup**.<br>The **System Backup** window opens. |
| 3 | Select the backup location. Use one of these options:<br>■ The **Backup server defined for this gateway** - To define a backup server for this Security Gateway, double-click the Security Gateway object, and click **Network Management** > **System Backup**<br>■ Enter the details of the backup server<br>**Note** - The path to the backup directory must start and end with forward slash (/) character. For example: `/ftroot/backup/`, or just `/` for the root directory of the server.<br>The file name must be according to this convention:<br>`backup_<Name of Security Gateway object>_<Date of Backup>.tgz` |
| 4 | Click **OK**.<br>The status of the backup operation shows in **Tasks**. |
| 5 | When the task is complete, double-click the entry to see the file path and name of the backup file.<br>**Notes:**<br>■ This name is necessary to do a system restore.<br>■ You can do backup on multiple Security Gateways at the same time.<br>■ When you back up a cluster, the system does backup on all members. |

# Restoring the System

### Restoring the system

| Step | Instructions |
|---|---|
| 1 | In the **Gateways & Servers** view, right-click the Security Gateway object you want to restore. |
| 2 | Select **Actions** > **System Restore**.<br>The **System Restore** window opens. |
| 3 | Enter the required information.<br>**Note** - If you cannot find the name of the file in **Tasks**, or did not save the file name after you completed the backup process:<br>a. Right-click the Security Gateway object.<br>b. Select **Actions** > **Open Shell**.<br>c. On the Security Gateway, run the Gaia Clish command:<br>`show backup logs`<br>d. Find the name of the compressed backup file.<br>The file is named according to this convention:<br>`backup_<Name of Security Gateway object>_<Date of Backup>.tgz` |
| 4 | Click **OK**.<br>a. Connectivity to the Security Gateway is lost.<br>b. The Security Gateway automatically reboots. |
| 5 | Install the policy on the Security Gateway object.<br>The status of the restore operation shows in **Tasks** tab. |

# Opening Gaia Portal and Gaia Clish

In SmartConsole, you can open a Security Gateway's the command line window, or the Gaia Portal. You can select the command line or the Gaia Portal from the right-click menu of a Security Gateway object, or from the top toolbar > **Actions** button.

### Opening a command line window on the Security Gateway

| Step | Instructions |
|---|---|
| 1 | In SmartConsole, right-click the Security Gateway object. |
| 2 | Select **Actions > Open Shell**.<br>■ Log in with your Gaia credentials.<br>■ The Open Shell uses public key authentication.<br>■ For a cluster object, select the member, to which you want to connect.<br>A command line window opens with default shell that was configured for the specified user. |

### Opening a Security Gateway Gaia Portal

| Step | Instructions |
|---|---|
| 1 | In SmartConsole, right-click the Security Gateway object. |
| 2 | Select **Actions > Gaia Portal**.<br>**Note** - For a cluster, select the cluster member, for which you want to open the Gaia Portal.<br>The Gaia Portal opens in the default web browser.<br>The URL is taken from the **Platform Portal** page of the Security Gateway object. |

# Network Management

This chapter includes configuration procedures for:

- Interfaces (Physical, VLAN, Bond, Bridge, Loopback, VTI, Alias)
- ARP
- DHCP Server
- Hosts
- DNS
- Static Routes
- NetFlow Export

# Network Interfaces

Gaia supports these network interface types:

| Interface Type | Comments |
|---|---|
| Ethernet physical | |
| Alias | This feature adds Secondary IP addresses on different interface types.<br>■ ClusterXL does **not** support this feature.<br>■ On Scalable Platforms (Maestro and Chassis), it is necessary to set the value of the kernel parameter **fwha_arp_support_aliases** to **1** before the configuration. The feature is not supported in VSX mode. |
| VLAN | |
| VxLAN | Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation PMTR-60874). |
| Bond | |
| MAGG | This section applies **only** to Scalable Platforms (ElasticXL, Maestro, and Chassis). |
| Bridge | |
| Loopback | |
| VPN tunnel | Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation 00737055). |
| 6in4 tunnel | Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-12823). |
| PPPoE | Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature. |
| GRE | Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation PMTR-60868). |

**Note** - When you add, delete or make changes to interface IP addresses, it is possible that when you use the **Get Topology** option in SmartConsole in the Security Gateway or Cluster object, the incorrect topology is shown. If this occurs, run the "`cpstop`" and then the "`cpstart`" commands on the Security Gateway or Cluster Members.

# Physical Interfaces

*In This Section:*



This section has configuration procedures and examples for defining different types of interfaces on a Gaia platform.

Gaia automatically identifies physical interfaces (NICs) installed on the computer.

You cannot add or delete a physical interface in the Gaia Portal or Gaia Clish.

You cannot add, change or remove physical interface cards while the Gaia computer is running.

**Adding or removing an interface card**

| Step | Instructions |
|---|---|
| 1 | Turn off the Gaia computer:<br>■ In Gaia Portal:<br>Click **Maintenance > Shut Down**, and click **Halt**<br>■ In Gaia Clish:<br>Run: `halt` |
| 2 | Add, remove, or replace the interface cards. |
| 3 | Turn on the Gaia computer. |

Gaia automatically identifies the new or changed physical interfaces and assigns an interface name. The physical interfaces show in the list in the Gaia Portal.

## Configuring Physical Interfaces in Gaia Portal

This section includes procedures for changing physical interface parameters in the Gaia Portal.

**Note** - There are settings that you can configure only in Gaia Clish.

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Configuring a physical interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Select an interface from the list and click **Edit**. |
| 3 | Select the **Enable** option to set the interface status to UP. |
| 4 | In the **Comment** field, enter the applicable comment text (up to 100 characters). |
| 5 | On the **IPv4** tab, do one of these:<br>■ Select **Obtain IPv4 address automatically** to get the IPv4 address from the DHCPv4 server.<br>**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246).<br>■ Enter the IPv4 address and subnet mask in the applicable fields. |

| Step | Instructions |
|---|---|
| 6 | **Optional:** On the **IPv6** tab, do one of these:<br>■ Select **Obtain IPv6 address automatically via Autoconfig**.<br>■ Select **Obtain IPv6 address automatically via Normal DHCPv6**.<br>■ Select **Obtain IPv6 address automatically via Prefix Delegation**.<br>■ Select **Use the following IPv6 address.**<br>**Important:**<br>■ First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*).<br>■ R82 does **not** support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313).<br>■ On a Multi-Domain Security Management Server, follow these instructions to configure an IPv6 address - *"Configuring an IPv6 Address on a Multi-Domain Server" on page 710*.To configure an IPv6 address on a Multi-Domain Security Management Server, see the *R82 Gaia Administration Guide*.<br>■ Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature |
| 7 | On the **Ethernet** tab:<br>■ Select **Auto Negotiation**, or select a link speed and duplex setting from the list.<br>■ In the **Hardware Address** field, enter the Hardware MAC address (if not automatically received from the NIC).<br>**Caution** - Do not manually change the MAC address unless you are sure that it is incorrect or has changed. An incorrect MAC address can lead to a communication failure.<br>■ In the **MTU** field, enter the applicable Maximum Transmission Unit (MTU) value (minimum value is 68, maximum value is 16000, and default value is 1500).<br>■ Select **Monitor Mode**, if needed.<br>For the configuration procedure:<br>• On a Security Gateway and ClusterXL, see the *R82 Installation and Upgrade Guide* > Chapter *Special Scenarios for Security Gateways* > Section *Deploying a Security Gateway in Monitor Mode*.<br>• For Scalable Platforms, see the *R82 Scalable Platforms Administration Guide* > Chapter *Deploying a Security Group in Monitor Mode*. |
| 8 | Click **OK**. |

# Configuring Physical Interfaces in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

## Syntax

### Configuring an interface

```
set interface <Name of Physical Interface>
      auto-negotiation {on | off}
      comments "Text"
      ipv4-address <IPv4 Address> {subnet-mask <Mask> | mask-
length <Mask Length>}
      ipv6-address <IPv6 Address> mask-length <Mask Length>
      ipv6-autoconfig {on | off}
      link-speed {10M/half | 10M/full | 100M/half | 100M/full |
1000M/full | 10000M/full}
      mac-addr <MAC Address>
      monitor-mode {on | off}
      mtu <68-16000 | 1280-16000>
      rx-ringsize <0-4096>
      state {on | off}
      tx-ringsize <0-4096>
```

### Viewing all configured settings of all interfaces

```
show interfaces all
```

### Viewing all configured settings of a specific interface

```
show interface <Name of Physical Interface>
```

### Viewing the specific configured setting of a specific interface

```
show interface <Name of Physical Interface><SPACE><TAB>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| `interface <Name of Physical Interface>` | Specifies a physical interface. |

| Parameter | Description |
|---|---|
| `auto-negotiation {on \| off}` | Configures automatic negotiation of interface link speed and duplex settings:<br>■ `on` - Enabled<br>■ `off` - Disabled |
| `comments "Text"` | Configures an optional free text comment.<br>■ Write the text in double quotes.<br>■ Text must be up to 100 characters.<br>■ This comment appears in the Gaia Portal and in the output of the "`show configuration`" command. |
| `ipv4-address <IPv4 Address>` | Configures the IPv4 address. |
| `ipv6-address <IPv6 Address>` | Configures the IPv6 address.<br>**Important:**<br>■ First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*).<br>■ R82 does **not** support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313). |
| `links <Number>` | Configures the minimum number of required link interfaces for a ClusterXL Bond Load Sharing. |
| `subnet-mask <Mask>` | Configures the IPv4 subnet mask using dotted decimal notation (X.X.X.X). |
| `mask-length <Mask Length>` | Configures the IPv4 or IPv6 subnet mask length using the CIDR notation (integer between 2 and 32). |

| Parameter | Description |
|---|---|
| `ipv6-autoconfig {on \| off}` | Configures if this interface gets an IPv6 address from a DHCPv6 Server:<br>■ `on` - Gets an IPv6 address from a DHCPv6 Server<br>■ `off` - Does not get an IPv6 address from a DHCPv6 Server (you must assign it manually)<br>**Important:**<br>■ First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*).<br>■ Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature |
| `link-speed {10M/half \| 10M/full \| 100M/half \| 100M/full \| 1000M/full \| 1000M/full}` | Configures the interface link speed and duplex status. Available speed and duplex combinations are:<br>■ `10M/half`<br>■ `10M/full`<br>■ `100M/half`<br>■ `100M/full`<br>■ `1000M/full`<br>■ `10000M/full` |
| `mac-addr <MAC Address>` | Configures the hardware MAC address. |

| Parameter | Description |
|---|---|
| `monitor-mode {on \| off}` | Configures Monitor Mode on this interface:<br>■ `on` - Enabled<br>■ `off` - Disabled<br>**Default:** `off`<br>For the configuration procedure:<br>■ On a Security Gateway and ClusterXL, see the *R82 Installation and Upgrade Guide* > Chapter *Special Scenarios for Security Gateways* > Section *Deploying a Security Gateway in Monitor Mode*.<br>■ On Maestro, see the *R82 Scalable Platforms Administration Guide* > Chapter *Deploying a Security Group in Monitor Mode*.<br>■ On Scalable Chassis, see the *R82 Scalable Platforms Administration Guide* > Chapter *Deploying a Security Group in Monitor Mode*. |
| `mtu <68-16000 \| 1280-16000>` | Configures the Maximum Transmission Unit size for an interface.<br>For IPv4:<br>■ **Range:** 68 - 16000 bytes<br>■ **Default:** 1500 bytes<br>For IPv6:<br>■ **Range:** 1280 - 16000 bytes<br>■ **Default:** 1500 bytes |
| `rx-ringsize <0-4096>` | Configures the receive buffer size.<br>■ **Range:** 0 - 4096 bytes<br>■ **Default:** Depends on the interface driver |
| `state {on \| off}` | Configures the interface state:<br>■ `on` - Enabled<br>■ `off` - Disabled |
| `tx-ringsize <0-4096>` | Configures the transmit buffer size.<br>■ **Range:** 0 - 4096 bytes<br>■ **Default:** Depends on the interface driver |

**Example**

```
gaia> set interface eth2 ipv4-address 40.40.40.1 subnet-mask
255.255.255.0
gaia> set interface eth2 mtu 1400
gaia> set interface eth2 state on
gaia> set interface eth2 link-speed 100M/full
```

# Aliases

*In This Section:*



This section shows you how to configure an alias in the Gaia Portal and Gaia Clish.

Interface aliases let you assign more than one IPv4 address to physical or virtual interfaces (Bonds, Bridges, VLANs, and Loopbacks).

**Notes:**

- ClusterXL does **not** support aliases.
- You cannot change settings of an existing interface alias.

## Configuring Aliases in Gaia Portal

**Note** - This section does **not** apply to Scalable Platforms (ElasticXL, Maestro, and Chassis).

### Adding an interface alias

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Click **Add** > **Alias**. |
| 3 | On the **IPv4** tab, enter the IPv4 address and subnet mask. |
| 4 | On the **Alias** tab, select the applicable interface, to which this alias is assigned. |
| 5 | Click **OK**. |

**Note** - The new alias interface name is automatically created by adding a sequence number to the interface name. For example, the name of first alias added to **eth1** is **eth1:1**. The second alias added is **eth1:2**, and so on.

### Deleting an interface alias

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |

| Step | Instructions |
|---|---|
| 2 | Select an interface alias and click **Delete**. |
| 3 | Click **OK**, when the confirmation message shows. |

# Configuring Aliases in Gaia Clish

**Note** - This section does **not** apply to Scalable Platforms (ElasticXL, Maestro, and Chassis).

## Syntax

### Adding an alias

```
add interface <Name of Interface> alias <IPv4 Address>/<Mask Length>
```

**Note** - A new alias interface name is automatically created by adding a sequence number to the original interface name. For example, the name of first alias added to **eth1** is **eth1:1**. The second alias added is **eth1:2**, and so on.

### Viewing the configured aliases

```
show interface <Name of Interface> aliases
```

### Deleting an alias

```
delete interface <Name of Interface> alias <Name of Alias Interface>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| *<Name of Interface>* | Specifies the name of the interface, on which to create an alias IPv4 address |
| *<IPv4 Address>* | Assigns the alias IPv4 address |
| *<Mask Length>* | Configures alias IPv4 subnet mask length using the CIDR notation (integer between 2 and 32) |
| *<Name of Alias Interface>* | Specifies the name of the alias interface in the format `<IF>:XX`, where `XX` is the automatically assigned sequence number |

**Example**

```
gaia> add interface eth1 alias 10.10.99.1/24
gaia> show interface eth1 aliases
gaia> delete interface eth1 alias eth1:2
```

## Configuring Aliases on Scalable Platforms

**Notes:**

- This section applies **only** to Scalable Platforms (ElasticXL, Maestro, and Chassis).
- The feature is not supported in VSX mode.

**Important:**

- To control the support of aliases, you use the kernel parameter **fwha_arp_support_aliases**:

| Value of the Kernel Parameter | Gaia Behavior on Scalable Platforms |
|---|---|
| `fwha_arp_support_aliases=0` | This is the default.<br>Support of aliases is disabled. |
| `fwha_arp_support_aliases=1` | Support of aliases is enabled.<br>Gaia OS sends GARP packets from alias interfaces as well. |

- You can configure aliases only in Gaia gClish of the applicable Security Group.
- You cannot change settings of an existing interface alias. You must delete it and add a new alias.

For additional information, see sk167073.

**Adding an alias**

| Step | Instructions |
|---|---|
| 1 | Set the value of the kernel parameter **fwha_arp_support_aliases** to **1**:<br>a. Connect to the command line on the Security Group.<br>b. Log in to the Expert mode.<br>c. Configure the value *temporarily* (does not survive reboot):<br>`g_fw ctl set int fwha_arp_support_aliases 1`<br>d. Make sure the new value is set:<br>`g_fw ctl get int fwha_arp_support_aliases`<br>e. Configure the value *permanently* (requires reboot - you can reboot later at any time):<br>`g_update_conf_file $FWDIR/boot/modules/fwkern.conf fwha_arp_support_aliases=1` |

| Step | Instructions |
|---|---|
| 2 | In Gaia gClish of the applicable Security Group, add the applicable interface alias:<br>a. Connect to the command line on the Security Group.<br>b. Log in to Gaia Clish.<br>c. On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.<br>d. Add the applicable interface alias:<br>`add interface <Name of Interface> alias <IPv4 Address>/<Mask Length>`<br>**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.<br>**Note** - A new alias interface name is automatically created by adding a sequence number to the original interface name. For example, the name of first alias added to **eth1** is **eth1:1**. The second alias added is **eth1:2**, and so on. |
| 3 | Update the topology of the Security Gateway object in SmartConsole:<br>a. Connect with SmartConsole to the Management Server that manages this Security Group.<br>b. Open the applicable Security Gateway object.<br>c. From the left tree, click **Network Management**.<br>d. Click **Get Interfaces** > **Get Interfaces with Topology**.<br>**Best Practice** - In the **Topology** > **Leads To** section, use the default topology settings in the interface, on which you add an interface alias (and not the **Override** option). Otherwise, it is not possible to link alias networks to the applicable interface.<br>e. Make sure the information is correct and click **Accept**.<br>f. Click **OK**. |
| 4 | Install the Access Control Policy on this Security Gateway object. |
| 5 | Make sure the configuration is consistent on all Security Group Members:<br>a. Connect to the command line on the Security Group.<br>b. Log in to the Expert mode.<br>c. Run:<br>`config_verify -v` |

### Deleting an alias

| Step | Instructions |
|---|---|
| 1 | In Gaia gClish of the applicable Security Group, delete the applicable interface alias:<br>a. Connect to the command line on the Security Group.<br>b. Log in to Gaia Clish.<br>c. On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.<br>d. Add the applicable interface alias:<br>`delete interface <Name of Interface> alias <Name of Alias Interface>`<br>**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently. |
| 2 | Update the topology of the Security Gateway object in SmartConsole:<br>a. Connect with SmartConsole to the Management Server that manages this Security Group.<br>b. Open the applicable Security Gateway object.<br>c. From the left tree, click **Network Management**.<br>d. Click **Get Interfaces** > **Get Interfaces with Topology**.<br>**Best Practice** - In the **Topology** > **Leads To** section, use the default topology settings in the interface, on which you delete an interface alias (and not the **Override** option).<br>e. Make sure the information is correct and click **Accept**.<br>f. Click **OK**. |
| 3 | Install the Access Control Policy on this Security Gateway object. |
| 4 | Make sure the configuration is consistent on all Security Group Members:<br>a. Connect to the command line on the Security Group.<br>b. Log in to the Expert mode.<br>c. Run:<br>`config_verify -v` |

### Viewing the configured aliases

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on the applicable Security Group. |
| 2 | Log in to Gaia Clish. |
| 3 | On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter. |
| 4 | View the interface aliases:<br>`show interface <Name of Interface> aliases` |

### CLI Parameters

| Parameter | Description |
|---|---|
| *<Name of Interface>* | Specifies the name of the interface, on which to create an alias IPv4 address |
| *<IPv4 Address>* | Assigns the alias IPv4 address |
| *<Mask Length>* | Configures alias IPv4 subnet mask length using the CIDR notation (integer between 2 and 32) |
| *<Name of Alias Interface>* | Specifies the name of the alias interface in the format `<IF>:XX`, where `XX` is the automatically assigned sequence number |

### Example

```
[Global] HostName-ch01-01 > add interface eth1 alias
10.10.99.1/24
[Global] HostName-ch01-01 > show interface eth1 aliases
[Global] HostName-ch01-01 > delete interface eth1 alias eth1:2
```

# VLAN Interfaces

*In This Section:*



This section shows you how to configure VLAN interfaces in the Gaia Portal and Gaia Clish.

You can configure virtual LAN (VLAN) interfaces on Ethernet interfaces.

VLAN interfaces let you configure subnets with a secure private link to Security Gateways and Management Servers using your existing topology.

With VLAN interfaces, you can multiplex Ethernet traffic into many channels using one cable.

**Important** - In a Cluster, you must configure all the Cluster Members in the same way.

**Notes:**

- The name of a VLAN interface in Gaia is "`<Name of Physical Interface>.<VLAN ID>`".
  For example, the name of a VLAN interface with a VLAN ID of 5 on a physical interface `eth1` is "*eth1.5*".
- The VLAN tunnel is not secure, because it is not encrypted.
- To configure MTU on a VLAN interface, you must configure MTU on the physical interface.
  This MTU applies to all VLAN interfaces configured on this physical interface.

## Configuring VLAN Interfaces in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Adding a VLAN interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Make sure that the physical interface, on which you add a VLAN interface, does not have an IP address. |
| 3 | Click **Add** > **VLAN**. |
| 4 | In the **Add VLAN** window, select the **Enable** option to set the VLAN interface to UP. |
| 5 | On the **IPv4** tab, do one of these:<br>■ Select **Obtain IPv4 address automatically** to get the IPv4 address from the DHCPv4 server.<br>**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246).<br>■ Enter the IPv4 address and subnet mask in the applicable fields. |
| 6 | **Optional:** On the **IPv6** tab, do one of these:<br>■ Select **Obtain IPv6 address automatically via Autoconfig**.<br>■ Select **Obtain IPv6 address automatically via Normal DHCPv6**.<br>■ Select **Obtain IPv6 address automatically via Prefix Delegation**.<br>■ Select **Use the following IPv6 address.**<br>**Important:**<br>■ First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*).<br>■ R82 does **not** support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313).<br>■ On a Multi-Domain Security Management Server, follow these instructions to configure an IPv6 address - *"Configuring an IPv6 Address on a Multi-Domain Server" on page 710*.To configure an IPv6 address on a Multi-Domain Security Management Server, see the *R82 Gaia Administration Guide*.<br>■ Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246). |
| 7 | On the **VLAN** tab, enter or select a **VLAN ID** (VLAN tag) between 2 and 4094. |
| 8 | In the **Member Of** field, select the applicable physical interface. |
| 9 | Click **OK**. |

### Editing a VLAN interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Select a VLAN interface and click **Edit**. |
| 3 | Configure the applicable settings. |
| 4 | Click **OK**. |

**Note** - You cannot change the VLAN ID or physical interface for an existing VLAN interface. To change these parameters, delete the VLAN interface and then create a new VLAN interface.

### Deleting a VLAN interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Select a VLAN interface and click **Delete**. |
| 3 | Click **OK**, when the confirmation message shows. |

# Configuring VLAN Interfaces in Gaia Clish

**Important:**

- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- Make sure that the physical interface, on which you wish to add a VLAN interface, does **not** have an IP address.

## Syntax

### Adding a new VLAN interface

```
add interface <Name of Physical Interface> vlan <VLAN ID>
```

### Configuring a VLAN interface

```
set interface <Name of Physical Interface>.<VLAN ID>
      comments "Text"
      ipv4-address <IPv4 Address>
            subnet-mask <Mask>
            mask-length <Mask Length>
      ipv6-address <IPv6 Address> mask-length <Mask Length>
      ipv6-autoconfig {on | off}
      mtu <68-16000 | 1280-16000>
      state {on | off}
```

**Note** - You cannot change the VLAN ID or physical interface for an existing VLAN interface. To change these parameters, delete the VLAN interface and then create a new VLAN interface.

### Viewing the configuration of a specific VLAN interface

```
show interface<SPACE><TAB>
```

```
show interface <Name of VLAN Interface>
```

### Deleting a VLAN interface

```
delete interface <Name of Physical Interface> vlan <VLAN ID>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| `<Name of Physical Interface>` | Specifies a physical interface. |
| `comments "Text"` | Defines the optional comment.<br>■ Write the text in double quotes.<br>■ Text must be up to 100 characters.<br>■ This comment appears in the Gaia Portal and in the output of the "`show configuration`" command. |
| `<VLAN ID>` | Configures the ID of the VLAN interface (integer between 2 and 4094). |
| `<IPv4 Address>` | Assigns the IPv4 address. |
| `<IPv6 Address>` | Assigns the IPv6 address.<br>**Important** - First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*). |
| `subnet-mask <Mask>` | Configures the IPv4 subnet mask using the dotted decimal notation (X.X.X.X) - integer between 2 and 32.. |
| `mask-length <Mask Length>` | Configures the IPv6 subnet mask length using CIDR notation (/xx) - integer between 1 and 128. |
| `ipv6-autoconfig {on \| off}` | Configures if this interface gets an IPv6 address from a DHCPv6 Server:<br>■ `on` - Gets an IPv6 address from a DHCPv6 Server<br>■ `off` - Does not get an IPv6 address from a DHCPv6 Server (you must assign it manually)<br>**Important** - First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*). |

| Parameter | Description |
|---|---|
| `mtu <68-16000 \| 1280-16000>` | Configures the Maximum Transmission Unit size for an interface.<br>For IPv4:<br>■ **Range:** 68 - 16000 bytes<br>■ **Default:** 1500 bytes<br>For IPv6:<br>■ **Range:** 1280 - 16000 bytes<br>■ **Default:** 1500 bytes |
| `state {on \| off}` | Configures interface's state:<br>■ `on` - Enabled<br>■ `off` - Disabled |

**Example**

```
gaia> add interface vlan eth1
gaia> set interface eth1.99 ipv4-address 99.99.99.1 subnet-mask
255.255.255.0
gaia> set interface eth1.99 ipv6-address 209:99:1 mask-length 64
gaia> delete interface eth1 vlan 99
```

## Access Mode VLAN and Trunk Mode VLAN

VLAN traffic can pass through a Bridge interface in one of these modes:

### Access Mode VLAN

If you configure the switch ports in Access Mode, create the Bridge interface with two VLAN interfaces as its subordinate interfaces.

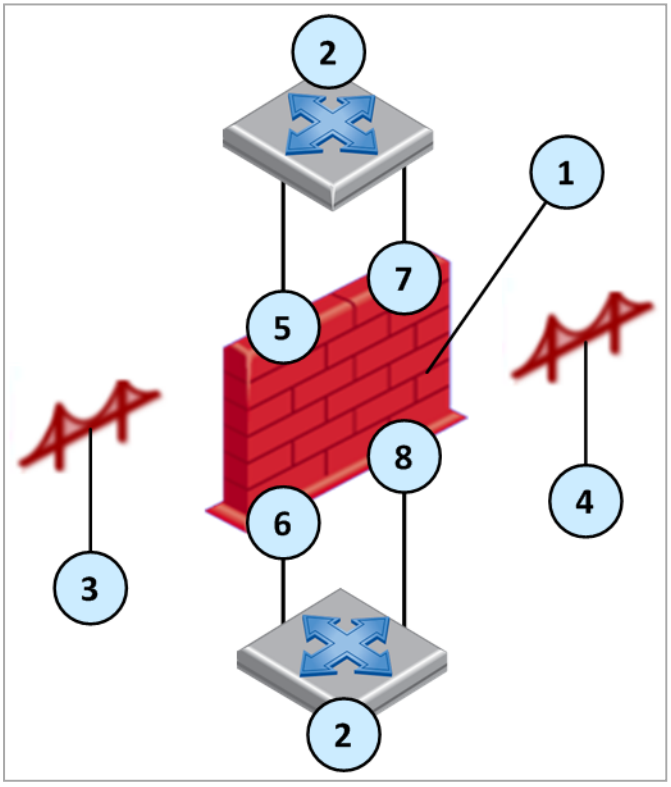
For **VLAN translation**, use different numbered VLAN interfaces to create the Bridge interface.

You can build multiple VLAN translation bridges on the same Security Gateway.

1. Configure two VLAN interfaces.
2. Create a Bridge interface and select the VLAN interfaces as its subordinate interfaces (see *"Bridge Interfaces" on page 168*).

**Note** - VLAN translation is not supported over bridged ports of a FONIC (Fail-Open NIC, see sk85560).

**Example topology:**




| Item | Description |
|---|---|
| 1 | Security Gateway |

| Item | Description |
|---|---|
| 2 | Switch |
| 3 | Access mode bridge 1 with VLAN translation |
| 4 | Access mode bridge 2 with VLAN translation |
| 5 | VLAN 3 (eth 1.3) |
| 6 | VLAN 33 (eth 2.33) |
| 7 | VLAN 2 (eth 1.2) |
| 8 | VLAN 22 (eth 2.22) |

### Trunk Mode VLAN

If you configure the switch ports as VLAN trunk, the Check Point Bridge interface should **not** interfere with the VLANs.

To configure a Bridge interface with VLAN trunk, create the Bridge interface with two physical (non-VLAN) interfaces as its subordinate interfaces (see *"Bridge Interfaces" on page 168*).

The Security Gateway processes the tagged packet and does not remove VLAN tags from them.

The traffic passes with the original VLAN tag to its destination.

**Note** - VLAN translation is not supported in Trunk mode.

# VXLAN Interfaces

*In This Section:*



**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation PMTR-60874).

This section shows you how to configure VXLAN interfaces in the Gaia Portal and Gaia Clish.

Virtual Extensible LAN (VXLAN) is a network virtualization technology that attempts to address the scalability problems associated with large cloud computing deployments. VXLAN uses a VLAN-like encapsulation technique to encapsulate OSI Layer 2 Ethernet frames within Layer 4 UDP datagrams. See RFC 7348.

**Notes:**

- The name of a VXLAN interface in Gaia OS is "`vxlan<`*`VNI`*`>`".
  For example, the name of a VXLAN interface with a VXLAN VNI of 5 is "*vxlan5*".
- The VXLAN tunnel is not secure, because it is not encrypted.

For additional information, see sk170014.

# Configuring VXLAN Interfaces in Gaia Portal

### Adding a VXLAN interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Click **Add** > **VXLAN**. |
| 3 | In the **Add VXLAN** window, select the **Enable** option to set the VXLAN interface to UP. |
| 4 | On the **IPv4** tab, enter the local IPv4 address and subnet mask for the VXLAN interface. |
| 5 | **Optional:** On the **IPv6** tab, do one of these:<br>■ Select **Obtain IPv6 address automatically via Autoconfig**.<br>■ Select **Obtain IPv6 address automatically via Normal DHCPv6**.<br>■ Select **Obtain IPv6 address automatically via Prefix Delegation**.<br>■ Select **Use the following IPv6 address.**<br>**Important:**<br>■ First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*).<br>■ R82 does **not** support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313).<br>■ On a Multi-Domain Security Management Server, follow these instructions to configure an IPv6 address - *"Configuring an IPv6 Address on a Multi-Domain Server" on page 710*.To configure an IPv6 address on a Multi-Domain Security Management Server, see the *R82 Gaia Administration Guide*.<br>■ Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246). |

| Step | Instructions |
|---|---|
| 6 | On the **VXLAN Tunnel** tab:<br>a. In the **VXLAN VNI** field, enter or select the VXLAN Network Identifier (or VXLAN Segment ID) between 1 and 16,777,215.<br>**Important** - This value must be the same on the VXLAN peers.<br>b. In the **Member Of** field, select the physical interface related to this VXLAN.<br>c. In the **Remote Address** field, enter the IPv4 address of the applicable physical interface on the remote VXLAN peer.<br>d. In the **DST Port** field, enter or select the destination UDP port number between 1 and 65535 (default is 4789 - see *IANA Service Name and Port Number Registry*).<br>**Best Practice** - Use the default UDP port 4789. |
| 7 | Click **OK**. |

**Example**

Security Gateway "GW1" and Security Gateway "GW2" create a VXLAN.

[GW1] (physical interface `eth1`) (VXLAN interface) <==>
<==> (Internet) <==>
<==> (VXLAN interface) (physical interface `eth2` [GW2]

The VXLAN interface configuration on these VXLAN peers:

| Setting | Security Gateway "GW1" | Security Gateway "GW2" |
|---|---|---|
| Local physical interface | `eth1` with IPv4 10.10.10.11 / 24 | `eth2` with IPv4 172.30.40.22 / 24 |
| (VXLAN) IPv4 Address | 192.168.10.11 / 24 | 192.168.10.22 / 24 |
| VXLAN VNI | 33 | 33 |
| Member Of | eth1 | eth2 |
| Remote Address | 172.30.40.22 | 10.10.10.11 |

**Editing a VXLAN interface**

**Important** - It is not supported to edit the settings of an existing VxLAN interface. You must delete the existing VxLAN interface and create a new VxLAN interface.

### Deleting a VXLAN interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Select a VXLAN interface and click **Delete**. |
| 3 | Click **OK**, when the confirmation message shows. |

# Configuring VXLAN Interfaces in Gaia Clish

## Syntax

### Adding a VXLAN interface

```
add vxlan id <VXLAN VNI> dev <Name of local physical interface>
remote <IPv4 address of physical interface on remote peer>
dstport <Destination UDP port>
```

### Viewing the configured VxLAN interface

```
show configuration vxlan
```

```
show vxlan id <VXLAN ID>
```

### Editing a VXLAN interface

**Important** - It is not supported to edit the settings of an existing VxLAN interface. You must delete the existing VxLAN interface and create a new VxLAN interface.

### Deleting a VXLAN interface

```
delete vxlan id <VXLAN VNI>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### CLI Parameters

| Parameter | Description |
|---|---|
| `id <VXLAN VNI>` | Configures the VXLAN Network Identifier (or VXLAN Segment ID) of the VXLAN interface (integer between 1 and 16,777,215).<br>**Important** - This value must be the same on the VXLAN peers. |
| `comments "Text"` | Defines the optional comment.<br>■ Write the text in double quotes.<br>■ Text must be up to 100 characters.<br>■ This comment appears in the Gaia Portal and in the output of the "`show configuration`" command. |
| `dev <Name of local physical interface>` | Specifies a local physical interface. |

| Parameter | Description |
|---|---|
| `dstport <Destination UDP port>` | Specifies the destination UDP port number between 1 and 65535 (default is 4789 - see *IANA Service Name and Port Number Registry*).<br>**Important** - This value must be the same on the VXLAN peers.<br>**Best Practice** - Use the default UDP port 4789. |
| `remote <IPv4 address of physical interface on remote peer>` | Specifies the IPv4 address of the applicable physical interface on the remote VXLAN peer. |

**Example**

Security Gateway "GW1" and Security Gateway "GW2" create a VXLAN.

[GW1] (physical interface `eth1`) (VXLAN interface) <==>
<==> (Internet) <==>
<==> (VXLAN interface) (physical interface `eth2` [GW2]

The VXLAN interface configuration on these VXLAN peers:

| Setting | Security Gateway "GW1" | Security Gateway "GW2" |
|---|---|---|
| Local physical interface | `eth1` with IPv4 10.10.10.11 / 24 | `eth2` with IPv4 172.30.40.22 / 24 |
| (VXLAN) IPv4 Address | 192.168.10.11 / 24 | 192.168.10.22 / 24 |
| VXLAN VNI | 33 | 33 |
| Member Of | eth1 | eth2 |
| Remote Address | 172.30.40.22 | 10.10.10.11 |

The VXLAN interface configuration on the Security Gateway "GW1":

```
gaia1> add vxlan id 33 dev eth1 remote 172.30.40.22 dstport 4789
```

The VXLAN interface configuration on the Security Gateway "GW2":

```
gaia2> add vxlan id 33 dev eth2 remote 10.10.10.11 dstport 4789
```

## Configuring VXLAN Interfaces on Cluster Members

For more information, see the *R82 ClusterXL Administration Guide*.

In Cluster, you have these options:

**To use a VXLAN interface as a cluster interface with a Virtual IP address**

1. Configure a VXLAN interface on all the Cluster Members.

   You must configure the *same* **VXLAN VNI** and **Remote Address** on each Cluster Member.
2. Connect with SmartConsole to the Management Server.
3. From the left navigation panel, click **Gateways & Servers**.
4. Double-click the cluster object.
5. From the left tree, click **Network Management**.
6. From the toolbar, click **Get Interfaces** > **Get Interfaces With Topology** and confirm.

   Make sure you see the new VXLAN interface from each Cluster Member.
7. Select the new VXLAN interface and click **Edit**.
8. From the left tree, click the **General** page.
9. In the **General** section, in the **Network Type** field, select **Cluster**.
10. In the **IPv4** field, configure the applicable cluster Virtual IP address.
11. In the **Member IPs** section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.
12. Click **OK**.
13. Publish the SmartConsole session.
14. Install the Access Control Policy on this cluster object.

**To use a VXLAN interface only on a specific Cluster Member**

1. Configure a VXLAN interface on a specific Cluster Member.
2. Connect with SmartConsole to the Management Server.
3. From the left navigation panel, click **Gateways & Servers**.
4. Double-click the cluster object.
5. From the left tree, click **Network Management**.
6. From the toolbar, click **Get Interfaces** > **Get Interfaces With Topology** and confirm.

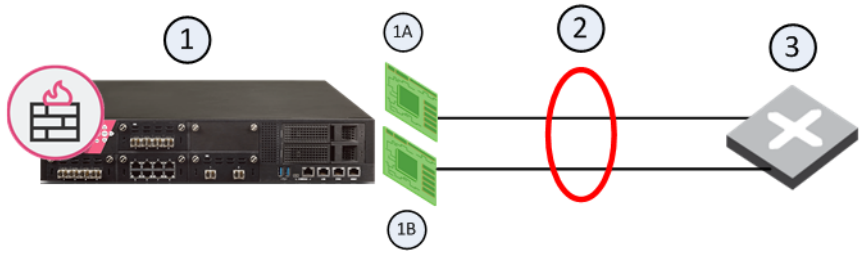
Make sure you see the new VXLAN interface from the specific Cluster Member, on which you configured it.

7. Select the new VXLAN interface and click **Edit**.
8. From the left tree, click the **General** page.
9. In the **General** section, in the **Network Type** field, select **Private**.
10. Click **OK**.
11. Publish the SmartConsole session.
12. Install the Access Control Policy on this cluster object.

# Bond Interfaces (Link Aggregation)

Check Point security devices support **Link Aggregation**, a technology that joins multiple physical interfaces into one virtual interface, known as a **bond interface**.

The bond interface share the load among many interfaces, which gives fault tolerance and increases throughput. Check Point devices support the IEEE 802.3ad Link Aggregation Control Protocol (LACP) for dynamic link aggregation.




| Item | Description |
|---|---|
| 1 | Security Gateway |
| 1A | Interface 1 |
| 1B | Interface 2 |
| 2 | Bond Interface |
| 3 | Router |

A **bond interface** (also known as a **bonding group** or **bond**) is identified by its **Bond ID** (for example: *bond1*) and is assigned an IP address. The physical interfaces included in the bond are called **subordinate interfaces** and do not have IP addresses.

You can configure a bond interface to use one of these functional strategies:

**High Availability (Active/Backup)**

Gives redundancy when there is an interface or a link failure. This strategy also supports switch redundancy.

Bond High Availability works in **Active/Backup** mode - interface Active/Standby mode. When an Active subordinate interface is down, the connection automatically fails over to the primary subordinate interface. If the primary subordinate interface is not available, the connection fails over to a different subordinate interface.

**Load Sharing (Active/Active)**

All subordinate interfaces in the UP state are used simultaneously.

Traffic is distributed among the subordinate interfaces to maximize throughput. Bond Load Sharing does not support switch redundancy.

**Note** - Bonding Load Sharing mode requires SecureXL to be enabled on Security Gateway or each Cluster Member.

You can configure Bond Load Sharing to use one of these modes:

| Mode | Description |
|---|---|
| **Round Robin** | Selects the Active subordinate interfaces sequentially.<br>**Note** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-4080). |
| **802.3ad** | Dynamically uses Active subordinate interfaces to share the traffic load. This mode uses the LACP protocol, which fully monitors the interface link between the Check Point Security Gateway and a switch. |
| **XOR** | All subordinate interfaces in the UP state are Active for Load Sharing. Traffic is assigned to Active subordinate interfaces based on one of these transmit hash policies:<br>■ Layer 2 information (XOR of hardware MAC addresses)<br>■ Layer 3+4 information (IP addresses and Ports) |
| **ABXOR** | Subordinate interfaces in the UP state are assigned to sub-groups called *bundles*.<br>Only one bundle is Active at a time.<br>All subordinate interfaces in the Active bundle share the traffic load.<br>The system assigns traffic to all interfaces in the Active bundle based on the defined transmit hash policy.<br>**Note** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-1520). |

For Bonding High Availability mode and for Bonding Load Sharing mode:

- The number of bond interfaces that can be defined is limited by the maximum number of interfaces supported by each platform.

  See the *R82 Release Notes*.

- Up to 8 physical subordinate interfaces can be configured in a single bond interface.

# Configuring Bond Interfaces in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Make sure that the subordinate interfaces, which you wish to add to the Bond interface, do not have IP addresses. |
| 3 | For a new bond interface, select **Add** > **Bond**.<br>To edit an existing Bond interface, select the Bond interface and click **Edit**. |
| 4 | On the **IPv4** tab, enter the IPv4 address and subnet mask.<br>You can optionally select the **Obtain IPv4 Address automatically** option.<br>**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246). |
| 5 | **Optional:** On the **IPv6** tab, do one of these:<br>■ Select **Obtain IPv6 address automatically via Autoconfig**.<br>■ Select **Obtain IPv6 address automatically via Normal DHCPv6**.<br>■ Select **Obtain IPv6 address automatically via Prefix Delegation**.<br>■ Select **Use the following IPv6 address.**<br>**Important:**<br>■ First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*).<br>■ R82 does **not** support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313).<br>■ On a Multi-Domain Security Management Server, follow these instructions to configure an IPv6 address - *"Configuring an IPv6 Address on a Multi-Domain Server" on page 710*.To configure an IPv6 address on a Multi-Domain Security Management Server, see the *R82 Gaia Administration Guide*.<br>■ Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246). |

| Step | Instructions |
|---|---|
| 6 | On the **Bond** tab:<br>a. Select or enter a **Bond Group ID**. This parameter is an integer between 0 and 1024.<br>b. Select the subordinate interfaces from the **Available Interfaces** list and then click **Add**.<br>**Note** - Make sure that the subordinate interfaces do not have any IP addresses or aliases configured.<br>c. Select an **Operation Mode**:<br>▪ **Round Robin** (default)<br>Bond uses all subordinate interfaces sequentially (High Availability + Load Sharing).<br>**Note** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-4080).<br>▪ **Active-Backup**<br>Bond uses one subordinate interface at a time (High Availability).<br>▪ **XOR**<br>Bond uses subordinate interfaces based on a hash function (High Availability + Load Sharing).<br>▪ **802.3ad**<br>Dynamic bonding according to IEEE 802.3ad (Load Sharing). |
| 7 | On the **Advanced** tab:<br>a. Configure the required **MTU** for your network (if not sure, leave the default value).<br>b. Configure the **Monitor Interval** - How much time to wait between checking each subordinate interface for link-failure. The valid range is 1-5000 ms. The default is 100 ms.<br>c. Configure the **Down Delay** - How much time to wait, after sending a monitor request to a subordinate interface, before bringing down the subordinate interface. The valid range is 1-5000 ms. The default is 200 ms.<br>d. Configure the **Up Delay** - How much time to wait, after sending a monitor request to a subordinate interface, before bringing up the subordinate interface. The valid range is 1-5000 ms. The default is 200 ms. |

| Step | Instructions |
|---|---|
| 8 | Additional configuration settings are available depending on the selected Bond Operation Mode:<br>■ If you selected the **Round Robin** bond operation mode, then there are no additional configuration settings.<br>■ If you selected the **Active-Backup** bond operation mode, then select the **Primary Interface**.<br>By default, the first subordinate interface added to the bond group, becomes the primary.<br>**Important** - You must **not** configure the primary subordinate interface explicitly in ClusterXL when you configure the Sync interface on a bonding group for redundancy. For more information, see the *R82 ClusterXL Administration Guide* > Chapter *ClusterXL Requirements and Compatibility* > Section *Supported Topologies for Synchronization Network*.<br>■ If you selected the **XOR** bond operation mode, then select the **Transmit Hash Policy** - the algorithm for subordinate interface selection according to the specified TCP/IP Layer.<br>Select either **Layer 2** (uses XOR of the physical interface MAC address), or **Layer 3+4** (uses Layer 3 and Layer 4 protocol data).<br>■ If you selected the **802.3ad** bond operation mode, then perform these two steps:<br>a. Select the **Transmit Hash Policy** - the algorithm for subordinate interface selection according to the specified TCP/IP Layer.<br>Select either **Layer 2** (uses XOR of the physical interface MAC address), or **Layer 3+4** (uses IP addresses and Ports).<br>b. Select the **LACP Rate** - how frequently the LACP partner should transmit LACPDUs.<br>Select either **Slow** (every thirty seconds), or **Fast** (every one second). |
| 9 | Click **OK**. |

**Notes:**

- The name of a Bond interface in Gaia is "`bond<Bond Group ID>`".
  For example, the name of a bond interface with a Bond Group ID of 5 is "*bond5*".
- To configure MTU on a Bond subordinate interface, you must configure MTU on the Bond interface.
  This MTU applies to all subordinate interfaces assigned to this Bond interface.

## Configuring Bond Interfaces in Gaia Clish

In Gaia Clish, bond interfaces are called **bonding groups**.

| Step | Instructions |
|---|---|
| 1 | Make sure that the physical subordinate interfaces do not have IP addresses. |
| 2 | Add a new bonding group. |
| 3 | Set the state of the physical subordinate interfaces to **UP**. |
| 4 | Add subordinate interfaces to the bonding group. |
| 5 | Configure the bond operating mode. |
| 6 | Configure other bond parameters: primary interface, media monitoring, and delay rate. |
| 7 | Examine the bonding group configuration. |
| 8 | Save the configuration. |

**Notes:**

- You configure an IP address on a Bonding Group in the same way as you do on a physical interface (see *"Physical Interfaces" on page 103*).
- The name of a Bond interface in Gaia is "`bond<Bond Group ID>`".
  For example, the name of a bond interface with a Bond Group ID of 5 is "*bond5*".
- To configure MTU on a Bond subordinate interface, you must configure MTU on the Bond interface.
  This MTU applies to all subordinate interfaces assigned to this Bond interface.

**Important:**

- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Syntax

#### Adding a new Bonding Group

##### Syntax

```
add bonding group <Bond Group ID>
```

##### Example

```
gaia> add bonding group 777
```

**Note** - Do **not** change the state of bond interface manually using the "`set interface <Bond ID> state`" command. This is done automatically by the bonding driver.

#### Adding a new subordinate interface to an existing Bonding Group

##### Syntax

```
add bonding group <Bond Group ID> interface <Name of Subordinate Interface>
```

**Important** - Make sure that the subordinate interfaces, which you wish to add to the Bonding Group, do not have IP addresses.

##### Example

```
gaia> add bonding group 777 interface eth4
gaia> add bonding group 777 interface eth5
```

**Notes:**

- The subordinate interfaces must not have IP addresses assigned to them.
- The subordinate interfaces must not have aliases assigned to them.
- A bond interface can contain between two and eight subordinate interfaces.

### Configuring an existing Bonding Group

#### Syntax

```
set bonding group <Bond Group ID>
      mode active-backup [primary <Name of Subordinate
Interface>]
      mode round-robin
      mode 8023AD [lacp-rate {slow | fast}]
      mode xor xmit-hash-policy {layer2 | layer3+4}
      mode ABXOR xmit-hash-policy {layer2 | layer3+4} [abxor-
threshold <min number of UP subordinate interfaces>]
      [up-delay <0-5000>]
      [down-delay <0-5000>]
      [mii-interval <1-5000>]
      [min-links <0-8>]
```

#### Configuring the Bond Operating Mode

Bond operating mode specifies how subordinate interfaces are used in a bond interface.

#### Syntax

```
set bonding group <Bond Group ID> mode
      round-robin
      active-backup [primary <Name of Subordinate Interface>]
      xor xmit-hash-policy {layer2 | layer3+4}
      8023AD [lacp-rate {slow | fast}]
      ABXOR xmit-hash-policy {layer2 | layer3+4} [abxor-
threshold <Min number of UP subordinate interfaces>]
```

#### Example

```
gaia> set bonding group 1 mode active-backup primary eth2
gaia> set bonding group 2 mode xor xmit-hash-policy layer3+4
```

**Notes:**

- The Active-Backup mode supports configuration of the primary subordinate interface.
- The XOR mode requires the configuration of the transmit hash policy.
- The 8023AD mode supports the configuration of the LACP packet transmission rate and the transmit hash policy.

### Configuring the Up Delay Time

The **Up-Delay** specifies show much time in milliseconds to wait before enabling a subordinate interface after link recovery was detected.

#### Syntax

```
set bonding group <Bond Group ID> up-delay <0-5000>
```

#### Example

```
gaia> set bonding group 1 up-delay 100
```

**Note** - The default `up-interval` value is 200 ms.

### Configuring the Down Delay Time

The **Down-Delay** specifies how much time in milliseconds to wait before disabling a subordinate interface after link failure was detected.

#### Syntax

```
set bonding group <Bond Group ID> down-delay <0-5000>
```

#### Example

```
gaia> set bonding group 1 down-delay 100
```

**Note** - The default `down-interval` value is 200 ms.

### Configuring the Media Monitoring Interval

The **Media Monitoring Interval** specifies how much time in milliseconds to wait before checking the link on subordinate interfaces for a failure.

#### Syntax

```
set bonding group <Bond Group ID> mii-interval <1-5000>
```

#### Example

```
gaia> set bonding group 1 mii-interval 100
```

**Note** - The default `mii-interval` value is 100 ms.

### Configuring the minimum number of required interface links for a bonding group in the 802.3AD mode

You can configure the minimum number of required interface links for a bonding group in the 802.3AD mode.

If fewer subordinate interfaces in a bonding group have their link in the "up" state, the Gaia changes the state of the bonding group to "down".

#### Syntax

```
set bonding group <Bond Group ID> min-links <0-8>
```

#### Example

```
gaia> set bonding group 1 min-links 2
```

**Note** - The default "`min-links`" value is 0. With this value, Gaia does not count how many subordinate interfaces in a bonding group have their link in the "up" state.

### Configuring an IP address on the existing Bonding Group

```
set interface <Bond Group ID>
      comments "Text"
      ipv4-address <IPv4 Address> {subnet-mask <Mask> | mask-
length <Mask Length>}
      ipv6-address <IPv6 Address> mask-length <Mask Length>
      ipv6-autoconfig {on | off}
      link-speed {10M/half | 10M/full | 100M/half | 100M/full |
1000M/full | 10000M/full}
      mac-addr <MAC Address>
```

For more information, see *"Configuring Physical Interfaces in Gaia Clish" on page 106*.

### Deleting a subordinate interface from an existing Bonding Group

#### Syntax

```
delete bonding group <Bond Group ID> [interface <Interface Name>
| force-ignore-routes]
```

#### Example

```
gaia> delete bonding group 777 interface eth4
```

**Note** - You must delete all non-primary subordinate interfaces before you remove the primary subordinate interface.

### Deleting the Bonding Group

#### Syntax

```
delete bonding group <Bond Group ID> interface <Name of
Subordinate Interface 1>
delete bonding group <Bond Group ID> interface <Name of
Subordinate Interface 2>
delete bonding group <Bond Group ID> interface <Name of
Subordinate Interface ...>
delete bonding group <Bond Group ID> interface <Name of
Subordinate Interface N>
delete bonding group <Bond Group ID>
```

#### Example

```
gaia> delete bonding group 777
```

**Notes:**

- You must delete all non-primary subordinate interfaces before you remove the primary subordinate interface.
- You must delete all subordinate interfaces from the bonding group before you remove the bonding group.
- Do **not** change the state of bond interface manually using the "`set interface bondID state`" command.
  This is done automatically by the bonding driver.

### Viewing the Bonding Group configuration

#### Syntax

```
show bonding {group <Bond Group ID> | groups}
```

#### Parameters

#### CLI Parameters

| Parameter | Description |
|---|---|
| *<Bond Group ID>* | Configures the Bond Group ID.<br>■ **Range:** 0 - 1024<br>■ **Default:** No default value |

| Parameter | Description |
|---|---|
| `<Name of Subordinate Interface>` | Specifies the name of the subordinate physical interface, which you add to (or remove from) the bond group.<br>Make sure that the subordinate interfaces do not have any IP addresses or aliases configured. |
| `mode <Mode>` | Configures the Bond operating mode (see *"Bond Interfaces (Link Aggregation)" on page 135*):<br>■ `round-robin`<br>Bond uses all subordinate interfaces sequentially (High Availability + Load Sharing).<br>This is the default mode.<br>**Note** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-4080).<br>■ `active-backup [primary <Name of Subordinate Interface>]`<br>Bond uses one subordinate interface at a time (High Availability)<br>■ `xor xmit-hash-policy {layer2 \| layer3+4}`<br>Bond uses subordinate interfaces based on a hash function (High Availability + Load Sharing)<br>■ `8023AD [lacp-rate {slow \| fast}]`<br>Dynamic bonding according to IEEE 802.3ad - LACP (Load Sharing)<br>■ `ABXOR xmit-hash-policy ...`<br>Subordinate interfaces in the UP state are assigned to sub-groups called *bundles*.<br>Only one bundle is Active at a time.<br>All subordinate interfaces in the Active bundle share the traffic load.<br>The system assigns traffic to all interfaces in the Active bundle based on the defined transmit hash policy.<br>**Note** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-1520). |

| Parameter | Description |
|---|---|
| `primary <Name of Subordinate Interface>` | Specifies the name of the *primary* subordinate interface in the bond.<br>By default, the first subordinate interface added to the bond group, becomes the primary.<br>**Important** - You must **not** configure the primary subordinate interface explicitly in ClusterXL when you configure the Sync interface on a bonding group for redundancy. For more information, see the *R82 ClusterXL Administration Guide* > Chapter *ClusterXL Requirements and Compatibility* > Section *Supported Topologies for Synchronization Network*.<br>**Note** - Applies only to the Active-Backup bond mode. |
| `up-delay <0-5000>` | Specifies the time in milliseconds to wait before enabling a subordinate interface after link recovery was detected.<br>■ **Range:** 0 - 5000 ms<br>■ **Default:** 200 ms |
| `down-delay <0-5000>` | Specifies the time in milliseconds to wait before disabling a subordinate interface after link failure was detected.<br>■ **Range:** 0 - 5000 ms<br>■ **Default:** 200 ms |
| `lacp-rate {fast \| slow}` | Specifies the Link Aggregation Control Protocol (LACP) packet transmission rate:<br>■ `slow` - LACPDU packets are sent every 30 seconds<br>■ `fast` - LACPDU packets are sent every second<br>**Note** - Applies only to the 802.3AD bond mode. |
| `mii-interval <1-5000>` | Specifies the time in milliseconds to wait before checking the link on subordinate interfaces for a failure.<br>■ **Range:** 1 - 5000 ms<br>■ **Default:** 100 ms |

| Parameter | Description |
|---|---|
| `min-links <0-8>` | Specifies the minimum number of required interface links for a bonding group in the 802.3AD mode.<br>If fewer subordinate interfaces in a bonding group have their link in the "up" state, the Gaia changes the state of the bonding group to "down".<br>■ **Range:** 0 - 8<br>■ **Default:** 0 (Gaia does not count how many subordinate interfaces in a bonding group have their link in the "up" state)<br>**Notes:**<br>■ Applies only to the 802.3AD bond mode.<br>■ In a cluster, also refer to the command "`set interface <Bond Group ID> links`". For more information, see the *R82 ClusterXL Administration Guide* > Chapter *ClusterXL Requirements and Compatibility* > Section *Configuring the Minimum Number of Required Subordinate Interfaces for Bond Load Sharing*. |
| `xmit-hash-policy {layer2 \| layer3+4}` | Specifies the algorithm to use for assigning the traffic to Active subordinate interfaces:<br>■ `layer2` - Based on the XOR of hardware MAC addresses<br>■ `layer3+4` - Based on the IP addresses and Ports<br>**Note** - Applies only to the XOR and the 802.3AD bond modes. |
| `abxor-threshold <Min number of UP subordinate interfaces>` | Specifies the minimum number of subordinate interfaces that must be in the UP sate for a bundle to be Active.<br>**Notes:**<br>■ Applies only to the ABXOR and the 802.3AD bond modes.<br>■ Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-1520). |

## Examples

### Example 1 - Configuring Bond in "Active-Backup" mode with default settings

```
gaia> add bonding group 1
gaia> add bonding group 1 interface eth2
gaia> add bonding group 1 interface eth3
gaia> set bonding group 1 mode active-backup primary eth2
gaia> show bonding group 1
Bond Configuration
    xmit-hash-policy Not configured
    down-delay 200
    primary eth2
    lacp-rate Not configured
    mode active-backup
    up-delay 200
    mii-interval 100
    Bond Interfaces
        eth2
        eth3
gaia>
```

### Example 2 - Configuring Bond in "XOR" mode with default settings

```
gaia> add bonding group 1
gaia> add bonding group 1 interface eth2
gaia> add bonding group 1 interface eth3
gaia> set bonding group 1 mode xor xmit-hash-policy layer3+4
gaia> show bonding group 1
Bond Configuration
    xmit-hash-policy layer3+4
    down-delay 200
    primary Not configured
    lacp-rate Not configured
    mode xor
    up-delay 200
    mii-interval 100
    Bond Interfaces
        eth2
        eth3
gaia>
```

## Making Sure that Bond Interface is Working

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on the Security Gateway or Cluster Member. |
| 2 | Log in to the Expert mode. |
| 3 | Examine the Bond interface state and configuration:<br>`[Expert@MyGaia:0]# cat /proc/net/bonding/<Bond Group ID>` |

**Example 1 - Output for Bond Operating Mode "Round Robin"**

```
[Expert@MyGaia:0]# cat /proc/net/bonding/bond1
Ethernet Channel Bonding Driver: v3.2.4 (January 28, 2008)

Bonding Mode: load balancing (round-robin)
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 200
Down Delay (ms): 200

Slave Interface: eth2
MII Status: up
Link Failure Count: 0
Permanent HW addr: 00:50:56:a3:73:69

Slave Interface: eth3
MII Status: up
Link Failure Count: 0
Permanent HW addr: 00:50:56:a3:73:70
[Expert@MyGaia:0]#
```

**Note** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-4080).

### Example 2 - Output for Bond Operating Mode "Active-Backup"

```
[Expert@MyGaia:0]# cat /proc/net/bonding/bond1
Ethernet Channel Bonding Driver: v3.2.4 (January 28, 2008)

Bonding Mode: fault-tolerance (active-backup)
Primary Slave: eth2
Currently Active Slave: eth2
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 200
Down Delay (ms): 200

Slave Interface: eth2
MII Status: up
Link Failure Count: 0
Permanent HW addr: 00:50:56:a3:73:69

Slave Interface: eth3
MII Status: up
Link Failure Count: 0
Permanent HW addr: 00:50:56:a3:73:70
[Expert@MyGaia:0]#
```

### Example 3 - Output for Bond Operating Mode "XOR"

```
[Expert@MyGaia:0]# cat /proc/net/bonding/bond1
Ethernet Channel Bonding Driver: v3.2.4 (January 28, 2008)

Bonding Mode: load balancing (xor)
Transmit Hash Policy: layer2 (0)
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 200
Down Delay (ms): 200

Slave Interface: eth2
MII Status: up
Link Failure Count: 0
Permanent HW addr: 00:50:56:a3:73:69

Slave Interface: eth3
MII Status: up
Link Failure Count: 0
Permanent HW addr: 00:50:56:a3:73:70
[Expert@MyGaia:0]#
```

**Example 4 - Output for Bond Operating Mode "802.3ad" (LACP)**

```
[Expert@MyGaia:0]# cat /proc/net/bonding/bond1
Ethernet Channel Bonding Driver: v3.2.4 (January 28, 2008)

Bonding Mode: IEEE 802.3ad Dynamic link aggregation
Transmit Hash Policy: layer2 (0)
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 200
Down Delay (ms): 200

802.3ad info
LACP rate: slow

Slave Interface: eth2
MII Status: up
Link Failure Count: 0
Permanent HW addr: 00:50:56:a3:73:69
Aggregator ID: 1

Slave Interface: eth3
MII Status: up
Link Failure Count: 0
Permanent HW addr: 00:50:56:a3:73:70
Aggregator ID: 1
[Expert@MyGaia:0]#
```

# Configuring Bond High Availability in VRRP Cluster

**Note** - This section does **not** apply to Scalable Platforms (ElasticXL, Maestro, and Chassis).

The R80.20 version introduced an improved Active/Backup Bond mechanism (Enhanced Bond) when working in ClusterXL.

If you work with ClusterXL, the Enhanced Bond feature is enabled by default, and no additional configuration is required.

If you change your cluster configuration from ClusterXL to VRRP (MCVR & VRRP), or configure the VRRP (MCVR & VRRP) cluster from scratch, the Enhanced Bond feature is disabled by default.

If you change your cluster configuration from VRRP to ClusterXL, you must manually enable the Enhanced Bond feature.

To enable the Enhanced Bond feature in VRRP Cluster, set the value of the kernel parameter `fwha_bond_enhanced_enable` to 1 on *each* VRRP Cluster Member. You can set the value of the kernel parameter temporarily, or permanently.

**Setting the value of the kernel parameter temporarily**

**Important** - This change does not survive reboot.

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on *each* VRRP Cluster Member. |
| 2 | Log in to the Expert mode. |
| 3 | Set the value of the kernel parameter `fwha_bond_enhanced_enable` to 1:<br>`fw ctl set int fwha_bond_enhanced_enable 1` |
| 4 | Make sure the value of the kernel parameter `fwha_bond_enhanced_enable` was set to 1:<br>`fw ctl get int fwha_bond_enhanced_enable` |

**Setting the value of the kernel parameter permanently**

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on *each* Cluster Member. |
| 2 | Log in to the Expert mode. |
| 3 | Back up the current `$FWDIR/boot/modules/fwkern.conf` file:<br>`cp -v $FWDIR/boot/modules/fwkern.conf{,_BKP}` |
| 4 | Edit the current `$FWDIR/boot/modules/fwkern.conf` file:<br>`vi $FWDIR/boot/modules/fwkern.conf` |
| 5 | Add this line to the file (spaces and comments are not allowed):<br>`fwha_bond_enhanced_enable=1` |
| 6 | Save the changes in the file and exit the editor. |
| 7 | Reboot the Cluster Member. |
| 8 | Make sure the value of the kernel parameter `fwha_bond_enhanced_enable` was set to 1:<br>`fw ctl get int fwha_bond_enhanced_enable` |

**Important** - If you change your cluster configuration from VRRP to ClusterXL, you must remove the kernel parameter configuration from each Cluster Member.

# MAGG Interfaces

*In This Section:*



Management Aggregation (MAGG) is a High Availability and Load Sharing solution for management interfaces on Scalable Platforms (Maestro and Chassis).

You can create a Bond interface on the Management Ports. This can be useful for testing purposes, or as a proxy interface for an unnumbered interface.

This section shows you how to configure a MAGG interface in the Gaia Portal and Gaia Clish.

**Notes:**

- MAGG interface does **not** support VLAN interfaces on its management bonding group.
- The name of a MAGG interface in Gaia is "`magg<Bond Group ID>`".
  For example, the name of a MAGG interface with a Bond Group ID of 1 is "*magg1*".
- To configure MTU on a MAGG subordinate interface, you must configure MTU on the Bond interface.
  This MTU applies to all subordinate interfaces assigned to this MAGG interface.

## Configuring MAGG Interfaces in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Adding a MAGG interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Interface Management** > **Network Interfaces**. |
| 2 | Click **Add** > **Magg**. |
| 3 | In the **Comment** field, enter the applicable comment text (up to 100 characters). |
| 4 | On the **IPv4** tab, do one of these:<br>■ Select **Obtain IPv4 address automatically** to get the IPv4 address from the DHCPv4 server.<br>**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246).<br>■ Enter the IPv4 address and subnet mask in the applicable fields. |
| 5 | **Optional:** On the **IPv6** tab, do one of these:<br>■ Select **Obtain IPv6 address automatically via Autoconfig**.<br>■ Select **Obtain IPv6 address automatically via Normal DHCPv6**.<br>■ Select **Obtain IPv6 address automatically via Prefix Delegation**.<br>■ Select **Use the following IPv6 address.**<br>**Important:**<br>■ First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*).<br>■ R82 does **not** support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313).<br>■ Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246). |
| 6 | On the **Magg** tab:<br>a. Select or enter a **Bond Group** ID. This parameter is an integer between 0 and 1024.<br>b. Select the subordinate interface **eth<*X*>-Mgmt<*Y*>** interfaces from the **Available Interfaces** list and then click **Add**.<br>**Note** - Make sure that the subordinate interfaces do not have any IP addresses or aliases configured. |

| Step | Instructions |
|---|---|
| 7 | On the **Advanced** tab:<br>a. Configure the **Monitor Interval** - How much time to wait between checking each subordinate interface for link-failure. The valid range is 1-5000 ms. The default is 100 ms.<br>b. Configure the **Down Delay** - How much time to wait, after sending a monitor request to a subordinate interface, before bringing down the subordinate interface. The valid range is 1-5000 ms. The default is 200 ms.<br>c. Configure the **Up Delay** - How much time to wait, after sending a monitor request to a subordinate interface, before bringing up the subordinate interface. The valid range is 1-5000 ms. The default is 200 ms.<br>d. Select the **Transmit Hash Policy** - the algorithm for subordinate interface selection according to the specified TCP/IP Layer.<br>Select either **Layer 2** (uses XOR of the physical interface MAC address), or **Layer 3+4** (uses IP addresses and Ports). |
| 8 | Click **OK**. |

### Configuring a MAGG interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Interface Management** > **Network Interfaces**. |
| 2 | Select a MAGG interface and click **Edit**. |
| 3 | In the **Edit magg<ID>** window, it is possible to change all available settings. |
| 4 | Click **OK**. |

### Deleting a MAGG interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Select a MAGG interface and click **Delete**. |
| 3 | Click **OK**, when the confirmation message shows. |

# Configuring MAGG Interfaces in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | Make sure that the physical subordinate interfaces do not have IP addresses. |
| 2 | Add a new management bonding group. |
| 3 | Set the state of the physical subordinate interfaces to **UP**. |
| 4 | Add subordinate interfaces to the management bonding group. |
| 5 | Configure the management bond operating mode. |
| 6 | Configure other bond parameters: media monitoring, and delay rate. |
| 7 | Examine the management bonding group configuration. |
| 8 | Save the configuration. |

## Syntax

### Adding a new management Bonding Group

#### Syntax

```
add bonding group <Bond Group ID> mgmt
```

#### Example

```
gaia> add bonding group 777 mgmt
```

**Note** - Do **not** change the state of bond interface manually using the "`set interface <Bond ID> state`" command. This is done automatically by the bonding driver.

### Adding a new subordinate interface to an existing management Bonding Group

#### Syntax

```
add bonding group <Bond Group ID> mgmt interface <Name of
Subordinate Interface eth<X>-Mgmt<Y>>
```

**Important** - Make sure that the subordinate interfaces, which you wish to add to the Bonding Group, do not have IP addresses.

#### Example

```
gaia> add bonding group 777 mgmt interface eth1-Mgmt1
gaia> add bonding group 777 mgmt interface eth2-Mgmt1
```

**Notes:**

- The subordinate interfaces must not have IP addresses assigned to them.
- The subordinate interfaces must not have aliases assigned to them.
- A bond interface can contain between two and eight subordinate interfaces.

### Configuring an existing management Bonding Group

#### Syntax

```
set bonding group <Bond Group ID>
      mode active-backup
      mode xor xmit-hash-policy {layer2 | layer3+4}
      [up-delay <0-5000>]
      [down-delay <0-5000>]
      [mii-interval <1-5000>]
```

### Configuring the Bond Operating Mode

Bond operating mode specifies how subordinate interfaces are used in a bond interface.

#### Syntax

```
set bonding group <Bond Group ID>
      active-backup [primary <Name of Subordinate Interface>]
      mode xor xmit-hash-policy {layer2 | layer3+4}
```

#### Example

```
gaia> set bonding group 1 mode active-backup primary eth1-
Mgmt1
gaia> set bonding group 2 mode xor xmit-hash-policy layer3+4
```

**Notes:**

- The MAGG interface only support the Active/Backup or the XOR mode.
- The Active-Backup mode supports configuration of the primary subordinate interface.
- The XOR mode requires the configuration of the transmit hash policy.

### Configuring the Up Delay Time

The **Up-Delay** specifies show much time in milliseconds to wait before enabling a subordinate interface after link recovery was detected.

#### Syntax

```
set bonding group <Bond Group ID> up-delay <0-5000>
```

#### Example

```
gaia> set bonding group 1 up-delay 100
```

**Note** - The default `up-interval` value is 200 ms.

### Configuring the Down Delay Time

The **Down-Delay** specifies how much time in milliseconds to wait before disabling a subordinate interface after link failure was detected

#### Syntax

```
set bonding group <Bond Group ID> down-delay <0-5000>
```

#### Example

```
gaia> set bonding group 1 down-delay 100
```

**Note** - The default `down-interval` value is 200 ms.

### Configuring the Media Monitoring Interval

The **Media Monitoring Interval** specifies how much time in milliseconds to wait before checking the link on subordinate interfaces for a failure.

#### Syntax

```
set bonding group <Bond Group ID> mii-interval <1-5000>
```

#### Example

```
gaia> set bonding group 1 mii-interval 100
```

**Note** - The default `mii-interval` value is 100 ms.

## Deleting a subordinate interface from an existing Bonding Group

#### Syntax

```
delete bonding group <Bond Group ID> [interface <Interface Name>
| force-ignore-routes]
```

#### Example

```
gaia> delete bonding group 777 interface eth2-Mgmt1
```

**Note** - You must delete all non-primary subordinate interfaces before you remove the primary subordinate interface.

### Deleting the bonding group

#### Syntax

```
delete bonding group <Bond Group ID> interface <Name of
Subordinate Interface 1>
delete bonding group <Bond Group ID> interface <Name of
Subordinate Interface 2>
delete bonding group <Bond Group ID> interface <Name of
Subordinate Interface ...>
delete bonding group <Bond Group ID> interface <Name of
Subordinate Interface N>
delete bonding group <Bond Group ID>
```

#### Example

```
gaia> delete bonding group 777
```

**Notes:**

- You must delete all non-primary subordinate interfaces before you remove the primary subordinate interface.
- You must delete all subordinate interfaces from the bonding group before you remove the bonding group.
- Do **not** change the state of bond interface manually using the "`set interface bondID state`" command.
  This is done automatically by the bonding driver.

### Viewing the Bonding Group configuration

#### Syntax

```
show bonding {group <Bond Group ID> | groups}
```

#### Parameters

##### CLI Parameters

| Parameter | Description |
|---|---|
| *<Bond Group ID>* | Configures the Bond Group ID.<br>■ **Range:** 0 - 1024<br>■ **Default:** No default value |

| Parameter | Description |
|---|---|
| `<Name of Subordinate Interface>` | Specifies the name of the subordinate physical interface, which you add to (or remove from) the bond group.<br>Make sure that the subordinate interfaces do not have any IP addresses or aliases configured. |
| `mode <Mode>` | Configures the Bond operating mode (see *"Bond Interfaces (Link Aggregation)" on page 135*).<br>The MAGG interface only support the Active/Backup or the XOR mode:<br>■ `active-backup [primary <Name of Subordinate Interface>]`<br>Bond uses one subordinate interface at a time (High Availability)<br>■ `xor xmit-hash-policy {layer2 \| layer3+4}`<br>Bond uses subordinate interfaces based on a hash function (High Availability + Load Sharing) |
| `primary <Name of Subordinate Interface>` | Specifies the name of the *primary* subordinate interface in the bond.<br>By default, the first subordinate interface added to the bond group, becomes the primary.<br>**Note** - Applies only to the Active-Backup bond mode. |
| `up-delay <0-5000>` | Specifies the time in milliseconds to wait before enabling a subordinate interface after link recovery was detected.<br>■ **Range:** 0 - 5000 ms<br>■ **Default:** 200 ms |
| `down-delay <0-5000>` | Specifies the time in milliseconds to wait before disabling a subordinate interface after link failure was detected.<br>■ **Range:** 0 - 5000 ms<br>■ **Default:** 200 ms |
| `mii-interval <1-5000>` | Specifies the time in milliseconds to wait before checking the link on subordinate interfaces for a failure.<br>■ **Range:** 1 - 5000 ms<br>■ **Default:** 100 ms |

| Parameter | Description |
|---|---|
| `xmit-hash-policy {layer2 \| layer3+4}` | Specifies the algorithm to use for assigning the traffic to Active subordinate interfaces:<br>▪ `layer2` - Based on the XOR of hardware MAC addresses<br>▪ `layer3+4` - Based on the IP addresses and Ports<br>**Note** - Applies only to the XOR bond mode. |

## Examples

### Example 1 - Configuring Bond in "Active-Backup" mode with default settings

```
gaia> add bonding group 1 mgmt
gaia> add bonding group 1 mgmt interface eth1-Mgmt1
gaia> add bonding group 1 mgmt interface eth2-Mgmt1
gaia> set bonding group 1 mode active-backup primary eth1-Mgmt1
gaia> show bonding group 1
Bond Configuration
    xmit-hash-policy Not configured
    down-delay 200
    primary eth1-Mgmt1
    lacp-rate Not configured
    mode active-backup
    up-delay 200
    mii-interval 100
    Bond Interfaces
        eth1-Mgmt1
        eth2-Mgmt1
gaia>
```

**Example 2 - Configuring Bond in "XOR" mode with default settings**

```
gaia> add bonding group 1 mgmt
gaia> add bonding group 1 mgmt interface eth1-Mgmt1
gaia> add bonding group 1 mgmt interface eth2-Mgmt1
gaia> set bonding group 1 mode xor xmit-hash-policy layer3+4
gaia> show bonding group 1
Bond Configuration
    xmit-hash-policy layer3+4
    down-delay 200
    primary Not configured
    lacp-rate Not configured
    mode xor
    up-delay 200
    mii-interval 100
    Bond Interfaces
        eth1-Mgmt1
        eth2-Mgmt1
gaia>
```

# Bridge Interfaces

Configure interfaces as a bridge to deploy security devices in a topology without reconfiguration of the IP routing scheme. This is an important advantage for large-scale, complex environments.

Bridge interfaces connect two different interfaces (*bridge ports*). Bridging two interfaces causes every Ethernet frame that is received on one bridge port to be transmitted to the other port. Thus, the two bridge ports participate in the same Broadcast domain (different from router port behavior). The security policy inspects every Ethernet frame that passes through the bridge.

**Important** - Only two interfaces can be connected by one Bridge interface, creating a virtual two-port switch. Each port can be a physical, VLAN, or bond device.

It is possible to configure bridge mode with one Security Gateway, a Cluster, or a Scalable Platform Security Group. The bridge functions without an assigned IP address. Bridged Ethernet interfaces (including aggregated interfaces) to work like ports on a physical bridge. It is possible to configure the topology for the bridge ports in SmartConsole. A separate network or group object represents the networks or subnets that connect to each port.

**Notes:**

- The name of a Bridge interface in Gaia is "`br<Bridge Group ID>`".
  For example, the name of a bridge interface with a Bridge Group ID of 5 is "*br5*".
- Gaia OS supports bridge interfaces that implement native, Layer 2 bridging.
- Gaia OS does **not** support Spanning Tree Protocol (STP) bridges.
- A subordinate interface that is a part of a bond interface cannot be a part of a bridge interface.
- For UserCheck to work properly, bridge group must use an IP address on the same subnet as clients or routers that connect to a Security Gateway, Cluster, or Security Group.
- Scalable Chassis 60000 / 40000 do **not** generate BPDU (STP) frames.
- Scalable Chassis 60000 / 40000 forward BPDU (STP) packets between subordinate interfaces of the bridge.
- To configure MTU on a Bridge subordinate interface, you must configure MTU on the Bridge interface.
  This MTU applies to all subordinate interfaces assigned to this Bridge interface.

The bridge interfaces send traffic with Layer 2 addressing. On the same device, you can configure some interfaces as bridge interfaces, while other interfaces work as Layer 3 interfaces. Traffic between bridge interfaces is inspected at Layer 2. Traffic between two Layer 3 interfaces, or between a bridge interface and a Layer 3 interface is inspected at Layer 3.

# Configuring Bridge Interfaces in Gaia Portal

**Note** - For additional information:

- For Security Gateways or ClusterXL - see the *R82 Installation and Upgrade Guide* > Chapter *Special Scenarios for Security Gateways* > Section *Deploying a Security Gateway or a ClusterXL in Bridge Mode*.
- For Scalable Platforms - see the *R82 Scalable Platforms Administration Guide* > Chapter *Deploying a Security Group in Bridge Mode*.

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | In the left navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Make sure that the subordinate interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned. |
| 3 | Click **Add** > **Bridge**.<br>To configure an existing Bridge interface, select the Bridge interface and click **Edit**. |
| 4 | On the **Bridge** tab, enter or select a **Bridge Group** ID (unique integer between 1 and 1024). |
| 5 | Select the interfaces from the **Available Interfaces** list and then click **Add**.<br>**Notes:**<br>■ Make sure that the subordinate interfaces do not have any IP addresses or aliases configured.<br>■ Do **not** select the interface that you configured as Gaia Management Interface.<br>■ A Bridge interface in Gaia can contain only two subordinate interfaces. |
| 6 | On the **IPv4** tab, enter the IPv4 address and subnet mask.<br>You can optionally select the **Obtain IPv4 Address automatically** option. |

| Step | Instructions |
|---|---|
| 7 | **Optional:** On the **IPv6** tab, do one of these:<br>■ Select **Obtain IPv6 address automatically via Autoconfig**.<br>■ Select **Obtain IPv6 address automatically via Normal DHCPv6**.<br>■ Select **Obtain IPv6 address automatically via Prefix Delegation**.<br>■ Select **Use the following IPv6 address.**<br>**Important:**<br>■ First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*).<br>■ R82 does **not** support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313).<br>■ On a Multi-Domain Security Management Server, follow these instructions to configure an IPv6 address - *"Configuring an IPv6 Address on a Multi-Domain Server" on page 710*.To configure an IPv6 address on a Multi-Domain Security Management Server, see the *R82 Gaia Administration Guide*.<br>■ Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246). |
| 8 | Click **OK**. |

**Notes:**

- The name of a Bridge interface in Gaia is "`br<Bridge Group ID>`".
  For example, the name of a bridge interface with a Bridge Group ID of 5 is "*br5*".
- To configure MTU on a Bridge subordinate interface, you must configure MTU on the Bridge interface.
  This MTU applies to all subordinate interfaces assigned to this Bridge interface.

# Configuring Bridge Interfaces in Gaia Clish

In Gaia Clish, bond interfaces are called **bridging groups**.

**Notes:**

- You configure an IP address on a Bridging Group in the same way as you do on a physical interface (see *"Physical Interfaces" on page 103*).
- The name of a Bridge interface in Gaia is "`br<Bridge Group ID>`".
  For example, the name of a bridge interface with a Bridge Group ID of 5 is "*br5*".
- To configure MTU on a Bridge subordinate interface, you must configure MTU on the Bridge interface.
  This MTU applies to all subordinate interfaces assigned to this Bridge interface.
- For additional information:
  - For Security Gateways or ClusterXL - see the *R82 Installation and Upgrade Guide* > Chapter *Special Scenarios for Security Gateways* > Section *Deploying a Security Gateway or a ClusterXL in Bridge Mode*.
  - For Scalable Platforms - see the *R82 Scalable Platforms Administration Guide* > Chapter *Deploying a Security Group in Bridge Mode*.

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

### Procedure

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on the Security Gateway, Cluster Member, or Security Group. |
| 2 | Log in to Gaia Clish. |
| 3 | Make sure that the subordinate interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned:<br>`show interface <Name of Subordinate Interface> ipv4-address`<br>`show interface <Name of Subordinate Interface> ipv6-address` |
| 4 | Add a new bridging group:<br>`add bridging group <Bridge Group ID 0 - 1024>`<br>**Note** - Do **not** change the state of bond interface manually using the "`set interface <Bridge Group ID> state`" command. This is done automatically by the bridging driver. |

| Step | Instructions |
|---|---|
| 5 | Add subordinate interfaces to the new bridging group:<br>`add bridging group <Bridge Group ID> interface <Name of First Subordinate Interface>`<br>`add bridging group <Bridge Group ID> interface <Name of Second Subordinate Interface>`<br>**Notes:**<br>■ Do **not** select the interface that you configured as Gaia Management Interface.<br>■ Only Ethernet, VLAN, and Bond interfaces can be added to a bridge group.<br>■ A Bridge interface in Gaia can contain only two subordinate interfaces. |
| 6 | Assign an IP address to the bridging group.<br>**Note** - You configure an IP address on a Bridging Group in the same way as you do on a physical interface (see *"Physical Interfaces" on page 103*).<br>■ To assign an IPv4 address, run:<br>`set interface <Name of Bridging Group> ipv4-address <IPv4 Address> {subnet-mask <Mask> \| mask-length <Mask Length>}`<br>You can optionally configure the bridging group to obtain an IPv4 Address automatically.<br>■ To assign an IPv6 address, run:<br>`set interface <Name of Bridging Group> ipv6-address <IPv6 Address> mask-length <Mask Length>`<br>You can optionally configure the bridging group to obtain an IPv6 Address automatically.<br>**Important** - First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*). |
| 7 | Save the configuration:<br>`save config` |

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Syntax

#### Adding a new bridging group

##### Syntax

```
add bridging group <Bridge Group ID>
```

**Note** - Do **not** change the state of bond interface manually using the "`set interface <Bridge Group ID> state`" command. This is done automatically by the bridging driver.

#### Adding a new subordinate interface to an existing bridging group

##### Syntax

```
add bridging group <Bridge Group ID> interface <Name of Subordinate Interface>
```

##### Example

```
gaia> add bridging group 56 interface eth1
```

**Note** - Make sure that the subordinate interfaces do not have any IP addresses or aliases configured.

#### Adding a fail-open interface to an existing bridging group

##### Syntax

```
add bridging group <Bridge Group ID> fail-open-interfaces <Name of Subordinate Interface>
```

### Configuring an existing Bridging Group

#### Syntax

```
set interface <Name of Bridge Interface>
      comments "Text"
      ipv4-address <IPv4 Address>
            subnet-mask <Mask>
            mask-length <Mask Length>
      ipv6-address <IPv6 Address> mask-length <Mask Length>
      ipv6-autoconfig {on | off}
      mac-addr <MAC Address>
      mtu <68-16000 | 1280-16000>
      rx-ringsize <0-4096>
      tx-ringsize <0-4096>
```

#### Example

```
gaia> set interface br1 ipv6-address 3000:40::1 mask-length 64
```

### Deleting a subordinate interface from an existing bridging group

#### Syntax

```
delete bridging group <Bridge Group ID> interface <Name of
Subordinate Interface>
```

#### Example

```
gaia> delete bridging group 56 interface eth1
```

### Deleting a fail-open interface from the bridging group

#### Syntax

```
delete bridging group <Bridge Group ID> fail-open-interfaces
<Name of Subordinate Interface>
```

### Deleting the bridging group

#### Syntax

```
delete bridging group <Bridge Group ID>
```

**Notes:**

- You must delete all subordinate interfaces from the bridging group before you delete the bridging group.
- Do **not** change the state of bond interface manually using the "`set interface <Bridge Group ID> state`" command. This is done automatically by the bridging driver.

#### Example

```
gaia> delete bridging group 56
```

### Viewing the subordinate interfaces of an existing bridging group

#### Syntax

```
show bridging group <Bridge Group ID>
```

### Viewing the configured bridging groups

#### Syntax

```
show bridging groups
```

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| *<Bridge Group ID>* | Configures the Bridge Group ID.<br>■ **Range:** 0 - 1024<br>■ **Default:** No default value |
| *<Name of Bridge Interface>* | Configures the name of the Bridge interface. |

| Parameter | Description |
|---|---|
| `<Name of Subordinate Interface>` | Specifies a physical subordinate interface. |
| `comments "Text"` | Configures an optional free text comment.<br>■ Write the text in double quotes.<br>■ Text must be up to 100 characters.<br>■ This comment appears in the Gaia Portal and in the output of the show configuration command. |
| `ipv4-address <IPv4 Address>` | Configures the IPv4 address. |
| `ipv6-address <IPv6 Address>` | Configures the IPv6 address.<br>**Important** - First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*). |
| `subnet-mask <Mask>` | Configures the IPv4 subnet mask using dotted decimal notation (X.X.X.X). |
| `mask-length <Mask Length>` | Configures the IPv4 or IPv6 subnet mask length using the CIDR notation (integer between 2 and 32). |
| `ipv6-autoconfig {on \| off}` | Configures if this interface gets an IPv6 address from a DHCPv6 Server:<br>■ `on` - Gets an IPv6 address from a DHCPv6 Server<br>■ `off` - Does not get an IPv6 address from a DHCPv6 Server (you must assign it manually)<br>**Important** - First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*). |
| `mac-addr <MAC Address>` | Configures the hardware MAC address. |

| Parameter | Description |
|---|---|
| `mtu <68-16000 \| 1280-16000>` | Configures the Maximum Transmission Unit size for an interface.<br>For IPv4:<br>■ **Range:** 68 - 16000 bytes<br>■ **Default:** 1500 bytes<br>For IPv6:<br>■ **Range:** 1280 - 16000 bytes<br>■ **Default:** 1500 bytes |
| `rx-ringsize <0-4096>` | Configures the receive buffer size.<br>■ **Range:** 0 - 4096 bytes<br>■ **Default:** Depends on the interface driver |
| `tx-ringsize <0-4096>` | Configures the transmit buffer size.<br>■ **Range:** 0 - 4096 bytes<br>■ **Default:** Depends on the interface driver |

### Example

```
gaia> add bridging group 56 interface eth1
gaia> set interface br1 ipv6-address 3000:40::1 mask-length 64
gaia> show bridging groups
gaia> delete bridging group 56 interface eth1
gaia> delete bridging group 56
```

## Accept, or Drop Ethernet Frames with Specific Protocols

**Important:**

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in the Expert mode on the applicable Security Group.

By default, a Security Gateway, a Cluster, or a Scalable Platform Security Group in Bridge mode *allows* Ethernet frames that carry protocols other than IPv4 (0x0800), IPv6 (0x86DD), or ARP (0x0806) protocols.

Administrator can configure a Security Gateway, a Cluster, or a Scalable Platform Security Group in Bridge Mode to either accept, or drop Ethernet frames that carry specific protocols.

When Access Mode VLAN (VLAN translation) is configured, BPDU frames can arrive with the wrong VLAN number to the switch ports through the Bridge interface. This mismatch can cause the switch ports to enter blocking mode.

In Active/Standby Bridge Mode only, you can disable BPDU forwarding to avoid such blocking mode:

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on the Security Gateway, each Cluster Member, or Scalable Platform Security Group. |
| 2 | Log in to the Expert mode. |
| 3 | Backup the current `/etc/rc.d/init.d/network` file:<br>■ On the Security Gateway / each Cluster Member:<br>`cp -v /etc/rc.d/init.d/network{,_BKP}`<br>■ On the Scalable Platform Security Group:<br>`g_cp -v /etc/rc.d/init.d/network{,_BKP}` |
| 4 | Edit the current `/etc/rc.d/init.d/network` file:<br>`vi /etc/rc.d/init.d/network` |
| 5 | After the line:<br>`./etc/init.d/functions`<br>Add this line:<br>`/sbin/sysctl -w net.bridge.bpdu_forwarding=0` |
| 6 | Save the changes in the file and exit the Vi editor. |

| Step | Instructions |
|---|---|
| 7 | On the Scalable Platform Security Group:<br>Copy the modified file to other Security Group Members:<br>`asg_cp2blades -b all /etc/rc.d/init.d/network` |
| 8 | Reboot.<br>■ On the Security Gateway / each Cluster Member:<br>`reboot`<br>■ On the Scalable Platform Security Group:<br>`g_reboot -a` |
| 9 | Make sure the new configuration is loaded:<br>■ On the Security Gateway / each Cluster Member:<br>`sysctl net.bridge.bpdu_forwarding`<br>■ On the Scalable Platform Security Group:<br>`g_all sysctl net.bridge.bpdu_forwarding`<br>The output must show:<br>`net.bridge.bpdu_forwarding = 0` |

# Loopback Interfaces

*In This Section:*



You can define a virtual loopback interface by assigning an IPv4 or IPv6 address to the `lo` (local) interface.

This can be useful for testing purposes or as a proxy interface for an unnumbered interface.

This section shows you how to configure a loopback interface in the Gaia Portal and Gaia Clish.

## Configuring Loopback Interfaces in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Adding a loopback interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Interface Management** > **Network Interfaces**. |
| 2 | Click **Add** > **Loopback**. |
| 3 | In the **Add loopback** window:<br>1. The **Enable** option is selected by default to set the loopback interface status to UP.<br>2. In the **Comment** field, enter the applicable comment text (up to 100 characters).<br>3. On the **IPv4** tab, enter the IPv4 address and subnet mask.<br>These IPv4 addresses are **not** allowed:<br>■ 0.x.x.x<br>■ 127.x.x.x<br>■ 224.x.x.x - 239.x.x.x (Class D)<br>■ 240.x.x.x - 255.x.x.x (Class E)<br>■ 255.255.255.255<br>4. **Optional:** On the **IPv6** tab, do one of these:<br>■ Select **Obtain IPv6 address automatically via Autoconfig**.<br>■ Select **Obtain IPv6 address automatically via Normal DHCPv6**.<br>■ Select **Obtain IPv6 address automatically via Prefix Delegation**.<br>■ Select **Use the following IPv6 address.**<br>**Important:**<br>■ First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*).<br>■ R82 does **not** support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313).<br>■ On a Multi-Domain Security Management Server, follow these instructions to configure an IPv6 address - *"Configuring an IPv6 Address on a Multi-Domain Server" on page 710*.To configure an IPv6 address on a Multi-Domain Security Management Server, see the *R82 Gaia Administration Guide*.<br>■ Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246). |
| 4 | Click **OK**. |

**Note** - When you add a new loopback interface, Gaia automatically assigns a name in the format "`loop<XX>`", where `XX` is a sequence number that starts from 00. The name of the first loopback interface is *loop00*. The name of the second loopback interface is *loop01*. And so on.

### Configuring a loopback interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Interface Management** > **Network Interfaces**. |
| 2 | Select a loopback interface and click **Edit**. |
| 3 | In the **Edit loop<NN>** window:<br>a. If required, change the IPv4 address and subnet mask.<br>b. If required, change the IPv6 address and mask length. |
| 4 | Click **OK**. |

### Deleting a loopback interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Select a loopback interface and click **Delete**. |
| 3 | Click **OK**, when the confirmation message shows. |

# Configuring Loopback Interfaces in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

## Syntax

### Adding a loopback interface

```
add interface lo loopback <IPv4 Address>/<Mask Length>
```

**Note** - When you add a new loopback interface, Gaia automatically assigns a name in the format "`loop<XX>`", where `XX` is a sequence number that starts from 00. The name of the first loopback interface is *loop00*. The name of the second loopback interface is *loop01*. And so on.

### Configuring a loopback interface

```
set interface <Name of Loopback Interface> {ipv4-address
<options> | ipv6-address <options>}
```

**Note** - You can only change IPv4 or IPv6 address on a loopback interface.

### Viewing a loopback interface

```
show interface<SPACE><TAB>
```

```
show interface <Name of Loopback Interface>
```

### Deleting a loopback interface

```
delete interface lo loopback <Name of Loopback Interface>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| `lo` | You must use the `lo` (local interface) keyword to define a loopback interface |

| Parameter | Description |
|---|---|
| *<IPv4 Address>* | Specifies the IPv4 address<br>These IPv4 addresses are not allowed:<br>■ 0.x.x.x<br>■ 127.x.x.x<br>■ 224.x.x.x - 239.x.x.x (Class D)<br>■ 240.x.x.x - 255.x.x.x (Class E)<br>■ 255.255.255.255 |
| *<Mask Length>* | Configures the IPv4 subnet mask length using the CIDR notation (integer between 2 and 32) |
| *<Name of Loopback Interface>* | Specifies a loopback interface name |

### Example

```
gaia> add interface lo loopback 10.10.99.1/24
gaia> delete interface lo loopback loop01
```

# VPN Tunnel Interfaces

Virtual Tunnel Interface (VTI) is a virtual interface that is used for establishing a Route-Based VPN tunnel. Each peer Security Gateway has one VTI that connects to the VPN tunnel.

The VPN tunnel and its properties are configured by the VPN community that contains the two Security Gateways.

You must configure the VPN community and its member Security Gateways before you can create a VTI.

To learn more about Route Based VPN, see the *R82 Site to Site VPN Administration Guide* > Chapter *Route Based VPN*.

**Note** - The name of a VPN Tunnel interface in Gaia is "`vpnt<VPN Tunnel ID>`". For example, the name of a VPN Tunnel interface with a VPN Tunnel ID of 5 is "*vpnt5*".

**Procedure:**

1. Create and configure the Security Gateways.
2. Enable the IPsec VPN Software Blade in the objects of the applicable Security Gateways.
3. Configure the VPN community in SmartConsole that includes the two peer Security Gateways.

   **Configuring VPN community**

   You must configure the VPN Community and add the member Security Gateways to it before you configure a VPN Tunnel Interface. This section includes the basic procedure for defining a Site-to-Site VPN Community. To learn more about VPN communities and their definition procedures, see the *R82 Site to Site VPN Administration Guide*.

| Step | Instructions |
|---|---|
| 1 | Connect with SmartConsole to the Management Server. |
| 2 | From the left navigation panel, click **Security Policies**. |
| 3 | In the **Access Tools** section, click **VPN Communities**. |
| 4 | From the top toolbar, click the **New** (✳) > select **Star Community** or **Meshed Community**.. |

| Step | Instructions |
|---|---|
| 5 | Configure the VPN community:<br>a. Enter the VPN community name.<br>b. From the left tree, click **Gateways**.<br>Select the applicable Security Gateways.<br>c. From the left tree, click **Encrypted Traffic**.<br>Select **Accept all encrypted traffic**.<br>This automatically adds a rule to encrypt all traffic between Security Gateways in a VPN community.<br>d. Configure other settings as necessary. |
| 6 | Publish the SmartConsole session. |

4. Make Route Based VPN the default option.

   Do this procedure one time for each.

   **Configuring Route Based VPN**

   When Domain Based VPN and Route Based VPN are configured for a Security Gateway, Domain Based VPN is active by default. You must do two short procedures to make sure that Route Based VPN is always active.

   The first procedure configures an empty encryption domain group for your VPN peer Security Gateways. You do this step one time for each Security Management Server. The second step is to make Route Based VPN the default option for all Security Gateways.

   **Configuring an empty group**

| Step | Instructions |
|---|---|
| 1 | In the SmartConsole, click **Objects** menu > **More object types** > **Network Object** > **Group** > **New Network Group**. |
| 2 | Enter a group name. |
| 3 | Do not add members to this group. |
| 4 | Click **OK**. |

   **Configuring the Route Based VPN as the default choice**

   Do these steps for each Security Gateway.

| Step | Instructions |
|---|---|
| 1 | From the left navigation panel, click **Gateways & Servers**. |
| 2 | Double-click the applicable Security Gateway object. |
| 3 | From the left tree, click **Network Management** > **VPN Domain**. |
| 4 | Select **Manually define** and then select the empty **Group** object you created earlier. |
| 5 | Install the Access Control Policy. |

5. Configure the VTI.

   You can configure the VPN Tunnel Interfaces (VTI) in Gaia Portal or Gaia Clish.

   **Configuring VTI in Gaia Portal**

   **Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | In the Gaia Portal, select **Network Management** > **Network Interfaces**. |
| 2 | Click **Add** > **VPN Tunnel**.<br>To configure an existing VTI interface, select the VTI interface and click **Edit**. |

| Step | Instructions |
|---|---|
| 3 | In the **Add/Edit** window, configure these parameters:<br>■ **VPN Tunnel ID** - Unique tunnel name (integer from 1 to 99). Gaia automatically adds the prefix "`vpnt`" to the Tunnel ID (example: `vnpt10`).<br>■ **Remote Peer Name** - Alphanumeric character string as configured for the Remote Peer Name in the VPN community. You must configure the two peers in the VPN community before you can configure the VTI.<br>■ **VPN Tunnel Type** - Select the applicable type:<br>• **Numbered** - Uses a specified, static IPv4 addresses for local and remote connections.<br>• **Unnumbered** - Uses the interface and the remote peer name to get IPv4 addresses.<br>■ **Local Address** - Configures the local peer IPv4 address. Applies to the Numbered VTI only.<br>■ **Remote Address** - Configures the remote peer IPv4 address. Applies to the Numbered VTI only.<br>■ **Physical Device** - Local peer interface name. Applies to the Unnumbered VTI only. |

### Configuring VTI in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

#### Syntax

■ To add a VPN Tunnel Interface (VTI):

```
add vpn tunnel <Tunnel ID>
      type
            numbered local <Local IP address> remote
<Remote IP address> peer <Peer Name>
            unnumbered peer <Peer Name> dev <Name of
Local Interface>
```

■ To see the configuration of the specific VPN Tunnel Interface (VTI):

```
show vpn tunnel <Tunnel ID>
```

■ To see all configured VPN Tunnel Interfaces (VTIs):

```
show vpn tunnels
```

- To delete a VPN Tunnel Interface (VTI):

```
delete vpn tunnel <Tunnel ID>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### CLI Parameters

| Parameter | Description |
|---|---|
| *<Tunnel ID>* | Configures the unique Tunnel ID (integer from 1 to 99).<br>Gaia automatically adds the prefix '`vpnt`' to the Tunnel ID.<br>Example: `vnpt10` |
| `type numbered` | Configures a **numbered** VTI that uses static IPv4 addresses for local and remote connections. |
| `type unnumbered` | Configures an **unnumbered** VTI that uses the interface and the remote peer name to get IPv4 addresses. |
| `local` *<Local IP address>* | Configures the VPN Tunnel IPv4 address in dotted decimal format on this Security Gateway or Cluster Member.<br>Applies to the Numbered VTI only. |
| `remote` *<Remote IP address>* | Configures the VPN Tunnel IPv4 address in dotted decimal format on the VPN peer.<br>Applies to the Numbered VTI only. |
| `peer` *<Peer Name* | Specifies the name of the remote peer object as configured in the VPN community in SmartConsole. |
| `dev` *<Name of Local Interface>* | Specifies the name of the local interface on this Security Gateway or Cluster Member.<br>The new VTI is bound to this local interface.<br>Applies to the Unnumbered VTI only. |

**Example**

```
gaia> add vpn tunnel 20 type numbered local 10.10.10.1
remote 20.20.20.1 peer MyPeer1
gaia>
gaia> add vpn tunnel 10 type unnumbered peer MyPeer2 dev
eth1
gaia>
gaia> show vpn tunnels
  Interface: vpnt20
        Local IP: 10.10.10.1
        Peer Name: MyPeer1
        Remote IP: 20.20.20.1
        Interface type: numbered
  Interface: vpnt10
        Physical device: eth1
        Peer Name: MyPeer2
        Interface type: unnumbered
gaia>
gaia> show vpn tunnel 20
Interface: vpnt20
Local IP: 10.10.10.1
Peer Name: MyPeer1
Remote IP: 20.20.20.1
Interface type: numbered
gaia>
gaia> delete vpn tunnel 20
```

6. Configure Route Based VPN Rules.

**Configuring Route Based VPN Rules**

To make sure that your security rules work correctly with Route Based VPN traffic, you must add directional matching conditions and allow OSPF traffic.

**(A) Defining Directional Matching VPN Rules**

This section contains the procedure for defining directional matching rules.

Directional matching is necessary for Route Based VPN when a VPN community is included in the VPN column in the rule.

This is because without bi-directional matching, the rule only applies to connections between a community and an encryption domain (Domain Based Routing).

| Name | Source | Destination | VPN | Service | Action |
|---|---|---|---|---|---|
| VPN Tunnel | Any | Any | MyIntranet | Any | Accept |

The directional rule must contain these directional matching conditions:

- Community > Community
- Community > Internal_Clear
- Internal_Clear > Community

| Name | Source | Destination | VPN | Service | Action |
|---|---|---|---|---|---|
| VPN Tunnel | Any | Any | MyIntranet > MyIntranet MyIntranet > Internal_Clear Internal_Clear > MyIntranet | Any | Accept |

**Notes:**

- **MyIntranet** is the name of a VPN Community.
- **Internal_Clear** refers to all traffic from IP addresses to and from the specified VPN community.
- It is not necessary to configure bidirectional matching rules if the VPN column contains the value **Any**.

**Enabling the VPN directional matching**

| Step | Instructions |
|---|---|
| 1 | In SmartConsole, click **Menu** > **Global properties**> expand **VPN** > click **Advanced**. |
| 2 | Select the **Enable VPN Directional Match in VPN Column** option and click **OK**. |
| 3 | From the left navigation panel, click **Gateways & Servers**. |

| Step | Instructions |
|---|---|
| 4 | For each VPN member gateway:<br>a. Double-click the Security Gateway object.<br>b. From the left tree, click **Network Management**.<br>c. Click **Get Interfaces** > **Get Interfaces with Topology**.<br>This updates the topology to include the newly configured VTIs.<br>d. Click **Accept**.<br>e. Click **OK**. |

**Configuring a VPN directional matching rule**

| Step | Instructions |
|---|---|
| 1 | From the left navigation panel, click **Security Policies**. |
| 2 | Click **Access Control** > **Policy**. |
| 3 | Right-click the **VPN** cell in the applicable rule and select **Directional Match Condition**. |
| 4 | In the **New Directional Match Condition** window, select the source (**Traffic reaching from**) and destination (**Traffic leaving to**). |
| 5 | Click **OK**. |
| 6 | Repeat Step 3-5 for each set of matching conditions. |
| 7 | Publish the SmartConsole session. |

### (B) Defining Rules to Allow OSPF Traffic

One advantage of Route Based VPN is the fact that you can use dynamic routing protocols to distribute routing information between Security Gateways.

The OSPF (Open Shortest Path First) protocol is commonly used with VTIs.

To learn about configuring OSPF, see the *R82 Gaia Advanced Routing Administration Guide*.

| Step | Instructions |
|---|---|
| 1 | In the Gaia Portal or Gaia Clish, add the applicable VPN Tunnel Interfaces to the OSPF configuration page. |

| Step | Instructions |
|---|---|
| 2 | In SmartConsole, add an Access Control rule that allows traffic to the VPN community (or all communities) that uses the OSPF service: |

| Name | Source | Destination | VPN | Service | Action |
|---|---|---|---|---|---|
| Allow OSPF for a VPN Community | `Any` | `Any` | `MyIntranet` | `ospf` | `Accept` |

7. Install the policy and test.

**Instructions**

You must save your configuration to the database and install policies to the Security Gateways before the VPN can be fully functional.

| Step | Instructions |
|---|---|
| 1 | Publish the SmartConsole session. |
| 2 | Install the Access Control policy on the Security Gateways. |
| 3 | Make sure traffic passes over the VTI tunnel correctly. |

# 6in4 Tunnel Interfaces

*In This Section:*



**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-12823).

This section shows you how to configure 6in4 Tunnel Interfaces in the Gaia Portal and Gaia Clish.

6in4 is a transparent mechanism that transmits IPv6 traffic on existing IPv4 networks.

To do this, 6in4 does these functions:

- Encapsulates IPv6 packets in IPv4 packets for transmission on the IPv4 network.
- Routes traffic between 6in4 and "native" IPv6 networks.

**Important** - Before you can configure 6in4 Tunnel interfaces, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*).

**Note** - The name of an 6in4 interface in Gaia is "`sit_6in4_<Tunnel ID>`". For example, the name of a 6in4 interface with a Tunnel ID of 5 is "*sit_6in4_5*".

# Configuring 6in4 Tunnel Interfaces in Gaia Portal

### Adding a 6in4 Tunnel interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Make sure that the physical interface, on which you add a 6in4 Tunnel interface, has an IPv4 address. |
| 3 | Click **Add** > **6in4 Tunnel**. |
| 4 | In the **Add 6in4 Tunnel** window, select the **Enable** option to set the VLAN interface to UP. |
| 5 | **Optional:** On the **IPv6** tab, do one of these:<br>■ Select **Obtain IPv6 address automatically via Autoconfig**.<br>■ Select **Obtain IPv6 address automatically via Normal DHCPv6**.<br>■ Select **Obtain IPv6 address automatically via Prefix Delegation**.<br>■ Select **Use the following IPv6 address.**<br>**Important:**<br>■ First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*).<br>■ R82 does **not** support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313).<br>■ On a Multi-Domain Security Management Server, follow these instructions to configure an IPv6 address - *"Configuring an IPv6 Address on a Multi-Domain Server" on page 710*.To configure an IPv6 address on a Multi-Domain Security Management Server, see the *R82 Gaia Administration Guide*.<br>■ Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246). |
| 6 | On the **6in4 Tunnel** tab:<br>■ In the **Interface** field, select the applicable physical interface.<br>■ In the **Tunnel ID** field, enter or select the Tunnel ID between 2 and 999999.<br>**Note** - The ID must be unique for every 6in4 tunnel that terminates on this Gaia.<br>■ In the **TTL** field, enter or select the Time-to-Live for the 6in4 packets between 0 and 255.<br>**Note** - This value must be the same on the peers. Default value is 0.<br>■ In the **Remote Address** field, enter the IPv4 address at the remote end of the 6in4 tunnel. |
| 7 | Click **OK**. |

### Editing a VLAN interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Select a VLAN interface and click **Edit**. |
| 3 | On the **IPv6** tab, enter the IPv6 address and mask length.<br>You can optionally select the **Obtain IPv6 address automatically** option. |
| 4 | Click **OK**. |

**Note** - You cannot change the settings on the **6in4 Tunnel** tab. To change these parameters, delete the 6in4 Tunnel interface and then create a new 6in4 Tunnel interface.

### Deleting a 6in4 Tunnel interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Select a 6in4 Tunnel interface and click **Delete**. |
| 3 | Click **OK**, when the confirmation message shows. |

# Configuring 6in4 Tunnel Interfaces in Gaia Clish

**Important** - Make sure that the physical interface, on which you wish to add a 6in4 Tunnel interface, have an IPv4 address.

## Syntax

### Adding a new 6in4 Tunnel interface

```
add interface <Name of Physical Interface> 6in4 <6in4 Tunnel ID>
remote <IPv4 Address on Remote Peer> [ttl <0-255>]
```

### Configuring a 6in4 Tunnel interface

```
set interface sit_6in4_<6in4 Tunnel ID>
      comments "Text"
      ipv6-address <IPv6 Address> mask-length <Mask Length>
      ipv6-autoconfig {on | off}
      mtu <1280-16000>
      state {on | off}
```

**Note** - You cannot change the 6in4 settings (*Name of Physical Interface*, *6in4 Tunnel ID*, *IPv4 Address on Remote Peer*, or *TTL*). To change these parameters, delete the 6in4 Tunnel interface and then create a new 6in4 Tunnel interface.

### Viewing the configuration of a specific 6in4 Tunnel interface

```
show interface sit_6in4_<6in4 Tunnel ID><SPACE><TAB>
```

### Deleting a 6in4 Tunnel interface

```
delete interface sit_6in4_<6in4 Tunnel ID> 6in4 <6in4 Tunnel ID>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| *<Name of Physical Interface>* | Specifies a physical interface. |
| *<6in4 Tunnel ID>* | Specifies the Tunnel ID between 2 and 999999.<br>**Note** - The ID must be unique for every 6in4 tunnel that terminates on this Gaia. |

| Parameter | Description |
|---|---|
| `<IPv4 Address on Remote Peer>` | Specifies the IPv4 address at the remote end of the 6in4 tunnel. |
| `ttl <0-255>` | Specifies the Time-to-Live for the 6in4 packets between 2 and 255.<br>**Note** - This value must be the same on the peers. Default value is 0. |
| `comments "Text"` | Defines the optional comment.<br>■ Write the text in double quotes.<br>■ Text must be up to 100 characters.<br>■ This comment appears in the Gaia Portal and in the output of the "`show configuration`" command. |
| `<IPv6 Address>` | Assigns the IPv6 address. |
| `mask-length <Mask Length>` | Configures the IPv6 subnet mask length using CIDR notation (/xx) - integer between 1 and 128. |
| `ipv6-autoconfig {on \| off}` | Configures if this interface gets an IPv6 address from a DHCPv6 Server:<br>■ `on` - Gets an IPv6 address from a DHCPv6 Server<br>■ `off` - Does not get an IPv6 address from a DHCPv6 Server (you must assign it manually) |
| `mtu <1280-16000>` | Configures the Maximum Transmission Unit size for an interface.<br>■ **Range:** 1280 - 16000 bytes<br>■ **Default:** 1500 bytes |
| `state {on \| off}` | Configures interface's state:<br>■ `on` - Enabled<br>■ `off` - Disabled |

**Example**

```
gaia> add interface eth0 6in4 55 remote 192.168.20.30 ttl 200
gaia> set interface comments "6in4 ID 55 with peer
192.168.20.30"
gaia> delete interface sit_6in4_55 6in4 55
```

# PPPoE Interfaces

*In This Section:*



This section shows you how to configure PPPoE Interfaces in the Gaia Portal and Gaia Clish.

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames.

PPPoE is used mainly with DSL services, where individual users connect to the DSL modem over Ethernet and in plain Ethernet networks.

**Notes:**

- The name of a PPPoE interface in Gaia is "`pppoe<`*`Tunnel ID`*`>`". For example, the name of a PPPoE interface with a Tunnel ID of 5 is "*pppoe5*".
- Check Point cluster does not support this interface as a cluster interface.
- Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature.

# Configuring PPPoE Interfaces in Gaia Portal

### Adding a PPPoE interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Make sure that the physical interface, on which you add a PPPoE interface, does not have an IP address. |
| 3 | Click **Add** > **PPPoE**. |
| 4 | In the **Add PPPoE** window, select the **Enable** option to set the PPPoE interface to UP. |
| 5 | On the **PPPoE** tab:<br>■ In the **PPPoE ID** field, enter or select the ID between 0 and 999.<br>**Note** - This ID must be unique for every PPPoE interface.<br>■ In the **Interface** field, select the applicable physical interface.<br>Gaia uses this interface to forward PPPoE frames.<br>■ In the **User Name** field, enter the username needed to connect to the PPPoE server at the Internet Service Provider (ISP). Get it from the ISP.<br>■ In the **Password** field, enter the password needed to connect to the PPPoE server at the Internet Service Provider (ISP). Get it from the ISP.<br>■ **Optional:** Select **Use Peer DNS** to allow the ISP to define the IPv4 DNS server for the Gaia. The ISP supplies either one IPv4 DNS server (the Primary) or two (Primary and Secondary).<br>**Important** - If you select this option, the PPPoE Peer DNS servers overwrite the IPv4 DNS servers configured in **Network Management > Hosts and DNS**.<br>■ **Optional:** Select **Use Peer as Default Gateway** to make the ISP server the Default Gateway for the Gaia.<br>**Important** - If you select this option, Gaia does not use anymore the Default Gateway configured in **Network Management > IPv4 Static Routes**. |
| 9 | Click **OK**. |

### Editing a PPPoE interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Select a PPPoE interface and click **Edit**. |

| Step | Instructions |
|---|---|
| 3 | Configure the applicable settings. |
| 4 | Click **OK**. |

**Note** - You cannot change the PPPoE ID for an existing PPPoE interface. To change this ID, delete the PPPoE interface and then create a new PPPoE interface.

### Deleting a PPPoE interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Select a PPPoE interface and click **Delete**. |
| 3 | Click **OK**, when the confirmation message shows. |

# Configuring PPPoE Interfaces in Gaia Clish

**Important** - Make sure that the physical interface, on which you wish to add a VLAN interface, does **not** have an IP address.

## Syntax

### Adding a new VLAN interface

```
add pppoe client id <PPPoE ID> interface <Name of Physical
Interface> user-name <PPPoE Username> {password <PPPoE Password>
| password_hash <PPPoE Password Hash>} [use-peer-dns {on | off}]
[use-peer-as-default-gateway {on | off}]
```

### Configuring a VLAN interface

```
set pppoe client id <PPPoE ID>
      fake-peer-address <IPv4 Address>
      interface <Name of Physical Interface>
      password <PPPoE Password>
      use-fake-peer-address {on | off}
      use-peer-as-default-gateway {on | off}
      use-peer-dns {on | off}
      user-name <PPPoE Username>
```

**Note** - You cannot change the PPPoE ID for an existing PPPoE interface. To change this parameters, delete the PPPoE interface and then create a new PPPoE interface.

### Viewing the PPPoE configuration

```
show configuration pppoe
```

```
show pppoe client id<SPACE><TAB>
show pppoe client id <PPPoE ID>
```

### Deleting a VLAN interface

```
delete pppoe client id <PPPoE ID>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| `id <PPPoE ID>` | Specifies the ID between 0 and 999.<br>**Note** - This ID must be unique for every PPPoE interface. |
| `interface <Name of Physical Interface>` | Specifies a local physical interface.<br>Gaia uses this interface to forward PPPoE frames. |
| `user-name <PPPoE Username>` | Specifies the username needed to connect to the PPPoE server at the Internet Service Provider (ISP). Get it from the ISP. |
| `password <PPPoE Password>` | Specifies the password needed to connect to the PPPoE server at the Internet Service Provider (ISP). Get it from the ISP. |
| `password_hash <PPPoE Password Hash>` | Specifies the hash of the password needed to connect to the PPPoE server at the Internet Service Provider (ISP). Get it from the ISP. |
| `use-peer-dns {on \| off}` | **Optional:** Specifies whether to allow the ISP to define the IPv4 DNS server for the Gaia. The ISP supplies either one IPv4 DNS server (the Primary) or two (Primary and Secondary).<br>■ `on` - Allow<br>■ `off` - Do not allow<br>**Important** - If you enable this option, the PPPoE Peer DNS servers overwrite the IPv4 DNS servers configured with the "`set dns`" command. |
| `use-peer-as-default-gateway {on \| off}` | **Optional:** Specifies whether to make the ISP server the Default Gateway for the Gaia<br>■ `on` - Allow<br>■ `off` - Do not allow<br>**Important** - If you enable this option, Gaia does not use anymore the Default Gateway configured with the "`set static-route default`" command. |

| Parameter | Description |
|---|---|
| `fake-peer-address <IPv4 Address>` | **Optional.** Configures the fake unicast peer IPv4 address (the default value is 0.0.0.0). |
| `use-fake-peer-address {on \| off}` | **Optional.** Configures whether to use the configured fake peer IPv4 address:<br>■ `on` - Enabled<br>■ `off` - Disabled |

**Example**

```
gaia> add pppoe client id 1 interface eth0 user-name JohnDoe
password 123456 use-peer-dns on
```

# GRE Interfaces

*In This Section:*



**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation PMTR-60868).

This section shows you how to configure a GRE Interface in the Gaia Portal and the Gaia Clish.

Generic Routing Encapsulation (GRE) is an IP encapsulation protocol, which is used to transport IP packets over a network.

GRE allows routing of IP packets between private IPv4 networks, which are separated over public IPv4 Internet.

**Notes:**

- The name of a GRE interface in Gaia OS is "`gre<`*`ID`*`>`".
  For example, the name of a GRE interface with a GRE ID of 5 is "*gre5*".
- The GRE tunnel is not secure, because it is not encrypted.
- By default, Gaia OS loads the GRE kernel driver.
  Therefore, Gaia OS has interfaces "`gre0`", "`gretap0`", and "`erspan0`" in the administratively down state.

For additional information, see sk169794.

# Configuring GRE Interfaces in Gaia Portal

### Adding a GRE interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Click **Add** > **GRE**. |
| 3 | On the **IPv4** tab, enter the local IPv4 address and subnet mask for the GRE interface. |
| 4 | On the **GRE Tunnel** tab:<br>a. In the **GRE Interface ID** field, enter or select the GRE Tunnel ID between 1 and 1024.<br>b. In the **Peer Address** field, enter the IPv4 address for the GRE interface on the remote GRE peer.<br>c. In the **Local Address** field, enter the IPv4 address of the applicable local physical interface.<br>d. In the **Remote Address** field, enter the IPv4 address of the applicable physical interface on the remote GRE peer.<br>e. In the **TTL** field, enter or select the Time-to-Live for the GRE packets between 0 and 255.<br>**Note** - This value must be the same on the GRE peers. |
| 5 | Click **OK**. |

### Example

Security Gateway "GW1" and Security Gateway "GW2" create a GRE Tunnel over a network.

[GW1] (physical interface `eth1`) (GRE Tunnel configuration) <==>
<==> (network) <==>
<==> (GRE Tunnel configuration) (physical interface `eth2` [GW2]

The GRE interface configuration on these GRE peers:

| Setting | Security Gateway "GW1" | Security Gateway "GW2" |
|---|---|---|
| Local physical interface | `eth1` with IPv4 10.10.10.11 / 24 | `eth2` with IPv4 172.30.40.22 / 24 |
| (GRE) IPv4 Address | 192.168.10.11 / 24 | 192.168.10.22 / 24 |
| GRE Interface ID | 33 | 33 |
| Peer Address | 192.168.10.22 | 192.168.10.11 |
| Remote Address | 172.30.40.22 | 10.10.10.11 |

## Editing a GRE interface

**Important** - It is not supported to edit the settings of an existing GRE interface. You must delete the existing GRE interface and create a new GRE interface.

## Deleting a GRE interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | Select a GRE interface and click **Delete**. |
| 3 | Click **OK** to confirm. |

# Configuring GRE interfaces in Gaia Clish

## Syntax

### Adding a GRE interface

```
add gre id <GRE Tunnel ID> local <IPv4 address of local physical interface> remote <IPv4 address of physical interface on remote peer> ttl <TTL> ip <IPv4 address of local GRE interface> mask <IPv4 subnet mask of local GRE interface> peer <IPv4 address of GRE interface on remote peer>
```

### Viewing the configured GRE interface

```
show configuration gre
```

```
show gre id <GRE Tunnel ID>
```

### Editing a GRE interface

**Important** - It is not supported to edit the settings of an existing GRE interface. You must delete the existing GRE interface and create a new GRE interface.

### Deleting a GRE interface

```
delete gre id <GRE Tunnel ID>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### CLI Parameters

| Parameter | Description |
|---|---|
| `id <GRE Tunnel ID>` | Specifies the GRE Tunnel ID between 1 and 1024. |
| `remote <IPv4 address of physical interface on remote peer>` | Specifies the IPv4 address of the applicable physical interface on the remote GRE peer. |
| `ttl <TTL>` | Specifies the Time-to-Live for the GRE packets between 1 and 255.<br>**Note** - This value must be the same on the GRE peers. |
| `ip <IPv4 address of local GRE interface>` | Specifies the local IPv4 address for the GRE interface. |
| `mask <IPv4 subnet mask of local GRE interface>` | Specifies the local IPv4 subnet mask for the GRE interface. |
| `peer <IPv4 address of GRE interface on remote peer>` | Specifies the IPv4 address for the GRE interface on the remote GRE peer. |

### Example

Security Gateway "GW1" and Security Gateway "GW2" create a GRE Tunnel over a network.

[GW1] (physical interface `eth1`) (GRE Tunnel configuration) <==>
<==> (network) <==>
<==> (GRE Tunnel configuration) (physical interface `eth2` [GW2]

The GRE interface configuration on these GRE peers:

| Setting | Security Gateway "GW1" | Security Gateway "GW2" |
|---|---|---|
| Local physical interface | `eth1` with IPv4 10.10.10.11 / 24 | `eth2` with IPv4 172.30.40.22 / 24 |
| (GRE) IPv4 Address | 192.168.10.11 / 24 | 192.168.10.22 / 24 |
| GRE Interface ID | 33 | 33 |
| Peer Address | 192.168.10.22 | 192.168.10.11 |
| Remote Address | 172.30.40.22 | 10.10.10.11 |

The GRE interface configuration on the Security Gateway "GW1":

```
gaia1> add gre id 33 remote 172.30.40.22 ttl <1-255> ip
192.168.10.11 mask 255.255.255.0 peer 192.168.10.22
```

The GRE interface configuration on the Security Gateway "GW2":

```
gaia2> add gre id 33 remote 10.10.10.11 ttl <1-255> ip
192.168.10.22 mask 255.255.255.0 peer 192.168.10.11
```

## Configuring GRE Interfaces on Cluster Members

For more information, see the *R82 ClusterXL Administration Guide*.

In Cluster, you have these options:

**Using a GRE interface as a cluster interface with a Virtual IP address**

1. Configure a GRE interface on all the Cluster Members.

   You must configure the *same* **GRE Interface ID** and **Remote Address** on each Cluster Member.
2. Connect with SmartConsole to the Management Server.
3. From the left navigation panel, click **Gateways & Servers**.
4. Double-click the cluster object.
5. From the left tree, click **Network Management**.
6. From the toolbar, click **Get Interfaces** > **Get Interfaces With Topology** and confirm.

   Make sure you see the new GRE interface from each Cluster Member.
7. Select the new GRE interface and click **Edit**.
8. From the left tree, click the **General** page.
9. In the **General** section, in the **Network Type** field, select **Cluster**.
10. In the **IPv4** field, configure the applicable cluster Virtual IP address.
11. In the **Member IPs** section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.
12. Click **OK**.
13. Publish the SmartConsole session.
14. Install the Access Control Policy on this cluster object.

**Using a GRE interface only on a specific Cluster Member**

1. Configure a GRE interface on a specific Cluster Member.
2. Connect with SmartConsole to the Management Server.
3. From the left navigation panel, click **Gateways & Servers**.
4. Double-click the cluster object.
5. From the left tree, click **Network Management**.
6. From the toolbar, click **Get Interfaces** > **Get Interfaces With Topology** and confirm.

Make sure you see the new GRE interface from the specific Cluster Member, on which you configured it.

7. Select the new GRE interface and click **Edit**.
8. From the left tree, click the **General** page.
9. In the **General** section, in the **Network Type** field, select **Private**.
10. Click **OK**.
11. Publish the SmartConsole session.
12. Install the Access Control Policy on this cluster object.

# Gaia Management Interface

This section shows you how to select the Gaia Management Interface.

This is the main interface, through which you connect to Gaia Operating System.

**Note** - You selected this interfaces during the Gaia First Time Configuration Wizard.

## Selecting Management Interface in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

**Procedure**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **Network Interfaces**. |
| 2 | In the section **Management Interface**, click **Set Management Interface**.<br>You can see the name of the current Management Interface above this button. |
| 3 | In the **Management Interface** field, select an interface. |
| 4 | Click **OK**. |

# Selecting Management Interface in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

## Syntax

### Viewing the current interface

```
show management interface
```

### Selecting a new interface

```
set management interface <Name of Interface>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| *<Name of Interface>* | Specifies the name of the interface, on which to create an alias IPv4 address |

### Example

```
gaia> show management interface
gaia> set management interface eth2
```

# Detection of IP Address Conflicts

From R81, the Gaia Operating System detects IPv4 address conflicts - if a different device on a directly connected network uses an IPv4 address that belongs to one of the Gaia interfaces.

Example: Gaia interface `eth1` has the IPv4 address 10.1.1.1, and some other device on the network connected to `eth1` uses the same IPv4 address 10.1.1.1. The device causes an IP address conflict.

**Important** - The detection of IP address conflicts:

- Is disabled by default.
- Supports only IPv4 addresses.
- Supports only interfaces with an assigned IPv4 address and with the state "on" ("enabled").
- Is configured only in Gaia Clish.

## Configuration in Gaia Clish

**Important:**

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

### Syntax

#### Viewing the current configuration

```
show ip-conflicts-monitor
      interfaces
      state
```

#### Configuring settings

```
set ip-conflicts-monitor
      interface {all | <Name of Interface>}
      state {off | on}
```

#### Removing the current configuration

```
delete ip-conflicts-monitor
      interface {all | <Name of Interface>}
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Parameters

#### CLI Parameters

| Command | Description |
|---|---|
| `set ip-conflicts-monitor interface {all \| <Name of Interface>}` | Specifies the interfaces, on which Gaia monitors for :<br>■ `all`<br>Detect IP address conflicts (duplicate IP addresses) on all supported interfaces<br>■ *<Name of Interface>*<br>Detect IP address conflicts on the specified interface only<br>You can run this command for each applicable interface<br>**Best Practice** - Enable this feature only for interfaces connected to your internal networks. If you enable this feature for all interfaces, or for interfaces connected to external networks, this feature generates too many log messages in the `/var/log/messages` file. |
| `set ip-conflicts-monitor state {off \| on}` | Enables (`on`) and disables (`off`) the feature. |
| `show ip-conflicts-monitor interfaces` | Shows the interfaces, on which Gaia detects IP address conflicts. |
| `show ip-conflicts-monitor state` | Shows the current state of the feature (`off` or `on`). |
| `delete ip-conflicts-monitor interfaces {all \| <Name of Interface>}` | Specifies the interfaces, on which Gaia stops to detect IP address conflicts:<br>■ `all`<br>Stop to detect IP address conflicts on all supported interfaces<br>■ *<Name of Interface>*<br>Stop to detect IP address conflicts on the specified interfaces only |

**Example**

```
gaia> show ip-conflicts-monitor state
IP conflict monitoring Disabled
gaia> set ip-conflicts-monitor interface eth2
gaia> set ip-conflicts-monitor on
gaia> show ip-conflicts-monitor state
IP conflict monitoring Enabled
gaia> show ip-conflicts-monitor interfaces
Monitored Interfaces: eth2
```

## Log Messages

After you enable and configure this feature, it generates one of these messages in the `/var/log/messages` file:

| Log Message | Description |
|---|---|
| `new station` | Gaia detected a new MAC address on a directly connected network and a new IP address is assigned to that MAC address. |
| `changed ethernet address` | Gaia detected that an IP address stored in the binding database is assigned to a new MAC address on a directly connected network. |
| `flip flop` | The second recent binding of a MAC address to an IP address is currently the most recent binding in the binding database.<br>This potentially indicates an IP address conflict on the network. |
| `reused old ethernet address` | The third (or older) recent binding of a MAC address to an IP address is currently the most recent binding in the binding database.<br>This very likely indicates a 3-way (or greater) IP address conflict. |

To see the applicable log messages:

| Step | Instructions |
|---|---|
| 1 | Connect to the command line. |
| 2 | Log in to the Expert mode. |
| 3 | Run:<br>`grep "arpwatch:" /var/log/messages*` |

Example:

```
[Expert@MyGaia:0]# grep "arpwatch:" /var/log/messages*
Aug  3 19:23:16 2020 MyGaia arpwatch: listening on eth0
Aug  3 19:23:16 2020 MyGaia arpwatch: new station 192.168.3.51
00:50:56:a3:73:26
Aug  3 19:23:17 2020 MyGaia arpwatch: new station 192.168.3.29
00:50:56:a3:68:60
... ... (truncated for brevity) ... ...
[Expert@MyGaia:0]#
```

## Additional Information

- The detection of IP address conflicts is based on the Linux arpwatch tool.
- When you enable this feature, Gaia runs the `/bin/arpwatch_launcher` daemon. This daemon is responsible to run the `/etc/rc.d/init.d/arpwatch` service.
- Gaia saves the applicable configuration in the Gaia database and in the `/etc/sysconfig/arpwatch` file.

  Gaia generates the `/etc/sysconfig/arpwatch` file automatically.
- Gaia saves the MAC-to-IP address binding information in the `/var/lib/arpwatch/arp.dat.<*Name of Interface*>` file.

  The information includes:

  - The detected MAC address
  - The IP address assigned to that MAC address
  - The time of detection (in Unix epoch format)

  It can take several minutes for Gaia to populate this database.

# Interface Link Status

You can see the status of physical and logical interfaces in Gaia Portal or Gaia Clish.

**Important:**

- On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.
- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

### To see interface status in Gaia Portal:

1. In the navigation tree, click **Network Management** > **Network Interfaces**.
2. Double-click an interface to see its parameters.

| Link Status | Description |
|---|---|
| Down (gray) | The physical interface is disabled (down). |
| No link (red) | The physical interface is enabled (up), but Gaia cannot find a network connection. |
| Up (green) | The physical interface is enabled (up) and connected to the network. |

### To see interface status in Gaia Clish:

Run one of these commands:

```
show interfaces all
show interface <Name of Interface>
```

# CLI Reference (interface)

This section summarizes the Gaia Clish "`interface`" command and its parameters.

**Note** - There are some command options and parameters that you cannot configure in the Gaia Portal.

**Important:**

- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Description

Add, configure, and delete interfaces and interface properties.

## Syntax

### Adding an interface

```
add interface<ESC><ESC>
```

### Configuring an interface

```
set interface<ESC><ESC>
```

### Viewing an interface configuration

```
show interface<SPACE><TAB>
show interfaces all
```

### Deleting an interface, or interface configuration

```
delete interface<ESC><ESC>
```

### Working with Gaia Management Interface

```
show management interface
set management interface <Name of Interface>
```

### Working with Gaia IP Conflict Detection

```
show ip-collisions-monitor
set ip-collisions-monitor
delete ip-collisions-monitor
```

# ARP

The Address Resolution Protocol (ARP) allows a host to find the physical address of a target host on the same physical network using only the target's IP address.

ARP is a low-level protocol that hides the underlying network physical addressing and permits assignment of an arbitrary IP address to every machine.

ARP is considered part of the physical network system and not as part of the Internet protocols.

# Configuring ARP in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Viewing dynamic ARP entries

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **ARP**. |
| 2 | In the upper right corner, click the **Monitoring** tab. |

### Viewing static ARP entries

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **ARP**. |
| 2 | In the upper right corner, click the **Configuration** tab. |

### Changing static and dynamic ARP parameters

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **ARP**. |
| 2 | In the upper right corner, click the **Configuration** tab. |
| 3 | In the **ARP Table Settings** section:<br>a. Enter the **Maximum Entries**.<br>This is the maximum number of entries in the ARP cache.<br>**Range:** 1024 - 131072 entries<br>**Default:** 4096 entries<br>**Note** - Make sure to configure a value large enough to accommodate at least 100 dynamic entries, in addition to the maximum number of static entries.<br>b. Enter the **Validity Timeout**.<br>This is the time, in seconds, resolved dynamic ARP entries are checked for validity.<br>If the entry is not referred to and is not used by traffic before the time elapses, it is marked as STALE.<br>Otherwise, a request is sent to verify the MAC address.<br>**Range:** 60 - 86400 seconds (24 hours)<br>**Default:** 60 seconds |

### Adding a static ARP entry

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **ARP**. |
| 2 | In the upper right corner, click the **Configuration** tab. |
| 3 | In the **Static ARP Entries** section, click **Add**. |
| 4 | Enter the **IP Address** of the static ARP entry and the **MAC Address** used when forwarding packets to the IP address. |
| 5 | Click **OK**. |

### Deleting a static ARP entry

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **ARP**. |
| 2 | In the upper right corner, click the **Configuration** tab. |
| 3 | In the **Static ARP Entries** section, select a Static ARP entry. |
| 4 | Click **Remove**. |

### Deleting all dynamic ARP entries

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **ARP**. |
| 2 | In the upper right corner, click the **Monitoring** tab. |
| 3 | Click **Flush All**. |

# Configuring ARP in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

**Note** - For Scalable Platforms (Maestro and Chassis), also refer to the "`asg_arp`" command in Gaia gClish. See the *R82 Scalable Platforms Administration Guide*.

## Syntax

### Adding a static ARP entry

```
add arp static ipv4-address <IPv4 Address> macaddress <MAC
Address>
```

### Deleting static and dynamic ARP entries

```
delete arp
      dynamic all
      static ipv4-address <IPv4 Address>
```

### Configuring ARP table parameters

```
set arp table
      validity-timeout <Seconds>
      cache-size <Number of Entries>
```

### Viewing ARP table parameters

```
show arp
      dynamic all
      static all
      table validity-timeout
      table cache-size
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| `static` | Configures static ARP entries. |
| `dynamic` | Configures dynamic ARP entries. |

| Parameter | Description |
|---|---|
| `ipv4-address <IPv4 Address>` | Configures IPv4 Address for a static ARP entry.<br>■ **Range:** Dotted-quad ([0-255].[0-255].[0-255].[0-255])<br>■ **Default:** No default value |
| `macaddress` | Configures the hardware MAC address (six hexadecimal octets separated by colons) for a static ARP entry.<br>■ **Range:** 00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF<br>■ **Default:** No default value |
| `table validity-timeout <Seconds>` | Configures the time, in seconds, resolved dynamic ARP entries in the ARP cache table are checked for validity.<br>If the entry is not referred to and is not used by traffic before this time elapses, the dynamic ARP entry is marked as STALE.<br>Otherwise, an ARP Request will be sent to verify the MAC address.<br>■ **Range:** 60 - 86400 seconds (24 hours)<br>■ **Default:** 60 seconds |
| `table cache-size <Number of Entries>` | Configures the maximum number of entries in the ARP cache table.<br>■ **Range:** 1024 - 131072<br>■ **Default:** 4096<br>**Note** - Make sure to configure a value large enough to accommodate at least 100 dynamic ARP entries, in addition to the maximum number of static ARP entries. |

# DHCP Server

**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246).

You can configure the Gaia device to be a Dynamic Host Configuration Protocol (DHCP) server.

The DHCP server gives IP addresses and other network parameters to network hosts.

DHCP makes it unnecessary to configure each host manually, and therefore reduces configuration errors.

You configure DHCP server subnets on the Gaia device interfaces.

A DHCP subnet allocates these network parameters to *hosts* behind the Gaia interface:

- IPv4 address
- Default Gateway (optional)
- DNS parameters (optional):
  - Domain name
  - Primary, secondary and tertiary DNS servers

Allocating DHCP parameters to hosts (for the details, see the next section)

### Workflow

| Step | Instructions |
|---|---|
| 1 | To define a DHCP subnet on a Gaia interface:<br>a. Enable DHCP Server on the Gaia network interface.<br>b. Define the network IPv4 address of the subnet on the interface.<br>c. Define an IPv4 address pool.<br>d. **Optional:** Define routing and DNS parameters for DHCP hosts. |
| 2 | Define additional DHCP subnets on other Gaia interfaces, as needed. |
| 3 | Enable the DHCP Server process for all configured subnets. |
| 4 | Configure the network hosts to use the Gaia DHCP server. |

# Configuring a DHCP Server in Gaia Portal

**Important**:

- Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246).
- Starting in R81.20, you can configure DHCP Server setting in the context of a VSX Virtual System. See *"Configuring a DHCP Server in Gaia Clish" on page 232*.

**Allocating DHCP parameters to hosts**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **DHCP Server**. |
| 2 | In the **DHCP Server Subnet Configuration** section, click **Add**.<br>The **Add DHCP** window opens.<br>You now define a DHCP subnet on an Ethernet interface of the Gaia device. Hosts behind the Gaia interface get IPv4 addresses from address pools in the subnet. |
| 3 | Select **Enable DHCP** to enable DHCP for the subnet you will configure. |
| 4 | On the **Subnet** tab:<br>Define the DHCP offer and lease settings: |
| 4A | In the **Network IP Address** field, enter the IPv4 address of the applicable interface's subnet.<br>In the **Subnet mask** field, enter the subnet mask.<br>**Note** - To do this automatically, click **Get from interface** and select the applicable interface. Click **OK**. |
| 4B | **Optional:**<br>In the **Address Pool** section, click **Add** to define the range of IPv4 addresses that the server assigns to hosts.<br>a. In the **Type** field, select **Include** or **Exclude**.<br>This specifies whether to include or exclude this range of IPv4 addresses in the IP pool.<br>b. In the **Status** field, select **Enable** of **Disable**.<br>This enables or disables the DHCP Server for this subnet, or the DHCP Server process (depending on the context).<br>c. In the **Start** field, enter the first IPv4 address of the range.<br>d. In the **End** field, enter the last IPv4 address of the range.<br>e. Click **OK**. |

| Step | Instructions |
|---|---|
| 4C | **Optional:**<br>In the **Lease Configuration** section, configure the DHCP lease settings:<br>a. In the **Default lease** field, enter the default lease time for all IPv4 address in this IPv4 subnet.<br>This applies only if DHCPv4 clients do not request a unique lease time.<br>The default value in this field is 43,200 seconds.<br>Valid values in this field are from 1 to the Maximum lease time.<br>b. In the **Maximum lease** field, enter the maximum lease time for all IPv4 address in this IPv4 subnet.<br>The default value in this field is 86,400 seconds.<br>Valid values in this field are from 1 to 4,294,967,295 seconds. |
| 5 | **Optional:**<br>On the **Routing & DNS** tab, define routing and DNS parameters for DHCP clients:<br>■ In the **Default Gateway** field, enter the IPv4 address of the default gateway for the DHCP clients.<br>■ In the **Domain Name** field, enter the domain name for the DHCP clients (for example, `example.com`).<br>■ In the **Primary DNS Server** field, enter the IPv4 address of the Primary DNS server for the DHCP clients.<br>■ In the **Secondary DNS Server** field, enter the IPv4 address of the Secondary DNS server for the DHCP clients (to use if the primary DNS server does not respond).<br>■ In the **Tertiary DNS Server** field, enter the IPv4 address of the Tertiary DNS server for the DHCP clients (to use if the primary and secondary DNS servers do not respond). |
| 6 | Click **OK**. |
| 7 | **Optional:** Define DHCP subnets on other Gaia interfaces, as needed. |
| 8 | In the **DHCP Server Configuration** section, select **Enable DHCP Server** and click **Apply**. |
| 9 | The DHCP server on Gaia is now configured and enabled.<br>You can now configure your network hosts to get their network parameters from the DHCP server on Gaia. |

### Changing the DHCP parameters in a subnet

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **DHCP Server**. |
| 2 | In the **DHCP Server Subnet Configuration** section, select the Subnet and click **Edit**. |
| 3 | Change the applicable settings. |
| 4 | Click **OK**. |

### Disabling DHCP server on all interfaces

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **DHCP Server**. |
| 2 | In the **DHCP Server Configuration** section, clear the **Enable DHCP Server**. |
| 3 | Click **Apply**. |

### Deleting DHCP subnet

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **DHCP Server**. |
| 2 | In the **DHCP Server Subnet Configuration** section, select the Subnet and click **Delete**. |
| 3 | Click **OK** to confirm. |

**Note** - Before you delete the last DHCP subnet, you must disable DHCP server on all interfaces.

# Configuring a DHCP Server in Gaia Clish

**Important:**

- Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246).
- On a VSX Gateway / each VSX Cluster Member, you must run these commands in the context of the applicable Virtual System (`set virtual-system <VS ID>`).

## Syntax

### Enabling or disabling the DHCP Server process

```
set dhcp server {enable | disable}
```

### DHCPv4 'add' commands

```
add dhcp server subnet <Subnet IPv4 Address>
      netmask <IPv4 Subnet Mask Length>
      exclude-ip-pool start <First IPv4 Address> end <Last IPv4
Address>
      include-ip-pool start <First IPv4 Address> end <Last IPv4
Address>
```

### DHCPv4 'set' commands

```
set dhcp server subnet <Subnet IPv4 Address>
      {enable | disable}
      exclude-ip-pool <First IPv4 Address-Last IPv4 Address>
{enable | disable}
      include-ip-pool <First IPv4 Address-Last IPv4 Address>
{enable | disable}
      default-lease <Lease in Seconds>
      max-lease <Maximum Lease in Seconds>
      default-gateway <IPv4 Address of Default Gateway>
      dns "<DNS Server 1>, <DNS Server 2>, <DNS Server 3>"
      domain <Domain Name>
```

### DHCPv4 'delete' commands

```
delete dhcp server subnet <Subnet IPv4 Address>
      exclude-ip-pool <First IPv4 Address-Last IPv4 Address>
      include-ip-pool <First IPv4 Address-Last IPv4 Address>
```

### DHCPv4 'show' commands

```
show dhcp server
      all
      status
      subnet <Subnet IPv4 Address> [ip-pools]
      subnets
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| `subnet <Subnet IPv4 Address>` | Specifies the IPv4 address of the DHCP subnet on an Ethernet interface of the Gaia device.<br>Hosts behind the Gaia interface get IPv4 addresses from address pools in the subnet.<br>For example: `192.0.2.0` |
| `netmask <IPv4 Subnet Mask Length>` | Specifies the IPv4 subnet mask length.<br>For example: `24` |
| `include-ip-pool start <First IPv4 Address> end <Last IPv4 Address>` | Specifies the IPv4 address that starts and the IPv4 address that ends the included allocated IP Pool range.<br>For example: `192.0.2.20` and `192.0.2.90` |
| `exclude-ip-pool start <First IPv4 Address> end <Last IPv4 Address>` | Specifies the IPv4 address that starts and the IPv4 address that ends the excluded allocated IP Pool range.<br>For example: `192.0.2.155` and `192.0.2.254` |
| `include-ip-pool <First IPv4 Address-Last IPv4 Address>` | Specifies the range of IPv4 addresses to include in the IP pool.<br>For example: `192.0.2.20-192.0.2.90` |
| `exclude-ip-pool <First IPv4 Address-Last IPv4 Address>` | Specifies the range of IPv4 addresses to exclude from the IP pool.<br>For example: `192.0.2.155-192.0.2.254` |
| `set dhcp server {enable \| disable}` | Enables or disables the DHCP Server subnet, or the DHCP Server process (depending on the context). |

| Parameter | Description |
|---|---|
| `default-lease <Lease in Seconds>` | Specifies the default DHCP lease in seconds, for host IPv4 addresses.<br>Applies only if DHCP clients do not request a unique lease time.<br>Range: 1 - 4294967295<br>Default: 43200 |
| `max-lease <Maximum Lease in Seconds>` | Specifies the maximum DHCP lease in seconds, for host IPv4 addresses.<br>Range: 1 - 4294967295<br>Default: 86400 |
| `default-gateway <IPv4 Address of Default Gateway>` | Optional. Specifies the IPv4 address of the default gateway for the network hosts |
| `domain <Domain Name>` | Optional. Specifies the domain name for DHCPv4 Clients.<br>For example: `example.com` |
| `dns "<DNS Server 1>, <DNS Server 2>, <DNS Server 3>"` | Optional. Specifies the IPv4 addresses of DNS servers that the network hosts will use to resolve hostnames. Optionally, specify a primary, secondary, and tertiary server in the order of precedence.<br>For example: `dns "192.0.2.101, 192.0.2.102, 192.0.2.103"` |
| `show dhcp server` | Shows the DHCPv6 Server settings:<br>■ `all`<br>Shows all DHCPv4 Server settings.<br>■ `status`<br>Shows the DHCPv4 Server status (enabled / disabled).<br>■ `subnet <Subnet IPv4 Address> [ip-pools]`<br>Shows the DHCPv4 settings for the specified subnet.<br>■ `subnets`<br>Shows the DHCPv4 settings for all configured subnets. |

### Example

```
gaia> add dhcp server subnet 192.168.2.0 netmask 24

gaia> add dhcp server subnet 192.168.2.0 include-ip-pool start
192.168.2.20 end 192.168.2.90

gaia> add dhcp server subnet 192.168.2.0 include-ip-pool start
192.168.2.120 end 192.168.2.150

gaia> add dhcp server subnet 192.168.2.0 exclude-ip-pool start
192.168.2.155 end 192.168.2.254

gaia> set dhcp server subnet 192.168.2.0 include-ip-pool
192.168.2.20-192.168.2.90 enable

gaia> set dhcp server subnet 192.168.2.0 include-ip-pool
192.168.2.120-192.168.2.150 disable

gaia> set dhcp server subnet 192.168.2.0 exclude-ip-pool
192.168.2.155-192.168.2.254 enable

gaia> set dhcp server subnet 192.168.2.0 default-lease 43200

gaia> set dhcp server subnet 192.168.2.0 max-lease 86400

gaia> set dhcp server subnet 192.168.2.0 default-gateway
192.168.2.103

gaia> set dhcp server subnet 192.168.2.0 domain example.com

gaia> set dhcp server subnet 192.168.2.0 dns 192.168.2.101,
192.168.2.102, 192.168.2.103

gaia> set dhcp server subnet 192.168.2.0 enable
```

```
gaia> add dhcp server subnet 172.30.4.0 netmask 24

gaia> add dhcp server subnet 172.30.4.0 include-ip-pool start
172.30.4.10 end 172.30.4.99

gaia> set dhcp server subnet 172.30.4.0 include-ip-pool
172.30.4.10-172.30.4.99 enable

gaia> set dhcp server subnet 172.30.4.0 default-lease 43200

gaia> set dhcp server subnet 172.30.4.0 max-lease 86400

gaia> set dhcp server subnet 172.30.4.0 disable
```

```
gaia> add dhcp server subnet 10.20.30.0 netmask 24

gaia> set dhcp server subnet 10.20.30.0 default-lease 43200

gaia> set dhcp server subnet 10.20.30.0 max-lease 86400

gaia> set dhcp server subnet 10.20.30.0 disable
```

```
gaia> show dhcp server all
DHCP Server Enabled
DHCP-Subnet 192.168.2.0
    State           Enabled
    Net-Mask        24
    Maximum-Lease   86400
    Default-Lease   43200
    Domain          example.com
    Default Gateway 192.168.2.103
    DNS             192.168.2.101, 192.168.2.102, 192.168.2.103
    Pools (Include List)
        192.168.2.20-192.168.2.90           : enabled
        192.168.2.120-192.168.2.150         : disabled
    Pools (Exclude List)
        192.168.2.155-192.168.2.254         : enabled
DHCP-Subnet 172.30.4.0
    State           Disabled
    Net-Mask        24
    Maximum-Lease   86400
    Default-Lease   43200
    Pools (Include List)
        172.30.4.10-172.30.4.99           : enabled
DHCP-Subnet 10.20.30.0
    State           Disabled
    Net-Mask        24
    Maximum-Lease   86400
    Default-Lease   43200
gaia>
```

# DHCPv6

The Dynamic Host Configuration Protocol v6 (DHCPv6) is a network management protocol that automates the assignment of IPv6 addresses and other communication parameters to devices on an IPv6 network. With the use of a client-server architecture, DHCPv6 streamlines network configuration and management.

You can configure the Gaia Operating System as follows:

- DHCPv6 Server - To assign IPv6 addresses to connected hosts.
- DHCPv6 Client (with or without Prefix Delegation) - To receive IPv6 address automatically on Gaia OS interfaces.

# Configuring DHCPv6 in Gaia Portal

**Step 1 - Configure DHCPv6 Server Settings**

| Step | Instructions |
|---|---|
| 1 | Open Gaia Portal and do the steps below. |
| 2 | In the **Network Management** section, click the **DHCPv6** page. |
| 3 | In the **DHCPv6 Server Subnet Configuration** section, configure the applicable subnet from which to assign IPv6 addresses to network hosts: |
| 3A | Click **Add**. |
| 3B | At the top, select **Enable DHCPv6 Subnet**.<br>Next, configure the applicable settings on the **Subnet** tab. |
| 3C | In the **IPv6 address** field, enter the IPv6 address of the subnet from which Gaia OS assigns IPv6 addresses to network hosts.<br>In the **Mask length** field, enter the applicable IPv6 mask length.<br>**Note** - To automate the process, click **Get from interface**, select the applicable interface, and then click **OK** to confirm your selection. |
| 3D | **Optional:**<br>In the **Address Pool** section, configure the applicable IPv6 address pools from which Gaia OS assigns these IPv6 addresses to network hosts:<br>a. Click **Add**.<br>b. In the **Type** field, select **Include** or **Exclude**.<br>This specifies whether to include or exclude this range of IPv6 addresses in the IPv6 address pool.<br>c. In the **Status** field, select **Enable** or **Disable**.<br>This enables or disables the DHCPv6 Server for this subnet, or the DHCPv6 Server process (depending on the context).<br>d. In the **Start** field, enter the first IPv6 address of the range.<br>e. In the **End** field, enter the last IPv6 address of the range.<br>f. Click **OK**. |

| Step | Instructions |
|---|---|
| 3E | **Optional:**<br>In the **Lease Configuration** section, configure the applicable lease time:<br>a. In the **Default lease** field, enter the default lease time for all addresses in this IPv6 subnet.<br>This applies only if DHCPv6 clients do not request a unique lease time.<br>The default value in this field is 43,00 seconds.<br>Valid values in this field are from 1 to the Maximum lease time.<br>b. In the **Maximum lease** field, enter the maximum lease time for all address in this IPv6 subnet.<br>The default value in this field is 86,400 seconds.<br>Valid values in this field are from 1 to 4,294,967,295 seconds. |
| 3F | **Optional:**<br>On the **DNS** tab, define routing and DNS parameters for DHCP clients:<br>■ In the **Domain Name** field, enter the domain name for the DHCPv6 clients (for example, `example.com`).<br>■ In the **Primary DNS Server** field, enter the IPv6 address of the Primary DNSv6 server for the DHCPv6 clients.<br>■ In the **Secondary DNS Server** field, enter the IPv6 address of the Secondary DNSv6 server for the DHCPv6 clients (to use if the primary DNSv6 server does not respond).<br>■ In the **Tertiary DNS Server** field, enter the IPv6 address of the Tertiary DNSv6 server for the DHCPv6 clients (to use if the primary and secondary DNSv6 servers do not respond). |
| 3G | Click **OK** at the bottom. |
| 4 | In the **DHCPv6 Server Configuration** section, select **Enable DHCPv6 Server** and click **Apply**. |

**Step 2 - Configure DHCPv6 Client Settings**

| Step | Instructions |
|---|---|
| 1 | In the **DHCPv6 Client Configuration** section, configure how Gaia OS interfaces receive their IPv6 addresses and click **Apply**:<br>■ **Normal** - Receive IPv6 address and configuration from a DHCPv6 server.<br>■ **Prefix-delegation** - Receive only IPv6 prefix from a compatible DHCPv6 server.<br>**Note** - Router discovery is automatically configured for the users. |
| 2 | **Note** - This step applies only if you select **Prefix-delegation** in step 1 above.<br>In the **DHCPv6 Prefix-Delegation Configuration** section, configure the applicable DHCPv6 Prefix settings: |
| 2A | In the **DHCPv6 Prefix-Delegation Requesting Interface** section, leave the default option as **None** or select the applicable interface. |
| 2B | In the **DHCPv6 Prefix-Delegation Method** section, select the applicable option:<br>■ **Manual** - Only calculate IPv6 addresses from the prefix and assign them to the interfaces configured to receive IPv6 through Prefix-Delegation.<br>■ **Router Discovery** - In addition to IPv6, automatically configure Router Discovery protocol on the configured interfaces.<br>■ **DHCPv6** - In addition to IPv6, automatically configure the DHCPv6 Server feature on the new subnets and configure the Router Discovery protocol with the "Managed Configuration" flag on. |
| 2C | In the **DHCPv6 Prefix-Delegation - Suffix Pools for DHCPv6 Server Method** section, configure the IPv6 address pools.<br>a. Click **Add**.<br>b. In the **Type** field, select **Include** or **Exclude**.<br>This specifies whether to include or exclude this range of IPv6 addresses in the IPv6 address pool.<br>c. In the **Start** field, enter the first IPv6 address of the range.<br>d. In the **End** field, enter the last IPv6 address of the range.<br>e. Click **OK**. |
| 3 | At the bottom of the page, click **Apply**. |

# Configuring DHCPv6 in Gaia Clish

**Important:**

- Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-3246).
- On a VSX Gateway / each VSX Cluster Member, you must run these commands in the context of the applicable Virtual System (`set virtual-system <VS ID>`).

### Workflow

#### Part 1 - Configure the DHCPv6 Server settings

1. Add the required IPv6 subnets and allocated IPv6 pools:

   ```
   add dhcp6 server subnet <Subnet IPv6 Address> prefix <Subnet Mask Length> [exclude-ip-pool ...] [include-ip-pool ...]
   ```

2. Enable the configured subnets:

   ```
   set dhcp6 server subnet <Subnet IPv6 Address> enable
   ```

3. Enable the DHCPv6 Server:

   ```
   set dhcp6 server enable
   ```

### Part 2 - Configure the DHCPv6 Client settings

Gaia OS can work in these DHCPv6 Client modes (these modes are mutually exclusive):

- Regular DHCPv6 Client mode (default).
  1. Configure the DHCPv6 Client mode:

     ```
     set dhcp6 client client-mode normal
     ```

  2. Configure the DHCPv6 Client settings:

     ```
     set dhcp6 client
           hostname ...
           interface ...
     ```

- Advanced DHCPv6 prefix-delegation mode (a mix of the DHCPv6 Client and the DHCPv6 Server).
  1. Configure the DHCPv6 Client mode:

     ```
     set dhcp6 client client-mode prefix-delegation
     ```

  2. Configure the DHCPv6 Prefix Delegation settings:

     ```
     set dhcp6 prefix-delegation ...
     ```

### Part 3 - Configure the DHCPv6 Prefix Delegation settings

This part applies only if you configured the DHCPv6 Client mode "`prefix-delegation`".

1. Configure the Prefix Delegation method:

   ```
   set dhcp6 prefix-delegation delegation-method ...
   ```

2. Configure the interface that will send DHCPv6 requests to the DHCPv6 server:

   ```
   set dhcp6 prefix-delegation request-from ...
   ```

3. Configure which interfaces should be configured with an IPv6 address in the relevant subnet and subsequently start assigning IPv6 addresses to hosts on that subnet:

   ```
   add dhcp6 prefix-delegation assign-to...
   ```

4. Configure the IPv6 addresses for the allocated IP Pools (if you configured the delegation method "`dhcpv6`"):

   ```
   add dhcp6 prefix-delegation suffix-pools ...
   ```

### Part 4 - Save the changes and examine the settings

1. Save the changes in the Gaia database:

   ```
   save config
   ```

2. Examine the DHCPv6 settings:

   ```
   show dhcp6 ...
   ```

## Syntax

### DHCP6 'add' commands

```
add dhcp6
      prefix-delegation
            assign-to <Name of Interface>
            suffix-pools
                  exclude-pool start <First IPv6 Address> end
<Last IPv6 Address>
                  include-pool start <First IPv6 Address> end
<Last IPv6 Address>
      server subnet <Subnet IPv6 Address>
            exclude-ip-pool start <First IPv6 Address> end <Last
IPv6 Address>
            include-ip-pool start <First IPv6 Address> end <Last
IPv6 Address>
            prefix <IPv6 Subnet Mask Length>
```

### DHCP6 'set' commands

```
set dhcp6
      client
            client-mode {normal | prefix-delegation}
            hostname <IPv6 Hostname>
            interface <Logical Name of Interface>
                  leasetime <0-4294967295>
                  reboot <0-4294967295>
                  retry <0-4294967295>
                  timeout <0-4294967295>
      prefix-delegation
            delegation-method {manual | rdisc6 | dhcpv6}
            request-from <Name of Interface>
      server {enable | disable}
      server subnet <Subnet IPv6 Address>
            {disable | enable}
            default-lease <Lease in Seconds>
            max-lease <Maximum Lease in Seconds>
            dns "<DNS Server 1>, <DNS Server 2>, <DNS Server 3>"
            domain <Domain Name>
            exclude-ip-pool <First IPv6 Address-Last IPv6
Address> {disable | enable}
            include-ip-pool <First IPv6 Address-Last IPv6
Address> {disable | enable}
```

### DHCP6 'delete' commands

```
delete dhcp6
      client interface <Logical Name of Interface>
      prefix-delegation
            assign-to <Name of Interface>
            request-from <Name of Interface>
            suffix-pools exclude-pool <First IPv6 Address>
            suffix-pools include-pool <First IPv6 Address>
      server subnet <Subnet IPv6 Address>
            exclude-ip-pool <First IPv6 Address>
            include-ip-pool <First IPv6 Address>
```

### DHCP6 'show' commands

```
show dhcp6
      client
            client-mode
            interface <Name of Interface>
            interfaces
      prefix-delegation
            all
            assign-to
            delegation-method
            request-from
            status
            suffix-pools
      server
            all
            status
            subnet <Subnet IPv6 Address> [ip-pools]
            subnets
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| `add dhcp6 prefix-delegation assign-to <Name of Interface>` | Specifies the interface that should be configured with an IPv6 address in the relevant subnet and subsequently start assigning IPv6 addresses to hosts on that subnet.<br>Gaia OS automatically creates a /64 network ID and uses it generate an IPv6 address for the assigned interfaces. |
| `add dhcp6 client interface <interface name` | Configures the interface as DHCPv6 client (in client-mode 'normal'). |
| `add dhcp6 prefix-delegation suffix-pools exclude-pool start <First IPv6 Address> end <Last IPv6 Address>` | Specifies the IPv6 address that starts and the IPv6 address that ends the excluded allocated IP Pool range.<br>**Note** - Applies only if you configured "`set dhcp6 prefix-delegation delegation-method dhcpv6`". |

| Parameter | Description |
|---|---|
| `add dhcp6 prefix-delegation suffix-pools include-pool start <First IPv6 Address> end <Last IPv6 Address>` | Specifies the IPv6 address that starts and the IPv6 address that ends the included allocated IP Pool range.<br>**Note** - Applies only if you configured "`set dhcp6 prefix-delegation delegation-method dhcpv6`". |
| `add dhcp6 server subnet <Subnet IPv6 Address>` | Specifies the IPv6 address of the DHCP subnet on an Ethernet interface of the Gaia device. Hosts behind the Gaia interface get IPv6 addresses from address pools in the subnet. |
| `add dhcp6 server subnet <Subnet IPv6 Address> exclude-pool start <First IPv6 Address> end <Last IPv6 Address>` | For the specified subnet, configures the IPv6 address that starts and the IPv6 address that ends the excluded allocated IP Pool range. |
| `add dhcp6 server subnet <Subnet IPv6 Address> include-pool start <First IPv6 Address> end <Last IPv6 Address>` | For the specified subnet, configures the IPv6 address that starts and the IPv6 address that ends the included allocated IP Pool range. |
| `add dhcp6 server subnet <Subnet IPv6 Address> prefix <Subnet Mask Length>` | For the specified subnet, configures the IPv6 Subnet Mask Length from 8 to 128. |
| `set dhcp6 server {enable \| disable}` | Enables and disables the DHCPv6 Server feature in Gaia OS. |

| Parameter | Description |
|---|---|
| `set dhcp6 client client-mode {normal \| prefix-delegation}` | Specifies the working mode of the DHCPv6 Client (of the `dhclient6` daemon):<br>■ `normal`<br>Receives IPv6 and DNS servers from the configured DHCPv6 server.<br>For additional settings, use the "`set dhcp6 client`" commands.<br>■ `prefix-delegation`<br>Receives only the IPv6 prefix from the configured DHCPv6 server.<br>Uses the assigned prefix in your network.<br>For additional settings, use the "`set dhcp6 prefix-delegation`" commands and "`add dhcp6 prefix-delegation suffix-pools`" commands.<br>These DHCPv6 Client modes are mutually exclusive. |
| `set dhcp6 client hostname <IPv6 Hostname>` | Optional. Specifies the hostname for the DHCPv6 Client.<br>If you do not specify this hostname, the DHCPv6 server assigns a hostname to the client. |
| `set dhcp6 client interface <Logical Name of Interface> leasetime <0-4294967295>` | Lease duration time, in seconds, requested from the server. |
| `set dhcp6 client interface <Logical Name of Interface> reboot <0-4294967295>` | Default: 10<br>Thee time interval, in seconds, the client will wait before trying to discover a new IP address, after it has already tried to reacquire its current IP address. |
| `set dhcp6 client interface <Logical Name of Interface> retry <0-4294967295>` | Default: 300<br>The time, in seconds, to wait before retrying to contact a server. |
| `set dhcp6 client interface <Logical Name of Interface> timeout <0-4294967295>` | Default: 60<br>The time interval, in seconds, during which the client will try contacting a server. |

| Parameter | Description |
|---|---|
| `set dhcp6 prefix-delegation delegation-method {manual \| rdisc6 \| dhcpv6}` | Specifies how Gaia OS configures the system after receiving a prefix from the DHCPv6 server. Each method is a trade-off between granularity and automation.<br>■ `manual`<br>Only calculates IPv6 addresses from the prefix and assigns them to the interfaces configured to receive IPv6 through Prefix-Delegation.<br>■ `rdisc6`<br>In addition to IPv6 addresses, configures the Router Discovery protocol on all configured interfaces.<br>Does not enabled the "Managed Configuration" flag (`ManagedFlag`).<br>■ `dhcpv6`<br>In addition to IPv6 addresses, configures the DHCPv6 Server feature on all assigned interfaces and configures the Router Discovery protocol with the enabled "Managed Configuration" flag (`ManagedFlag`).<br>This method requires at least one IPv6 range. |
| `set dhcp6 prefix-delegation request-from <Name of Interface>` | Specifies the interface, on which to send prefix-delegation requests. |
| `set dhcp6 server subnet <Subnet IPv6 Address>` | Specifies the existing subnet, for which to configure the settings. |
| `set dhcp6 server subnet <Subnet IPv6 Address> {disable \| enable}` | For the specified subnet, disables or enables the DHCPv6 Server. |
| `set dhcp6 server subnet <Subnet IPv6 Address> default-lease <Lease in Seconds>` | For the specified subnet, configures the default DHCPv6 lease time that should be granted to DHCPv6 clients.<br>Applies only if DHCPv6 clients do not request a unique lease time.<br>Range: 1 - 4294967295<br>Default: 43200 |

| Parameter | Description |
|---|---|
| `set dhcp6 server subnet <Subnet IPv6 Address> max-lease <Maximum Lease in Seconds>` | For the specified subnet, configures the maximum DHCPv6 lease time that should be granted to DHCPv6 clients that do not request a specific lease.<br>Range: 1 - 4294967295<br>Default: 86400 |
| `set dhcp6 server subnet <Subnet IPv6 Address> dns "<DNS Server IPv6 Addresses>"` | Optional. For the specified subnet, configures the IPv6 addresses of DNS servers that the network hosts will use to resolve hostnames. Configure the DNS servers in the order of precedence.<br>For example: `dns "2001:0ba0::1, 2001:0ba0::2, 2001:0ba0::3"` |
| `set dhcp6 server subnet <Subnet IPv6 Address> domain <Domain Name>` | Optional. For the specified subnet, configures the domain name of the network hosts.<br>For example: `example.com`<br>**Note** - Domain names that are also valid numeric IPv6 addresses (for example 2001:0ba0::1) are not supported. |
| `set dhcp6 server subnet <Subnet IPv6 Address> exclude-ip-pool <First IPv6 Address-Last IPv6 Address> {disable \| enable}` | Optional. For the specified subnet, disables or enables the excluded allocated IP Pool range. |
| `set dhcp6 server subnet <Subnet IPv6 Address> include-ip-pool <First IPv6 Address-Last IPv6 Address> {disable \| enable}` | Optional. For the specified subnet, configures the included allocated IP Pool range. |
| `delete dhcp6 client interface <Logical Name of Interface>` | Deletes the DHCPv6 client configuration for the specified logical interface. |
| `delete dhcp6 prefix-delegation assign-to <Name of Interface>` | Deletes the interface that is configured to get an IPv6 address through prefix delegation. |

| Parameter | Description |
|---|---|
| `delete dhcp6 prefix-delegation suffix-pools exclude-pool <First IPv6 Address>` | Deletes the excluded allocated IP Pool range. |
| `delete dhcp6 prefix-delegation suffix-pools include-pool <First IPv6 Address>` | Deletes the included allocated IP Pool range. |
| `delete dhcp6 server subnet <Subnet IPv6 Address> exclude-ip-pool <First IPv6 Address-Last IPv6 Address>` | For the specified subnet, deletes the excluded allocated IP Pool range. |
| `delete dhcp6 server subnet <Subnet IPv6 Address> include-ip-pool <First IPv6 Address-Last IPv6 Address>` | For the specified subnet, deletes the included allocated IP Pool range. |
| `show dhcp6 client client-mode` | Shows the configured DHCPv6 Client mode. |
| `show dhcp6 client interface <Name of Interface>` | Shows the DHCPv6 settings for the specified interface. |
| `show dhcp6 client interfaces` | Shows the DHCPv6 settings for all interfaces. |

| Parameter | Description |
|---|---|
| `show dhcp6 prefix-delegation` | Shows the DHCPv6 prefix delegation settings:<br>■ `all`<br>Shows the summary of the current DHCPv6 prefix-delegation settings.<br>■ `assign-to`<br>Shows the interfaces that are configured through prefix delegation.<br>■ `delegation-method`<br>Shows the configured delegation method.<br>■ `request-from`<br>Shows the interface that sends prefix delegation requests.<br>■ `status`<br>Shows the status of the prefix-delegation mode.<br>■ `suffix-pools`<br>Shows the suffix IP Pools. |
| `show dhcp6 server` | Shows the DHCPv6 Server settings:<br>■ `all`<br>Shows all DHCPv6 Server settings.<br>■ `status`<br>Shows the DHCPv6 Server status (enabled / disabled).<br>■ `subnet <Subnet IPv6 Address> [ip-pools]`<br>Shows the DHCPv6 settings for the specified subnet.<br>■ `subnets`<br>Shows the DHCPv6 settings for all configured subnets. |

# Hosts and DNS

This page lets you configure:

- System Name - Host Name and Domain Name (see *"System Name" on page 253*)
- Hosts (see *"Hosts" on page 255*)
- DNS settings (see *"DNS" on page 259*)

# System Name

You set the host name (system name) during initial configuration. You can change the name.

## Configuring Host Name and Domain Name in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management > Host and DNS**. |
| 2 | In the **System Name** section:<br>a. In the **Host Name** field, enter the network name of the Gaia device.<br>b. **Optional:** In the **Domain Name** field, enter the domain. For example, `example.com`.<br>c. Click **Apply**. |

## Configuring Host Name and Domain Name in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

### Description

Configure the host name of your platform.

### Syntax

- To configure a hostname:

```
set hostname <Name of Host>
```

- To show the configured hostname:

```
show hostname
```

- To configure a domain name (optional):

```
set domainname <Domain>
```

- To show the configured domain name:

```
show domainname
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

# Hosts

You should add host addresses for systems that communicate frequently with the Gaia system.

You can:

- View the entries in the hosts table.
- Add an entry to the list of hosts.
- Modify the IP address of a host.
- Delete a host entry.

## Configuring Hosts in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Adding a static host entry

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management > Hosts and DNS**. |
| 2 | In the **Hosts** section, click **Add**. |
| 3 | Enter:<br>■ **Host Name** - Must include only alphanumeric characters, dashes ('-'), and periods ('.'). Periods must be followed by a letter or a digit. The name may not end with a dash or a period. There is no default value.<br>■ **IPv4 address**<br>■ **IPv6 address** |

### Editing the static host entry

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management > Hosts and DNS**. |
| 2 | In the **Hosts** section, select a host entry and click **Edit**. |
| 3 | Edit:<br>■ **Host Name**<br>■ **IPv4 address**<br>■ **IPv6 address** |

### Deleting the static host entry

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management > Hosts and DNS**. |
| 2 | In the **Hosts** section, select a host entry and click **Delete**. |

# Configuring Hosts in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

## Description

Add, edit, delete and show the name and IP addresses for hosts that communicate frequently with the Gaia operating system.

## Syntax

### Adding a static host entry

```
add host name <Name of Host>
      ipv4-address <IPv4 Address of Host>
      ipv6-address <IPv6 Address of Host>
```

### Editing the static host entry

```
set host name <Name of Host>
      ipv4-address <IPv4 Address of Host>
      ipv6-address <IPv6 Address of Host>
```

### Deleting the static host entry

```
delete host name <Name of Host> {ipv4 | ipv6}
```

### Viewing the configured static host entry

```
show host name<SPACE><TAB>
```

```
show host name <Name of Host> {ipv4 | ipv6}
```

### Viewing all configured IP addresses of all hosts

```
show host names [ipv4 | ipv6]
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Parameters

#### CLI Parameters

| Parameter | Description |
|---|---|
| `name <Name of Host>` | The name of a static host. Must include only alphanumeric characters, dashes ('-'), and periods ('.'). Periods must be followed by a letter or a digit. The name must not end in a dash or a period. There is no default value. |
| `ipv4-address <IPv4 Address of Host>` | The IPv4 address of the host. |
| `ipv6-address <IPv6 Address of Host>` | The IPv6 address of the host. |

# DNS

Gaia uses the Domain Name Service (DNS) to translate host names into IP addresses.

To enable DNS lookups, you must enter the primary DNS server for your system. You can also enter secondary and tertiary DNS servers.

When the system resolves host names, it consults the primary name server. If a failure or time-out occurs, the system consults the secondary name server, and if necessary, the tertiary.

You can also define a DNS Suffix, which is a search for host-name lookup.

**Note** - From R81, you can configure specific DNS settings in each Virtual System.
See the *R82 VSX Administration Guide*.

## Configuring DNS in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Configuring the DNS Servers

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management > Hosts and DNS**. |
| 2 | In the **System Name** section:<br>In the **Domain Name** field, enter the domain name (for example, `example.com`). |

| Step | Instructions |
|---|---|
| 3 | In the **DNS** section:<br>a. In the **DNS Suffix** field, enter the domain name suffix.<br>Specifies the name that is put at the end of all DNS searches if they fail.<br>By default, it must be the local domain name.<br>A valid domain name suffix is made up of subdomain strings separated by periods.<br>Subdomain strings must begin with an alphabetic letter and can consist only of alphanumeric characters and hyphens.<br>The domain name syntax is described in RFC 1035 (modified slightly in RFC 1223).<br>**Note** - Domain names that are also valid numeric IP addresses (for example: 10.19.76.100), although syntactically correct, are not permitted.<br>Example:<br>You configured the DNS Suffix "`example.com`" and you try to ping the host "`foo`" (with the command "`ping foo`"). If Gaia cannot resolve "`foo`", then Gaia tries to resolve "`foo.example.com`".<br>b. In the **Primary DNS Server** field, enter the IPv4 or IPv6 address of the Primary DNS server.<br>c. **Optional:** In the **Secondary DNS Server** field, enter the IPv4 or IPv6 address of the Secondary DNS server (to use if the primary DNS server does not respond).<br>d. **Optional:** In the **Tertiary DNS Server** field, enter the IPv4 or IPv6 address of the Tertiary DNS server (to use if the primary and secondary DNS servers do not respond).<br>e. Click **Apply**. |

# Configuring DNS in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

## Description

Configure, show, and delete the settings for DNS servers and the DNS suffix in Gaia OS.

## Syntax

### Configuring the DNS servers and the DNS suffix

```
set dns
      primary <IPv4 or IPv6 Address>
      secondary <IPv4 or IPv6 Address>
      tertiary <IPv4 or IPv6 Address>
      timeout {<1-30> | default}
      suffix <Name for Local Domain>
```

### Viewing the configured DNS servers and the DNS suffix

```
show dns
      primary
      secondary
      tertiary
      timeout
      suffix
```

### Deleting the DNS servers and the DNS suffix

```
delete dns
      primary
      secondary
      tertiary
      suffix
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| `primary <IPv4 or IPv6 Address>` | Specifies the IPv4 or IPv6 address of the primary DNS server, which resolve host names.<br>This must be a host that runs a DNS server. |
| `secondary <IPv4 or IPv6 Address>` | Specifies the IPv4 or IPv6 address of the secondary DNS server, which resolves host names if the primary server does not respond.<br>This must be a host that runs a DNS server. |
| `tertiary <IPv4 or IPv6 Address>` | Specifies the IPv4 or IPv6 address of the tertiary DNS server, which resolves host names if the primary and secondary servers do not respond.<br>This must be a host that runs a DNS server. |
| `timeout {<1-30> \| default}` | Specifies and shows how long (in seconds) Gaia OS waits for a DNS server response before Gaia OS sends the DNS request to the next configured DNS server.<br>**Notes:**<br>■ The default timeout is 30 seconds.<br>■ This setting is available only in Gaia Clish.<br>■ In the VSX mode, this setting applies only to the context of the VSX Gateway itself (VS0). |
| `suffix <Name for Local Domain>` | Specifies the name that is put at the end of all DNS searches if they fail. By default, it must be the local domain name.<br>A valid domain name suffix is made up of subdomain strings separated by periods.<br>Subdomain strings must begin with an alphabetic letter and can consist only of alphanumeric characters and hyphens.<br>The domain name syntax is described in RFC 1035 (modified slightly in RFC 1223).<br>**Note** - Domain names that are also valid numeric IP addresses (for example: 10.19.76.100), although syntactically correct, are not permitted.<br>Example:<br>You configured the DNS Suffix "`example.com`" and you try to ping the host "`foo`" (with the command "`ping foo`"). If Gaia cannot resolve "`foo`", then Gaia tries to resolve "`foo.example.com`". |

# DNS Proxy Forwarding Domains

## Overview

The Domain Name System (DNS) is the hierarchical and decentralized naming system used to identify computers, services, and other resources reachable through the Internet or other Internet Protocol (IP) networks.

The "DNS Proxy Forwarding Domains" feature is a based on the Linux **dnsmasq** package.

Before the "DNS Proxy Forwarding Domains" feature was introduced, an administrator could only configure at most three DNS servers for all types of suffixes - for instance, `google.com` and `amazon.com` were translated with the same DNS servers.

With the "DNS Proxy Forwarding Domains" feature, an administrator can configure, for every suffix, what DNS server will translate this suffix.

For instance, an administrator can decide that `google.com` will be translated by the DNS server 8.8.4.4 (Google's public DNS), but `amazon.com` will be translated by the DNS server 1.1.1.1 (Cloudflare's public DNS), while other suffixes will be translated by the local DNS server.

To complete this feature, a sub-feature was introduced - "Listening Interfaces". The `dnsmasq` package uses the configured Listening Interfaces to know on what interfaces it should listen, so it could route DNS queries properly. The `dnsmasq` package will not route DNS queries on interfaces, on which it was not configured to listen.

## Configuring DNS Proxy Forwarding Domains in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

**Configuring the DNS Proxy Forwarding Domains settings**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management > Hosts and DNS**. |
| 2 | In the **DNS Proxy Forwarding Domains** section, click **Add**. |

| Step | Instructions |
|---|---|
| 3 | In the **New DNS Proxy Forwarding Domain** window, configure the applicable settings:<br>a. In the **DNS Suffix** field, enter the domain name suffix.<br>b. In the **Primary DNS Server** field, enter the IPv4 address of the Primary DNS server.<br>c. **Optional:** In the **Secondary DNS Server** field, enter the IPv4 address of the Secondary DNS server (to use if the Primary DNS server does not respond).<br>d. **Optional:** In the **Tertiary DNS Server** field, enter the IPv4 address of the Tertiary DNS server (to use if the Primary and Secondary DNS servers do not respond).<br>e. Click **OK**. |
| 4 | In the **Listening Interfaces** section:<br>a. Select the applicable interfaces:<br>▪ **Listen on all interfaces**<br>▪ **Listen on specific interfaces** and select the applicable interface(s)<br>b. Click **Apply**.<br><br>**Note** - This section applies to all configured DNS Suffixes. |

**Editing the DNS Proxy Forwarding Domains settings**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management > Hosts and DNS**. |
| 2 | In the **DNS Proxy Forwarding Domains** section:<br>a. Click the DNS suffix.<br>b. Click **Edit**. |
| 3 | In the **New DNS Proxy Forwarding Domain** window:<br>a. Configure the applicable settings.<br>b. Click **OK**. |

| Step | Instructions |
|---|---|
| 4 | In the **Listening Interfaces** section:<br>a. Select the applicable interfaces.<br>b. Click **Apply**.<br><br>**Note** - This section applies to all configured DNS Suffixes. |

### Deleting the DNS Proxy Forwarding Domains

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management > Hosts and DNS**. |
| 2 | In the **DNS Proxy Forwarding Domains** section:<br>a. Click the DNS suffix.<br>b. Click **Delete**. |
| 3 | Click **Yes** to confirm. |

# Configuring DNS Proxy Forwarding Domains in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

## Description

Configure, show, and delete the settings for DNS servers and the DNS suffix in Gaia OS.

## Syntax

### Configuring the DNS suffix and the Listening Interfaces

```
add dns proxy
      forwarding-domain <FQDN>
      listening-interface {<Name of Interface> | all}
```

### Configuring the DNS servers for the specified DNS suffix

```
set dns proxy forwarding-domain <FQDN>
      primary <IPv4 Address of DNS Server>
      secondary <IPv4 Address of DNS Server>
      tertiary <IPv4 Address of DNS Server>
```

### Viewing the configured DNS suffixes, DNS servers, and Listening Interfaces

```
show dns proxy
      forwarding-domain <FQDN> {primary | secondary | tertiary}
      forwarding-domains
      listening-interfaces
```

### Deleting the configured DNS suffixes, DNS servers, and Listening Interfaces

```
delete dns proxy
      forwarding-domain <FQDN> [{primary | secondary |
tertiary}]
      listening-interface {<Name of Interface> | all}
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Parameters

#### CLI Parameters

| Parameter | Description |
|---|---|
| `forwarding-domain <FQDN>` | Specifies the DNS suffix (for example, `example.com`). |
| `listening-interface {<Name of Interface> \| all}` | Specifies the Listening Interfaces. |
| `primary <IPv4 Address of DNS Server>` | Specifies the Primary DNS server. |
| `secondary <IPv4 Address of DNS Server>` | Optional. Specifies the Secondary DNS server (to use if the Primary DNS server does not respond). |
| `tertiary <IPv4 Address of DNS Server>` | Optional. Specifies the tertiary DNS server (to use if the Primary and Secondary DNS servers do not respond). |

# IPv4 Static Routes

A static route defines the destination and one or more paths (next hops) to get to that destination.

You define static routes manually in the Gaia Portal, or in Gaia Clish (in Gaia gClish on Security Groups) with the "`set static-route`" command.

Static routes let you add paths to destinations that are unknown by dynamic routing protocols. You can define multiple paths (next hops) to a destination and define priorities for selecting a path. Static routes are also useful for defining the default route.

Static route definitions include these parameters:

- Destination IPv4 address.
- Route type:
  - **Normal** - Accepts and forwards packets to the specified destination.
  - **Reject** - Drops packets and sends ICMP *unreachable* packet.
  - **Blackhole** - Drops packets and does not send ICMP *unreachable* packet.
- Next-hop type:
  - **Address** - Identifies the next hop gateway by its IPv4 address.
  - **Logical** - Identifies the next hop gateway by the name of the local interface that connects to it. Use this option only if the next hop gateway has an unnumbered interface.
- Gateway identifier - IPv4 address, or name of local interface.
- Priority (Optional) - Assigns a path priority when there are many different paths.
- Rank (Optional) - Selects a route when there are many routes to a destination that use different routing protocols. You must use the Gaia Clish (Gaia gClish on Security Groups) to configure the rank.

# Configuring IPv4 Static Routes in Gaia Portal

You can configure IPv4 static routes one at a time, or many routes at once.

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Configuring One IPv4 Static Route at a Time

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **IPv4 Static Routes**. |
| 2 | In the **IPv4 Static Routes** section, click **Add**.<br>The **Add Destination Route** window opens. |
| 3 | In the **Destination** field, enter the IPv4 address of destination host, or network. |
| 4 | In the **Subnet mask** field, enter the subnet mask. |
| 5 | In the **Next Hop Type** field, select one of these:<br>■ **Normal** - To accept and forward packets<br>■ **Blackhole** - To drop packets, and not send ICMP *unreachable* packet to the traffic source<br>■ **Reject** - To drop packets, and send ICMP *unreachable* packet to the traffic source |
| 6 | In the **Rank** field, leave the default value (60), or enter the relative rank of the IPv4 static route (an integer from 1 to 255).<br>This value specifies the rank for the configured route when there are overlapping routes from different protocols. |
| 7 | Select the **Local Scope** option, if needed.<br>Use this setting on a Cluster Member when the ClusterXL Virtual IPv4 address is in a different subnet than the IPv4 address of a physical interface.<br>This lets the Cluster Member accept static routes on the subnet of the Cluster Virtual IPv4 address.<br>To make sure that the `scopelocal` attribute is set correctly, run the "`cat /etc/routed.conf`" command. For more information, see sk92799. |
| 8 | In the **Comment** field, enter the applicable comment text (up to 100 characters). |

| Step | Instructions |
|---|---|
| 9 | Click **Add Gateway** and select one of these options:<br>■ Option 1:<br>a. Select **IP Address** to specify the next hop by its IPv4 address.<br>b. In the **IPv4 Address** field, enter the IPv4 address of the next hop gateway.<br>c. In the **Priority** field, either do not enter anything, or select an integer between 1 and 8.<br>d. Add **Monitored IPs**.<br>e. Click **OK**.<br>■ Option 2:<br>a. Select **Network Interface** to specify the next hop by the name of the local interface name that connects to it.<br>b. In the **Local Interface** field, select an interface that connects to the next hop gateway.<br>c. In the **Priority** field, either do not enter anything, or select an integer between 1 and 8.<br>d. Add **Monitored IPs**.<br>e. Click **OK**.<br>**Notes:**<br>■ *Priority* defines which next hop gateway to select when multiple next hop gateways are configured. The lower the priority, the higher the preference - priority 1 means the highest preference, and priority 8 means the lowest preference. You can define two or more paths with the same priority to specify a backup path with equal priority. A next hop gateway with no priority configured is preferred over a next hop gateway with priority configured.<br>■ Multihop ping in Static Routes uses ICMP Echo Request to monitor reachability of an IP address multiple hops away. Multihop ping in Static Routes updates the status of an associated next hop in accordance to the reachability status. The next hop status becomes "down", if that IP address is unreachable. |
| 10 | If you defined a next hop gateway by **IP Address**, you can select the **Ping** option, if you need to monitor next hops for the IPv4 static route with the `ping`.<br>The Ping feature sends ICMP Echo Requests to make sure the next hop gateway for a static route is working.<br>Gaia includes in the kernel forwarding table only next hop gateways, which are verified as working.<br>When Ping is enabled, Gaia adds an IPv4 static route to the kernel forwarding table only after at least one next hop gateway is reachable. |

| Step | Instructions |
|---|---|
| 11 | Click **Save**. |
| 12 | In the **Advanced Options** section, you can configure the Ping behavior.<br>If you changed the default settings, click **Apply**. |

### Configuring Many IPv4 Static Routes at Once

You can use the batch mode to configure multiple static routes in one step.

**Note** - This mode does not allow the configuration of static routes that use a logical interface as the next hop.

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **IPv4 Static Routes**. |
| 2 | In the **Batch Mode** section, click **Add Multiple Static Routes**. |
| 3 | In the **Add Multiple Routes** window, select the **Next Hop Type**:<br>■ **Normal** - To accept and forward packets<br>■ **Blackhole** - To drop packets, and not send ICMP *unreachable* packet to the traffic source<br>■ **Reject** - To drop packets, and send ICMP *unreachable* packet to the traffic source |
| 4 | Add the routes in the text box, using this syntax:<br>`<Destination IPv4 Address>/<Mask Length> <IPv4 Address of Next Hop Gateway> ["<Comment>"]`<br>Where:<br>■ `<Destination IPv4 Address>/<Mask Length>` - Specifies the IPv4 address of destination host or network using the CIDR notation (IPv4 Address / Mask Length).<br>Example: `192.168.2.0/24`<br>You can use the `default` keyword instead of an IPv4 address when referring to the default route.<br>■ `<IPv4 Address of Next Hop Gateway>` - Specifies the IPv4 address of the next hop gateway<br>■ `"<Comment>"` - Optional. Free text comment for the static route.<br>Write the text in double quotes. Maximum length of the text string is 100 characters.<br>Example:<br>`default 192.0.2.100 192.0.2.1 "Default Route"`<br>`192.0.2.200/24 192.0.2.18 "My Backup Route"` |
| 5 | Click **Apply**.<br>The newly configured static routes show in the **IPv4 Static Routes** section.<br>**Note** - The text box shows entries that contain errors with messages at the top of the page. |

| Step | Instructions |
|---|---|
| 6 | Correct errors and reload the affected routes. |
| 7 | In the top right corner, click the **Monitoring** tab to make sure that the routes are configured correctly. |

# Configuring IPv4 Static Routes in Gaia Clish

## Description

Configure, show, and delete IPv4 static routes.

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

## Syntax

**Note** - There are no "`add`" commands for the static route feature.

### Adding or configuring a default static IPv4 route

```
set static-route default
      comment {"Text" | off}
      nexthop
            gateway
                  address <IPv4 Address of Next Hop Gateway> [priority <Priority>] {on | off}
                  logical <Name of Local Interface> [priority <Priority>] {on | off}
            blackhole
            reject
      ping {on | off}
      rank <Rank>
      scopelocal {on | off}
```

### Adding or configuring a specific static IPv4 route

```
set static-route <Destination IPv4 Address>
      comment {"Text" | off}
      nexthop
            gateway
                  address <IPv4 Address of Next Hop Gateway>
                        {on | off}
                        monitored-ip <Monitored IP Address> {on | off}
                        monitored-ip-option {fail-all | fail-any | force-if-symmetry {on |
off}}
                        [priority <Priority>]
                  logical <Name of Local Interface>
                        {on | off}
                        [priority <Priority>]
            blackhole
            reject
      off
      ping {on | off}
      rank <Rank>
      scopelocal {on | off}
```

### Viewing all configured static IPv4 routes

```
show route static all
```

### Removing a default static IPv4 route

```
set static-route default off
```

### Removing a specific static IPv4 route

```
set static-route <Destination IPv4 Address> off
```

### Removing a specific path only, when multiple next hop gateways are configured

```
set static-route <Destination IPv4 Address> nexthop gateway <IPv4 Address of Next Hop Gateway> off
set static-route <Destination IPv4 Address> nexthop gateway <Name of Local Interface> off
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| `default` | Defines the default static IPv4 route. |
| *`<Destination IPv4 Address>`* | Specifies the IPv4 address of destination host or network using the CIDR notation (IPv4 Address / Mask Length).<br>Example: `192.168.2.0/24`<br>You can use the `default` keyword instead of an IPv4 address when referring to the default route. |
| `comment {"`*`Text`*`" \| off}` | Defines of removes the optional comment for the static route.<br>■ Write the text in double quotes.<br>■ Text must be up to 100 characters.<br>■ This comment appears in the Gaia Portal and in the output of the "`show configuration`" command. |
| `nexthop` | Defines the next hop path, which can be a `gateway`, `blackhole`, or `reject`. |
| `gateway` | Specifies that this next hop accepts and sends packets to the specified destination. |
| `blackhole` | Specifies that this next hop drops packets, but does not send ICMP *unreachable* packet to the traffic source. |
| `reject` | Specifies that this next hop drops packets and sends ICMP *unreachable* packet to the traffic source. |

| Parameter | Description |
|---|---|
| `address <IPv4 Address of Next Hop Gateway>` | Specifies the IPv4 address of the next hop gateway. |
| `logical <Name of Local Interface>` | Identifies the next hop gateway by the name of the local interface that connects to it.<br>Use this option only if the next hop gateway has an unnumbered interface. |
| `monitored-ip <Monitored IP Address> {on \| off}` | Remote IPv4 address to monitor for the next hop gateway.<br>Monitors IP address(es) configured with the "`ip-reachability-detection`".<br>The next hop gateway becomes usable with respect to reachability of IP address(es) reported from the "`ip-reachability-detection`". |
| `monitored-ip-option {fail-all \| fail-any \| force-if-symmetry {on \| off}}` | Set failure condition and flavor for the configured monitored IP address(es).<br>■ `fail-all`<br>Fails the next hop gateway when all monitored IP addresses become unreachable.<br>Restores the next hop gateway when one of the monitored IP addresses becomes reachable.<br>Default: `off`<br>■ `fail-any`<br>Fails the next hop gateway when one of the monitored IP addresses becomes unreachable.<br>Restores the next hop gateway when all monitored IP addresses become reachable.<br>Default: `on`<br>■ `force-if-symmetry`<br>Ignores IP reachability reports from IP addresses with asymmetric traffic.<br>Default: `off` |

| Parameter | Description |
|---|---|
| `priority <Priority>` | Defines which gateway to select as the next hop when multiple gateways are configured.<br>The lower the priority, the higher the preference - priority 1 means the highest preference, and priority 8 means the lowest preference.<br>You can define two or more paths with the same priority to specify a backup path with equal priority.<br>A next hop gateway with no priority configured is preferred over a next hop gateway with priority configured |
| `nexthop ... on` | Adds the specified next hop gateway. |
| `nexthop ... off` | Deletes the specified next hop gateway.<br>If you specify a next hop gateway, only the specified path is deleted.<br>If you do not specify a next hop gateway, the route and all related paths are deleted. |
| `off` | Removes the static route. |
| `ping {on \| off}` | Enables (`on`) or disables (`off`) the ping of specified next hop gateways for IPv4 static routes.<br>The Ping feature sends ICMP Echo Requests to make sure the next hop gateway for a static route is working.<br>Gaia includes in the kernel forwarding table only next hop gateways, which are verified as working.<br>When Ping is enabled, Gaia adds an IPv4 static route to the kernel forwarding table only after at least one next hop gateway is reachable.<br>To configure the ping behavior, run:<br>`set ping count <value>`<br>`set ping interval <value>` |

| Parameter | Description |
|---|---|
| `rank <Rank>` | Selects a route, if there are many routes to a destination that use different routing protocols.<br>The route with the lowest rank value is selected.<br>Use the `rank` keyword in place of the `nexthop` keyword with no other parameters.<br>Accepted values are: `default` (60), integer numbers from 0 to 255.<br>In addition, see this command: "`set protocol-rank protocol <Rank>`" |
| `scopelocal {on \| off}` | Defines a static route with a link-local scope.<br>Use this setting on a Cluster Member, when the ClusterXL Virtual IPv4 address is in a different subnet than the IPv4 address of a physical interface.<br>This lets the Cluster Member accept static routes on the subnet of the Cluster Virtual IPv4 address.<br>To make sure that the `scopelocal` attribute is set correctly, run the "`cat /etc/routed.conf`" command.<br>For more information, see sk92799. |

**Example**

```
gaia> set static-route 192.0.2.0/24 nexthop gateway address 192.0.2.155 on

gaia> set static-route 192.0.2.0/24 nexthop gateway address 192.0.2.155 off

gaia> set static-route 192.0.2.0/24 nexthop gateway logical eth0 on

gaia> set static-route 192.0.2.0/24 off

gaia> set static-route 192.0.2.100/32 nexthop blackhole

gaia> set static-route 192.0.2.100/32 rank 2

gaia> show route static
  Codes: C - Connected, S - Static, R - RIP, B - BGP,
       O - OSPF IntraArea (IA - InterArea, E - External, N - NSSA)
       A - Aggregate, K - Kernel Remnant, H - Hidden, P - Suppressed

S 0.0.0.0/0 via 192.168.3.1, eth0, cost 0, age 164115
S 192.0.2.100 is a blackhole route
S 192.0.2.240 is a reject route
gaia>
```

# IPv6 Static Routes

*In This Section:*



**Important** - First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*).

## Configuring IPv6 Static Routes in Gaia Portal

You can configure IPv6 static routes only one route at a time.

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

**Procedure**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Network Management** > **IPv6 Static Routes**. |
| 2 | In the **IPv6 Static Routes** section, click **Add**. |
| 3 | In the **Destination / Mask Length** field, enter the IPv6 address and prefix (default prefix is 64). |
| 4 | Select the **Next Hop Type** field select:<br>■ **Normal** - To accept and forward packets<br>■ **Blackhole** - To drop packets, and not send ICMP *unreachable* packet to the traffic source<br>■ **Reject** - To drop packets, and send ICMP *unreachable* packet to the traffic source |
| 5 | In the **Rank** field, leave the default value (60), or enter the relative rank of the IPv6 static route (an integer from 1 to 255).<br>This value specifies the rank for the configured route when there are overlapping routes from different protocols. |
| 6 | In the **Comment** field, enter the applicable comment text (up to 100 characters). |

| Step | Instructions |
|---|---|
| 7 | In the **Add Gateway** section, click **Add**. |
| 8 | In the **Gateway Address** field, enter the IPv6 address of the next hop gateway. |
| 9 | In the **Priority** field, either do not enter anything, or select an integer between 1 and 8.<br>*Priority* defines the order for selecting the next hop gateway when multiple next hop gateways are configured.<br>The lower the priority, the higher the preference - priority 1 means the highest preference, and priority 8 means the lowest preference.<br>A next hop gateway with no priority configured is preferred over a next hop gateway with priority configured.<br>You cannot configure two next hop gateways with the same priority, because IPv6 Equal Cost Multipath Routes are not supported. |
| 10 | Click **OK**. |
| 11 | Select the **Ping6** option, if you need to monitor next hops for the IPv6 static route using `ping6`.<br>The Ping6 feature sends ICMPv6 Echo Requests to make sure the next hop gateway for a static route is working. |
| 12 | Click **Save**. |
| 13 | In the **Advanced Options** section, you can configure the Ping6 behavior.<br>If you changed the default settings, you must click **Apply**. |

# Configuring IPv6 Static Routes in Gaia Clish

## Syntax

**Note** - There are no "`add`" commands for the static route feature.

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

### Adding or configuring the default static IPv6 route

```
set ipv6 static-route default
      comment {"Text" | off}
      nexthop
            gateway {<IPv6 Address of Next Hop Gateway> | logical}
                  [priority <Priority>] {on | off}
                  interface <Name of Local Interface> [priority <Priority>] {on | off}
            blackhole
            reject
      off
      ping6 {on | off}
      rank <Rank>
```

### Adding or configuring the specific static IPv6 route

```
set ipv6 static-route <Destination IPv6 Address>
      comment {"Text" | off}
      nexthop
            gateway {<IPv6 Address of Next Hop Gateway> | logical}
                  [priority <Priority>] {on | off}
                  interface <Name of Local Interface> [priority <Priority>] {on | off}
            blackhole
            reject
      off
      ping6 {on | off}
      rank <Rank>
```

### Viewing all configured static IPv6 routes

```
show ipv6 route static all
```

### Removing the default static IPv6 route

```
set ipv6 static-route default off
```

### Removing the specific static IPv6 route

```
set ipv6 static-route <Destination IPv6 Address> off
```

### Removing the specific path only, when multiple next hop gateways are configured

```
set ipv6 static-route <Destination IPv6 Address> nexthop gateway <IPv6 Address of Next Hop Gateway> off
```

```
set ipv6 static-route <Destination IPv6 Address> nexthop gateway <Name of Local Interface> off
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| `default` | Defines the default static IPv6 route. |
| `<Destination IPv6 Address>` | Defines the IPv6 address of destination host or network using the CIDR notation (IPv6 Address / Mask Length).<br>Example: `fc00::/64`<br>Mask length must be in the range 8-128. |
| `comment {"Text" \| off}` | Defines of removes the optional comment for the static route.<br>■ Write the text in double quotes.<br>■ Text must be up to 100 characters.<br>■ This comment appears in the Gaia Portal and in the output of the "`show configuration`" command. |
| `nexthop` | Defines the next hop path, which can be a `gateway`, `blackhole`, or `reject`. |
| `gateway` | Specifies that this next hop accepts and sends packets to the specified destination. |
| `blackhole` | Specifies that this next hop drops packets, but does not send ICMP *unreachable* packet to the traffic source. |
| `reject` | Specifies that this next hop drops packets and sends ICMP *unreachable* packet to the traffic source. |
| `address <IPv6 Address of Next Hop Gateway>` | Defines the IPv6 address of the next hop gateway. |
| `interface <Name of Local Interface>` | Identifies the next hop gateway by the local interface that connects to it.<br>Use this option only if the next hop gateway has an unnumbered interface. |

| Parameter | Description |
|---|---|
| `priority <Priority>` | Defines the order for selecting the next hop gateway when multiple next hop gateways are configured.<br>The lower the priority, the higher the preference - priority 1 means the highest preference, and priority 8 means the lowest preference.<br>A next hop gateway with no priority configured is preferred over a next hop gateway with priority configured.<br>You cannot configure two next hop gateways with the same priority, because IPv6 Equal Cost Multipath Routes are not supported. |
| `nexthop ... on` | Adds the specified next hop gateway. |
| `nexthop ... off` | Deletes the specified next hop gateway.<br>If you specify a next hop, only the specified path is deleted.<br>If you do not specify a next hop, the route and all related paths are deleted. |
| `off` | Removes the static route. |
| `ping6 {on \| off}` | Enables (`on`) or disables (`off`) the ping of specified next hop gateways for IPv6 static routes.<br>The Ping6 feature sends ICMPv6 Echo Requests to make sure the next hop gateway for a static route is working.<br>Gaia includes in the kernel forwarding table only next hop gateways, which are verified as working.<br>When Ping6 is enabled, Gaia adds an IPv6 static route to the kernel forwarding table only after at least one next hop gateway is reachable.<br>To configure the ping6 behavior, run:<br>`set ping count <value>`<br>`set ping interval <value>` |
| `rank <Rank>` | Selects a route, if there are many routes to a destination that use different routing protocols.<br>The route with the lowest rank value is selected.<br>Use the `rank` keyword in place of the `nexthop` keyword with no other parameters.<br>Accepted values are: `default` (60), integer numbers from 0 to 255.<br>In addition, see this command: `set protocol-rank protocol <Rank>` |

### Example

```
gaia> set ipv6 static-route 3100:192::0/64 nexthop gateway 3900:172::1 on

gaia> set ipv6 static-route 3100:192::0/64 nexthop gateway 3900:172::1 interface eth3 on

gaia> set ipv6 static-route 3100:192::0/64 nexthop gateway 3900:172::1 priority 3 on

gaia> set ipv6 static-route 3100:192::0/64 nexthop reject

gaia> set ipv6 static-route 3100:192::0/64 nexthop blackhole

gaia> set ipv6 static-route 3100:192::0/64 off

gaia> set ipv6 static-route 3100:192::0/64 nexthop gateway 3900:172::1 off

gaia> set ipv6 static-route 3100:192::0/64 nexthop gateway 3900:172::1 interface eth3 off

gaia> show ipv6 route static
  Codes: C - Connected, S - Static, B - BGP, Rg - RIPng, A - Aggregate,
       O - OSPFv3 IntraArea (IA - InterArea, E - External),
       K - Kernel Remnant, H - Hidden, P - Suppressed

S 3100:55::1/64 is directly connected
S 3200::/64 is a blackhole route
S 3300:123::/64 is a blackhole route
S 3600:20:20:11::/64 is directly connected, eth3
```

# Troubleshooting

### Scenario - SmartConsole does not let you enable the VPN Software Blade in the Security Gateway object

*Symptoms*

You cannot enable the VPN Software Blade. SmartConsole shows this message:

```
VPN blade demands gateway's IP address corresponding to the
interface's IP addresses
```

*Cause*

IPv6 feature is active on the Security Gateway, but the main IPv6 address is not configured in the Security Gateway object in SmartConsole.

*Next Steps*

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Gateway object.
3. From the left tree, click **General Properties**.
4. Configure the main IPv6 address.
5. Click **OK**.
6. Install the Access Control Policy on the Security Gateway object.

# Configuring IPv6 Neighbor Entries

### Description

You can add and delete entries in the Gaia IPv6 Neighbor table.

**Note** - You can add or delete Neighbor entries only from the Gaia Clish.

**Important:**

- First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 398*).
- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

### Syntax

- To add an IPv6 neighbor entry:

```
add neighbor-entry ipv6-address <IPv6 Address of Neighbor>
macaddress <MAC Address of Neighbor> interface <Name of Local
Interface>
```

- To show an IPv6 neighbor entry:

```
show neighbor<SPACE><TAB>
```

```
show neighbor TABLE
```

- To delete an IPv6 neighbor entry:

```
delete neighbor-entry ipv6-address <IPv6 Address of Neighbor>
interface <Name of Local Interface>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Parameters

| Parameter | Description |
|---|---|
| *<IPv6 Address of Neighbor>* | Specifies the IPv6 address of a new static Neighbor Discovery entry |

| Parameter | Description |
|---|---|
| *<MAC Address of Neighbor>* | Specifies the MAC address for respective IPv6 address |
| *<Name of Local Interface>* | Name of the local interface that connects to the Neighbor |

# NetFlow Export

*In This Section:*



## 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 Security Gateways and Cluster Members as an Exporter of NetFlow records for all the traffic that passes through.

**Note** - The state of the SecureXL on a Security Gateway is irrelevant for NetFlow export.

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 configuration.

You can configure a maxumum of three NetFlow Collectors. Gaia sends the NetFlow records go to all configured NetFlow Collectors. If you configure three NetFlow Collectors, Gaia sends each NetFlow record three times.

Regardless of which NetFlow export format you configure, Gaia 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).
- VSX VSID.

**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.

For more information, see sk102041.

# Configuration Procedure

**Important** - In a Cluster, you must configure all the Cluster Members in the same way.

1. **Configure the NetFlow Export settings in Gaia**

   You can configure these settings in Gaia Portal, or in Gaia Clish.

   **Configuring the NetFlow settings in Gaia Portal**

   a. In the left navigation tree, click **Network Management** > **NetFlow Export**.

   b. **Optional:** In the **Global Options** section, configure when the NetFlow starts to send the data after a connection opens, and click **Apply**.

      This configures how frequently the NetFlow sends the number of ongoing connections.

      Enter a value between 10 and 60 seconds, or enter the value 0 to disable.

   c. In the **Collectors** section, click **Add**.

d. Enter the required data for each collector:

| Parameter | Description |
|---|---|
| **IP Address** | The destination IPv4 address, to which Gaia sends the NetFlow packets.<br>This parameter is mandatory. |
| **UDP Port Number** | The destination UDP port number, on which the collector listens.<br>This parameter is mandatory.<br>There is no default or standard port number for NetFlow. |
| **Export Format** | The NetFlow protocol version to use:<br>■ **Netflow_V5** - Protocol NetFlow v5<br>■ **Netflow_V9** - Protocol NetFlow v9<br>■ **IPFIX** - Known as protocol "NetFlow v10"<br>Each protocol version has a different packet format.<br>The default is **Netflow_V9**. |
| **Source IP address** | **Optional:** The source IPv4 address of the NetFlow packets.<br>This must be an IPv4 address of the local host.<br>The default is an IPv4 address of the network interface, from which Gaia sends the NetFlow packets.<br>We recommend the default. |
| **Enable** | Select this option to enable the configured NetFlow Collector. |

e. Click **OK**.

f. In the **Advanced Options** section, the **NetFlow Fw rule** option controls for which traffic to enable the NetFlow export:

| Scenario | Instructions |
|---|---|
| You performed a Clean Install of R82 | ■ By default (this option is cleared) the NetFlow export is enabled for traffic accepted by **all** Access Control rules.<br>■ You can select this option to enable the NetFlow export **only** for traffic accepted by Access Control rules with the **Track** option **Log** and **Accounting** you configured in SmartConsole.<br>**Important** - If you selected this option, you must configure the applicable Access Control rules in SmartConsole. |
| You upgraded to R82 from R80.40 or lower version | You must:<br>i. Configure select this option in Gaia Portal and click **Apply**.<br>ii. Configure the applicable Access Control rules with the **Track** option **Log** and **Accounting** in SmartConsole. |

**Configuring the NetFlow settings in Gaia Clish**

a. **Optional:** Configure when the NetFlow starts to send the data after a connection opens.

```
set netflow liveconn_interval {<10-60> | 0}
```

Enter a value between 10 and 60 seconds, or enter the value 0 to disable.

b. Configure a new NetFlow collector:

```
add netflow collector ip <IPv4 Address of Collector>
port <Destination Port on Collector> [srcaddr <Source
IPv4 Address>] export-format {Netflow_V5 | Netflow_V9
| IPFIX} enable {yes | no}
```

c. Configure for which traffic to enable the NetFlow export:

```
set netflow fwrule {1 | 0}
```

| Scenario | Instructions |
|---|---|
| You performed a Clean Install of R82 | ▪ By default (value 0) the NetFlow export is enabled for traffic accepted by **all** Access Control rules.<br>▪ You can configure the value 1 to enable the NetFlow export **only** for traffic accepted by Access Control rules with the **Track** option **Log** and **Accounting** you configured in SmartConsole.<br>**Important** - If you configure the value 1, you must configure the applicable Access Control rules in SmartConsole. |
| You upgraded to R82 from R80.40 or lower version | You must:<br>i. Configure the value 0 in Gaia Clish.<br>ii. Configure the applicable Access Control rules with the **Track** option **Log** and **Accounting** in SmartConsole. |

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

2. **In SmartConsole, configure the explicit Access Control rules**

**Important** - This step is necessary only in these cases:
- In Gaia Portal you selected the option "**NetFlow Fw rule**"
- In Gaia Clish you ran the command "`set netflow fwrule 0`".

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:

**Important** - In the **Track** column, you must select **Log** and **Accounting**.

| 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 Security Gateway or Cluster object.

# Available Commands in Gaia Clish

### Syntax

- Configure when the NetFlow starts to send the data after a connection opens.

```
set netflow liveconn_interval {<10-60> | 0}
```

- To configure a new NetFlow collector:

```
add netflow collector ip <IPv4 Address of Collector> port
<Destination Port on Collector> [srcaddr <Source IPv4
Address>] export-format {Netflow_V5 | Netflow_V9 | IPFIX}
enable {yes | no}
```

- To change settings of an existing NetFlow collector:

```
set netflow collector
      ip <IPv4 Address of Collector> port <Destination Port
on Collector> export-format {Netflow_V5 | Netflow_V9 |
IPFIX} [srcaddr <Source IPv4 Address>] enable {yes | no}
      for-ip <IPv4 Address of Collector>
            ip <IPv4 Address of Collector> port <Destination
Port on Collector> export-format {Netflow_V5 | Netflow_V9 |
IPFIX} [srcaddr <Source IPv4 Address>] enable {yes | no}
            for-port <Destination Port on Collector> ip
<IPv4 Address of Collector> port <Destination Port on
Collector> export-format {Netflow_V5 | Netflow_V9 | IPFIX}
[srcaddr <Source IPv4 Address>] enable {yes | no}
```

- To configure for which traffic the NetFlow exports its records:

```
set netflow fwrule {1 | 0}
```

- To show the configured NetFlow collectors:

```
show netflow
      all
      collector
            enable
            export-format
            ip
            port
            srcaddr
            for-ip <IPv4 Address of Collector>
                  enable
                  export-format
                  port
                  srcaddr
                  for-port <Destination Port on Collector>
                        enable
                        export-format
                        srcaddr
```

- To show when the NetFlow starts to send the data after a connection opens:

```
show netflow liveconn_interval
```

- To show for which traffic the NetFlow exports its records:

```
show netflow fwrule
```

- To delete a configured NetFlow collector:

```
delete netflow collector for-ip <IPv4 Address of Collector>
[for-port <Destination Port on Collector>
```

### CLI Parameters

| Parameter | Description |
|---|---|
| `ip <IPv4 Address of Collector>` | Specifies the destination IPv4 address of the NetFlow Collector, to which Gaia sends the NetFlow packets.<br>This parameter is mandatory. |
| `port <Destination Port on Collector>` | Specifies the destination UDP port number on the NetFlow Collector, on which the collector listens.<br>This parameter is mandatory.<br>There is no default or standard port number for NetFlow. |

| Parameter | Description |
|---|---|
| `srcaddr <Source IPv4 Address>` | **Optional:** Specifies the source IPv4 address of the NetFlow packets.<br>This must be an IPv4 address of the local host.<br>The default is an IPv4 address of the network interface, from which Gaia sends the NetFlow packets.<br>We recommend the default. |
| `export-format {Netflow_V5 \| Netflow_V9 \| IPFIX}` | The NetFlow protocol version to use:<br>■ `Netflow_V5` - Protocol NetFlow v5<br>■ `Netflow_V9` - Protocol NetFlow v9 (default)<br>■ `IPFIX` - Known as protocol "NetFlow v10"<br>Each NetFlow protocol version has a different packet format. |
| `for-ip <IPv4 Address of Collector> for-port <Destination Port on Collector>` | These parameters specify the configured NetFlow Collector.<br>**Notes:**<br>■ If you configured only one collector, it is not necessary to use these parameters.<br>■ If you configured two or three collectors with different IP addresses, use the "`for-ip`" parameter.<br>■ If you configured two or three collectors with the same IP address and different UDP ports, you must use the "`for-ip`" and "`for-port`" parameters to identify the collectors. |

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><code>set netflow fwrule {1 | 0}</code></td><td>Specifies for which traffic to enable the NetFlow export:
<table>
<tr><th>Scenario</th><th>Instructions</th></tr>
<tr><td>You performed a Clean Install of R82</td><td>■ By default (value 0) the NetFlow export is enabled for traffic accepted by all Access Control rules.<br>■ You can configure the value 1 to enable the NetFlow export only for traffic accepted by Access Control rules with the Track option Log and Accounting you configured in SmartConsole.<br>Important - If you configure the value 1, you must configure the applicable Access Control rules in SmartConsole.</td></tr>
<tr><td>You upgraded to R82 from R80.40 or lower version</td><td>You must:<br>1. Configure the value 0 in Gaia Clish.<br>2. Configure the applicable Access Control rules with the Track option Log and Accounting in SmartConsole.</td></tr>
</table></td></tr>
<tr><td><code>set netflow liveconn_interval {<10-60> | 0}</code></td><td>Configures when the NetFlow starts to send the data after a connection opens.<br>Enter a value between 10 and 60 seconds, or enter the value 0 to disable</td></tr>
<tr><td><code>show netflow fwrule</code></td><td>Shows for which traffic the NetFlow exports its records:<br>■ <code>Yes</code><br>The NetFlow export is enabled for traffic accepted by all Access Control rules.<br>■ <code>No</code><br>The NetFlow export is enabled only for traffic accepted by Access Control rules with the Track option Log and Accounting you configured in SmartConsole.</td></tr>
</table>

# System Management

This chapter includes procedures and reference information for:

- Time and Date
- Cloning Groups
- SNMP
- Job Scheduler
- Mail Notification
- Login Messages
- Session in Gaia Portal and Gaia Clish
- Core Dump Files
- System Logging
- Network Access over Telnet
- GUI Clients for Security Management Server
- LLDP

# System Passwords

In this section, you can configure these passwords in Gaia OS:

- A password for the Expert mode
- A password for the Gaia GRUB (boot loader)

**Best Practice** - For security reasons, configure different passwords for the Expert mode and for GRUB.

# Configuring System Passwords in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

**Best Practice** - For security reasons, configure different passwords for the Expert mode and for GRUB.

## Configuring the Expert mode password

### Description

The Expert mode password protects the Expert shell against unapproved access.

The default Gaia shell is called `clish`.

Gaia Clish is a restrictive shell (role-based administration controls the number of commands available in the shell).

While the use of Gaia Clish is encouraged for security reasons, Gaia Clish does not give access to low level system functions.

For low-level configuration, use the more permissive Expert mode shell. In addition, see sk144112.

- To enter the Expert shell, run in Gaia Clish: `expert`
- To exit from the Expert shell and go back to Gaia Clish, run: `exit`

**Note** - If a command is supported in Gaia Clish, it is **not** supported to run the corresponding command in Expert mode.
For example, to work with interfaces, Gaia Clish provides the commands "`show interface`" and "`set interface`".
Therefore, it is **not** supported to run the `ifconfig` command in the Expert mode.

**Note** - There is **no** default password for the Expert mode. You must configure a password for the Expert mode before you can use it.

### Procedure

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`). |
| 2 | Click **System Management > System Passwords**. |
| 3 | In the section **Change Expert Password**, enter the required password.<br>The password must contain at least 6 characters. |
| 4 | Click **Apply**. |

# Configuring the GRUB password

### Description

The GRUB password protects the GRUB menu and GRUB terminal.

Gaia asks for this password when you boot into the Maintenance Mode and revert Gaia snapshots.

**Important:**

- You must configure a GRUB password before you boot into the Maintenance Mode or revert a Gaia snapshot.
- If do not know your GRUB password, and Gaia does not boot into the Normal Mode, you must contact *Check Point Support*.

### Procedure

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`). |
| 2 | Click **System Management > System Passwords**. |
| 3 | In the section **Change GRUB Password**, enter the required password.<br>The password must contain at least 6 characters. |
| 4 | Click **Apply**. |

# Configuring System Passwords in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

**Best Practice** - For security reasons, configure different passwords for the Expert mode and for GRUB.

## Configuring the Expert mode password

### Description

The Expert mode password protects the Expert shell against unapproved access.

The default Gaia shell is called `clish`.

Gaia Clish is a restrictive shell (role-based administration controls the number of commands available in the shell).

While the use of Gaia Clish is encouraged for security reasons, Gaia Clish does not give access to low level system functions.

For low-level configuration, use the more permissive Expert mode shell. In addition, see sk144112.

- To enter the Expert shell, run in Gaia Clish: `expert`
- To exit from the Expert shell and go back to Gaia Clish, run: `exit`

**Note** - If a command is supported in Gaia Clish, it is **not** supported to run the corresponding command in Expert mode.
For example, to work with interfaces, Gaia Clish provides the commands "`show interface`" and "`set interface`".
Therefore, it is **not** supported to run the `ifconfig` command in the Expert mode.

**Note** - There is **no** default password for the Expert mode. You must configure a password for the Expert mode before you can use it.

### Syntax to configure an Expert mode password in plain text

```
set expert-password
```

The password must contain at least 6 characters.

### Syntax to configure an Expert mode password as a salted hash

```
set expert-password-hash <Hash String>
```

**Important** - You must run the "`save config`" command to save the new Expert mode password permanently.

### Parameters

| Parameter | Description |
|---|---|
| `hash <Hash String>` | The password as an MD5, SHA256, or SHA512 salted hash instead of plain text (the password string must contain at least 6 characters).<br>Use this option when you upgrade or restore using backup scripts.<br>You can generate the hash of the password with the "`cpopenssl`" command (run: `cpopenssl passwd -help`).<br>To configure the default hash algorithm, see:<br>■ *"Password Hashing Algorithm" on page 524* (in Gaia Portal)<br>■ *"Configuring Hashing Algorithm" on page 533* (in Gaia Clish)<br><br>**Best Practice** - Do **not** use MD5 hash because it is not secure.<br><br>**Notes:**<br>■ Format:<br>`$<Hash Standard>$<Salt>$<Encrypted>`<br>■ The length of this hash string must be less than 128 characters.<br>■ *<Hash Standard>*<br>One of these digits:<br>• `1` = MD5<br>• `5` = SHA256<br>• `6` = SHA512<br>■ *<Salt>*<br>A string of these characters:<br>`a-z A-Z 0-9 . / [ ] _ ` ^`<br>The length of this string must be between 2 and 16 characters.<br>■ *<Encrypted>*<br>A string of these characters:<br>`a-z A-Z 0-9 . / [ ] _ ` ^`<br>The length of this string must be:<br>• For MD5, less than 22 characters.<br>• For SHA256, less than 43 characters.<br>• For SHA512, less than 86 characters. |

## Example

```
gaia> set expert-password
Enter current expert password: *******
Enter new expert password: *****
Enter new expert password (again): *****
Password is only 5 characters long; it must be at least 6 characters in length.
Enter new expert password: ******
Enter new expert password (again): ******
Password is not complex enough; try mixing more different kinds of characters (upper case, lower case, digits, and punctuation).
Enter new expert password: *******
Enter new expert password (again): *******

gaia> save config
```

# Configuring the GRUB password

### Description

The GRUB password protects the GRUB menu and GRUB terminal.

Gaia asks for this password when you boot into the Maintenance Mode and revert Gaia snapshots.

**Important:**

- You must configure a GRUB password before you boot into the Maintenance Mode or revert a Gaia snapshot.
- If do not know your GRUB password, and Gaia does not boot into the Normal Mode, you must contact *Check Point Support*.

### Syntax to configure a GRUB password in plain text

```
set grub2-password
```

The password must contain at least 6 characters.

### Syntax to configure a GRUB password as a SHA512 salted hash

```
set grub2-password-hash <Hash String>
```

Use the slated hash configuration when you upgrade or restore with user-defined shell scripts.

**Important** - Gaia saves the new GRUB password automatically.

### Parameters

| Parameter | Description |
|---|---|
| `hash <Hash String>` | The password as a SHA512 salted hash instead of plain text.<br>**Notes:**<br>■ To get a hash string for a password, run this command in the Expert mode:<br>`grub2-mkpasswd-pbkdf2`<br>■ Format of the hash string:<br>`grub.pbkdf2.sha512.<Rounds>.<Salt>.<Checksum>`<br>■ The length of this hash string must be between 282 and 512 characters.<br>■ `grub.pbkdf2.sha512`<br>A constant string.<br>■ *<Rounds>*<br>The number of iterations stored in the decimal format. In Gaia OS, this number is always 10000.<br>■ *<Salt>*<br>The salt string that is encoded using upper-case hexadecimal digits.<br>The length of this string must be 128 characters.<br>■ *<Checksum>*<br>The resulting derived key that is encoded using upper-case hexadecimal digits.<br>The length of this string must be 128 characters. |

### Example 1 - Plain text

```
gaia> set grub2-password
Enter new grub2 password: *
Enter new grub2 password (again): *
Password is only 1 characters long; it must be at least 6 characters in length.
Enter new grub2 password: ******
Enter new grub2 password (again): ******
Password is not complex enough; try mixing more different kinds of characters (upper case, lower case, digits, and punctuation).
Enter new grub2 password: *******
Enter new grub2 password (again): *******
gaia>

gaia> show configuration grub2-password
set grub2-password-hash grub.pbkdf2.sha512.10000.B8A(---truncated---)7D0.017(---truncated---)623
gaia>
```

### Example 2 - Salted SHA512 hash

```
[Expert@gaia:0]# grub2-mkpasswd-pbkdf2
Enter password: *******
Reenter password: *******
PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.B8A(---truncated---)7D0.017(---truncated---)623
[Expert@gaia:0]#

[Expert@gaia:0]# clish

gaia> set grub2-password-hash grub.pbkdf2.sha512.10000.B8A(---truncated---)7D0.017(---truncated---)623
gaia>

gaia> show configuration grub2-password
set grub2-password-hash grub.pbkdf2.sha512.10000.B8A(---truncated---)7D0.017(---truncated---)623
gaia>
```

# Proxy

## Proxy for Gaia Operating System

If this Gaia server connects to a network through a proxy server, then configure the applicable proxy server.

**Note** - This proxy configuration applies only to Gaia Operating System. It does not apply to Software Blades.

## Proxy for Check Point Servers

If your Management Server / Security Gateway / Cluster connects to Check Point servers to download updates and connect to ThreatCloud through a proxy server, you can configure the proxy server settings in SmartConsole:

| Location in SmartConsole | Description |
|---|---|
| **Menu** > **Global properties** > **Proxy** | This proxy configuration applies to the Management Server and all managed Security Gateways and Clusters. |
| Management Server / Security Gateway / Cluster object properties > **Network Management** > **Proxy** | This proxy configuration overrides the global proxy configuration in SmartConsole. |

**Note** - This proxy configuration applies only to Check Point Software Blades that run on top of Gaia Operating System.

## Security Gateway as an HTTP/HTTPS Proxy

You can configure a Security Gateway or Cluster as an HTTP/HTTPS Proxy. See the *R82 Quantum Security Gateway Guide* > Chapter "HTTP/HTTPS Proxy".

# Configuring Proxy in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Configuring a proxy server

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`). |
| 2 | Click **System Management > Proxy**. |
| 3 | Select **Use a Proxy server**. |
| 4 | Enter the applicable proxy server IP address or hostname. |
| 5 | Enter the applicable proxy server port. |
| 6 | Click **Apply**. |

### Editing the existing proxy server configuration

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`). |
| 2 | Click **System Management > Proxy**. |
| 3 | Enter the applicable proxy server IP address or hostname. |
| 4 | Enter the applicable proxy server port. |
| 5 | Click **Apply**. |

**Removing the existing proxy server configuration**

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`). |
| 2 | Click **System Management > Proxy**. |
| 3 | Clear **Use a Proxy server**. |
| 4 | Click **Apply**. |

# Configuring Proxy in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

## Syntax

### Configuring a proxy server or editing the existing proxy server configuration

```
set proxy address <IP Address or Hostname of the Proxy Server>
port <1-65535>
```

### Removing the existing proxy server configuration

```
delete proxy
      address
      all
      port
```

### Viewing the existing proxy server configuration

```
show proxy
      address
      port
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

# Time

All Security Management Servers, Security Gateways, and Cluster Members must synchronize their system clocks.

This is important for these reasons:

- SIC trust can fail if devices are not synchronized correctly.
- Cluster synchronization requires precise clock synchronization between members.
- SmartEvent Correlation uses time stamps that must be synchronized to approximately one a second.
- To make sure that cron jobs run at the correct time.
- To do certificate validation for applications based on the correct time.

You can use these methods to set the system date and time:

- Network Time Protocol (NTP).
- Manually, in the Gaia Portal, or Gaia Clish.

### Network Time Protocol (NTP)

NTP runs as a background client program on a client computer. It sends periodic time requests to specified servers to synchronize the client computer clock.

**Best Practice** - Configure more than one NTP server for redundancy.

# Configuring the Time and Date in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Configuring the Time and Date manually

| Step | Instructions |
|---|---|
| 1 | From the navigation tree, click **System Management** > **Time**. |
| 2 | Click **Set Time and Date**. |
| 3 | Click **Set Time and Date manually**. |
| 4 | Enter the time and date in the applicable fields. |
| 5 | Click **OK**. |

### Configuring the Time and Date automatically with an NTP Server

**Best Practice** - For redundancy, configure more than one NTP server, or configure an NTP Pool.

| Step | Instructions |
|---|---|
| 1 | From the navigation tree, click **System Management** > **Time**. |
| 2 | Click **Set Time and Date**. |
| 3 | Click **Set Time and Date automatically using Network Time Protocol (NTP)**. |
| 4 | Click **Add**. |
| 5 | In the **Type** field, select **Server**. |
| 6 | In the **Address** field, enter the Hostname or IP address of the NTP server. |
| 7 | In the **Version** field, select the NTP version of this server. |
| 8 | Click **Save**. |
| 9 | If you have two or more NTP servers / pools configured, then in the **Preferred Server** field, select the applicable NTP server / pool. |
| 10 | Click **OK**. |

### Configuring the Time and Date automatically with an NTP Pool

**Best Practice** - For redundancy, configure an NTP Pool.

An NTP Pool uses one IP address to represent a group of NTP servers.

| Step | Instructions |
|---|---|
| 1 | From the navigation tree, click **System Management** > **Time**. |
| 2 | Click **Set Time and Date**. |
| 3 | Click **Set Time and Date automatically using Network Time Protocol (NTP)**. |
| 4 | Click **Add**. |
| 5 | In the **Type** field, select **Pool**. |
| 6 | In the **Address** field, enter the Hostname or IP address of the NTP pool. |
| 7 | In the **Version** field, select the NTP version of this pool. |
| 8 | Click **Save**. |
| 9 | If you have two or more NTP pools / servers configured, then in the **Preferred Server/Pool** field, select the applicable NTP pool / server. |
| 10 | Click **OK**. |

### Editing a configured NTP Server / NTP Pool

| Step | Instructions |
|---|---|
| 1 | From the navigation tree, click **System Management** > **Time**. |
| 2 | Click **Set Time and Date**. |
| 3 | Click **Set Time and Date automatically using Network Time Protocol (NTP)**. |
| 4 | Click the applicable entry. |
| 5 | Click **Edit**. |
| 6 | Configure the applicable settings. |
| 7 | Click **Save**. |
| 8 | Click **OK**. |

### Deleting a configured NTP Server / NTP Pool

| Step | Instructions |
|---|---|
| 1 | From the navigation tree, click **System Management** > **Time**. |
| 2 | Click **Set Time and Date**. |
| 3 | Click **Set Time and Date automatically using Network Time Protocol (NTP)**. |
| 4 | Click the applicable entry. |
| 5 | Click **Remove**. |
| 6 | Click **Yes** to confirm. |
| 7 | Click **OK**. |

### Configuring the Time Zone

| Step | Instructions |
|---|---|
| 1 | From the navigation tree, click **System Management** > **Time**. |
| 2 | Click **Set Time Zone**. |
| 3 | Select the time zone from the list. |
| 4 | Click **OK**. |

# Configuring the Time and Date in Gaia Clish

**Important:**

- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### To show the current system Date and Time

#### Syntax

```
show clock
```

#### Example

```
gaia> show clock
Wed Jan  8 15:20:00 2020 GMT+1
gaia>
```

### Configuring and showing the Time

#### Syntax

- To configure the time:

  ```
  set time <Time of the Day>
  ```

- To show the current time:

  ```
  show time
  ```

#### Parameters

| Parameter | Description |
|---|---|
| *<Time of the Day>* | The current system time in HH:MM:SS format. |

### Configuring and showing the Date

#### Syntax

- To configure a date:

  ```
  set date <Date>
  ```

- To show the configured date:

  ```
  show date
  ```

#### Parameters

| Parameter | Description |
|---|---|
| *<date>* | The date in the YYYY-MM-DD format. |

#### Example

To configure the date to the 20th of January 2020, run:

```
gaia> set date 2020-01-20
```

### Configuring and showing the Time Zone

#### Syntax

- To configure the time zone:

```
set timezone <Area> / <Region>
```

**Important** - The spaces before and after the slash character (/) are mandatory.

- To show the configured time zone:

```
show timezone
```

#### Parameters

| Parameter | Description |
|---|---|
| *<Area>* | Continent or geographic area (case sensitive).<br>To see the valid values, select <SPACE> and <TAB>: |
| *<Region>* | Region within the specified area (case sensitive).<br>To see the valid values, select <SPACE> and <TAB>: |

#### Examples

```
gaia> set timezone America / Detroit
gaia> set timezone Asia / Tokyo
```

### Configuring and showing the NTP

**Best Practice** - For redundancy, configure more than one NTP server, or configure an NTP Pool.

#### Workflow

1. Add the required NTP servers / NTP pools (the default NTP version is 4):

   ```
   add ntp server address <IPv4 address or Hostname of NTP Server / NTP Pool> type {pool | server}
   ```

2. Optional: Add an NTP interface:

   ```
   add ntp interface <Name of Interface>
   ```

3. Configure the NTP version if it must be 3 or lower:

   ```
   set ntp server address <IPv4 address or Hostname of NTP Server / NTP Pool> version {1 | 2 | 3}
   ```

4. Optional: Configure the preferred NTP server / NTP pool:

   ```
   set ntp server preferred <IPv4 address or Hostname of NTP Server / NTP Pool>
   ```

5. Examine the NTP configuration:

   ```
   show ntp servers
   show ntp preferred
   show ntp interface
   ```

6. Enable the NTP configuration:

   ```
   set ntp active on
   ```

7. Save the changes

   ```
   save config
   ```

#### Syntax

- To add an NTP interface:

  By default, Gaia uses all interfaces to work with the configured NTP servers (based on the routing table).

You can configure Gaia to use only a specific interface to work with NTP.

To configure such an interface, it must have an IP address assigned.

```
add ntp interface <Name of Interface>
```

- To add a new NTP server:

  The default NTP version is 4.

  ```
  add ntp server address <IPv4 address or Hostname of NTP
  Server> type server
  ```

- To add a new NTP pool:

  The default NTP version is 4.

  ```
  add ntp server address <IPv4 address or Hostname of NTP
  Pool> type pool
  ```

- To configure the NTP settings:

  ```
  set ntp
        active {on | off}
        server
              address <IPv4 address or Hostname of NTP Server>
                    type {pool | server}
                    version {1|2|3|4}
              preferred <IPv4 address or Hostname of NTP
  Server / NTP Pool>
  ```

- To show NTP configuration:

  ```
  show ntp
        active
        current
        interface
        preferred
        servers
  ```

- To delete an NTP server / NTP pool:

  ```
  delete ntp server <IPv4 address or Hostname of NTP Server /
  NTP Pool>
  ```

- To delete an NTP interface:

If you delete all specific NTP interfaces, then by default, Gaia uses all interfaces to work with the configured NTP servers (based on the routing table).

```
delete ntp interface <Name of Interface>
```

### Parameters

| Parameter | Description |
|---|---|
| `active` | Shows the NTP status:<br>■ `Yes` - enabled<br>■ `No` - disabled |
| `current` | Shows the IP address or Host name of the NTP server / NTP pool that Gaia uses right now. |
| `interface` | Shows the specific NTP interfaces. |
| `servers` | Shows the configured NTP servers / NTP pools. |
| `active {on \| off}` | Enables (`on`) or disables (`off`) NTP. |
| `server` | Keyword that identifies the NTP server - time server, from which Gaia synchronizes its clock.<br>The specified time server does **not** synchronize to the local clock of Gaia. |
| `version {1\|2\|3\|4}` | Configures the version number of the NTP - 1, 2, 3, or 4.<br>**Best Practice** - Run NTP version 4. |
| `preferred` | Configured and shows the preferred NTP server / NTP pool. |
| *`<Name of Interface>`* | Press the TAB key to see the available interfaces. |

### Example

1. Add the required NTP servers / NTP pools (the default NTP version is 4):

```
gaia> add ntp server address ntp1.example.com type server
```

```
gaia> add ntp server address pool.ntp.org type pool
```

2. Add an NTP interface:

```
gaia> add ntp interface eth0
```

3. Optional: Configure the preferred NTP server / NTP pool:

```
gaia> set ntp server preferred ntp1.example.com
```

4. Examine the NTP configuration:

```
gaia> show ntp servers

IP Address                Type              Version
Preferred

ntp1.example.com          server            4         yes
pool.ntp.org              pool              4         no

gaia>
```

```
gaia> show ntp preferred
ntp1.example.com
gaia>
```

```
gaia> show ntp interface
eth0
gaia>
```

5. Enable the NTP configuration:

```
gaia> set ntp active on
```

6. Save the changes

```
gaia> save config
```

# Cloning Group

A Cloning Group is a collection of Gaia Security Gateways that synchronize their OS configurations and settings for a number of shared features, for example DNS or ARP.

**Important**:

- Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-4756).

# Configuring Cloning Groups in Gaia Portal

**Important**:

- Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-4756).
- If you change the members of a Gaia Cloning Group with many members down, you are logged out of the Gaia Portal with an incorrect error message:
  `Unable to connect to server`
  The correct message is:
  `An error occurred while applying configuration change to all cloning group members - the operation was successful only for online members.`
  This is the normal behavior of the cloning group. This error does not indicate a critical failure.

### Creating a new Cloning Group

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`). |
| 2 | Click **System Management > Cloning Group**. |
| 3 | Click **Start Cloning Group Creation Wizard**.<br>The **Cloning Group Creation Wizard** opens. |
| 4 | Select **Create a new Cloning Group**.<br>The **New Gaia Cloning Group** window opens.<br>a. In the **Cloning Group Name** field, enter a name for the Cloning Group.<br>b. In the **IP for cloning** field, select an IPv4 address (interface) for synchronizing settings between member Security Gateways.<br>Select an interface on a secure internal network.<br>c. In the **Password** field, enter a password for the administration account (*cadmin*).<br>This password is necessary to:<br>▪ Manage the Cloning Group<br>▪ Add other Security Gateways to the Cloning Group<br>▪ Create encrypted traffic between members of the Cloning Group<br>d. In the **Confirm Password** field, enter the password again. |

| Step | Instructions |
|---|---|
| 5 | In the **Shared Features** screen, select features to clone to other members of the Cloning Group.<br>Pay attention to the features you want to clone.<br>For example, you might not want to clone static routes to Security Gateways that are members of a cluster. |
| 6 | Click **Next** for the **Wizard Summary**. |
| 7 | Click **Finish**. |

### List of Shared Features

The features are listed in the same order, in which they are shown in Gaia Portal.

Table: Shared Features in Gaia Portal

| Shared Feature | Description |
|---|---|
| SNMP | Configure SNMP. |
| Banner Messages | Configure banner messages. |
| Job Scheduler | Schedule automated tasks that perform actions at a specific time. |
| DNS | Configure DNS servers. |
| ARP | Configure static ARP entries and proxy ARP entries, control dynamic ARP entries. |
| System Logging | Configure system logging settings. |
| Host Access Control | Configure which hosts are allowed to connect to the cluster devices. |
| Proxy Settings | Configure proxy settings. |
| Host Address Assignment | Configure known hosts. |
| NTP | Configure Network Time Protocol for synchronizing the system's clock over a network. |
| Password Policy | Configure password and account policies. |
| Time | Configure the time and date of the system. |
| Network Access | Configure network access to Gaia. |
| Display Format | Configure how the system displays time, date and netmask. |
| Mail Notification | Configure email address, to which Gaia sends mail notifications. |
| Inactivity timeout | Configure session parameters, such as inactivity timeout. |
| Users and Roles | Configure users and roles settings. |

Table: Shared Features in Gaia Portal (continued)

| Shared Feature | Description |
|---|---|
| Static Routes | Configure static routes. |
| DHCP Relay | Configure relay of DHCP and BOOTP messages between clients and servers on different IPv4 Networks. |
| IPv6 DHCP Relay | Configure relay of DHCPv6 messages between clients and servers on different IPv6 Networks. |
| BGP | Configure dynamic routing via the Border Gateway Protocol. |
| IGMP | Establish multicast group memberships via the Internet Group Management Protocol. |
| PIM | Configure Protocol-Independent Multicast. |
| Static Multicast Routes | Configure static multicast routes. |
| RIP | Configure IPv4 dynamic routing via the Routing Information Protocol. |
| RIPng | Configure IPv6 dynamic routing via the Routing Information Protocol. |
| OSPF | Configure IPv4 dynamic routing via the Open Shortest-Path First v2 protocol. |
| IPv6 OSPF | Configure IPv6 dynamic routing via the Open Shortest-Path First v3 protocol. |
| Route Aggregation | Create a supernet network from the combination of networks with a common routing prefix. |
| Inbound Route Filters | Configure Inbound Route Filters for RIP, OSPFv2, BGP, and OSPFv3 (supports IPv4 and IPv6). |
| IP Reachability Detection | Configure reachability detection of IP Addresses. |
| Route Redistribution | Configure advertisement of routing information from one protocol to another (supports IPv4 and IPv6). |
| Route Map | Configure dynamic routing route maps. |

Table: Shared Features in Gaia Portal (continued)

| Shared Feature | Description |
|---|---|
| Prefix Lists and Trees | Configure dynamic routing prefix lists and trees. |
| Routing Options | Configure protocol ranks and trace (debug) options. |
| Policy Based Routing | Configure policy based routing (PBR) priority rules and action tables. |
| Scheduled Backups | Configure Gaia scheduled backups. |

### Managing a Cloning Group

| Step | Instructions |
|---|---|
| 1 | Sign out of the Gaia Portal. |
| 2 | Sign in *to the same Gaia Portal* using the *cadmin* account and password. (Alternatively, log in to the Gaia Portal on the Security Gateway using the *cadmin* credentials.)<br>**Important** - No unique URL or IP address is needed to access the Cloning Group Portal or Clish command line. Use the URL or IP address of the member Security Gateway. |
| 3 | In **System Management > Cloning Group**, select features from the **Shared Features**. |
| 4 | Click **Set Shared Features**.<br>The shared features are propagated to all members of the group.<br>If, for example, you then configure a primary DNS server on one member of the Cloning Group, and DNS is one of the **Shared Features**, then the DNS settings are propagated to all members of the group. The DNS settings in the Portal of each member are grayed out. |

**Note** - A user that gets cloning group administration privileges (the RBA role `CloningGroupManagement`), can manage specific Cloning Groups features granted by the administrator and grant Cloning Group capabilities to other users, including remote users. When these privileges are assigned, the **Group Mode** button shows in Gaia Portal.

**Managing a Cloning Group as an assigned administrator**

| Step | Instructions |
|---|---|
| 1 | Connect to the Gaia Portal on a Cloning Group member Security Gateway.<br>With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`). |
| 2 | At the top, click **Group Mode**.<br>The Security Gateway switches to Cloning Group management mode. |

**Joining an existing Cloning Group**

| Step | Instructions |
|---|---|
| 1 | Connect to the Gaia Portal on a Security Gateway.<br>With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`). |
| 2 | In **System Management > Cloning Group**, click **Start Cloning Group Creation Wizard**.<br>The **Cloning Group Wizard** opens. |
| 3 | Select **Join an existing Cloning Group**. |
| 4 | The **Join Existing Cloning Group** window opens.<br>■ In the **Remote Member Address** field, enter the IPv4 address of a remote member of the Cloning Group.<br>■ In the **IP for cloning** field, select an IP address (interface) for synchronizing the settings between Security Gateways.<br>Select an interface on a secure internal network. Make sure there is a physical connectivity to the Gaia computer that runs the Cloning Group, to which you wish to join.<br>■ In the **Password** field, enter a password for the Cloning Group administration account (*cadmin*).<br>(The same password you entered when you created the Cloning Group, to which you wish to join.)<br>The *cadmin* password:<br>• Lets you log in to the *cadmin* account<br>• Is used to create authentication credentials for members during synchronization |
| 5 | Click **Finish**. |

### Creating a Cloning Group that follows ClusterXL

Select this option, if the Security Gateway is a member of a ClusterXL.

**Important** - In a Cluster, you must configure all the Cluster Members in the same way.

| Step | Instructions |
|---|---|
| 1 | Connect to the Gaia Portal on a Security Gateway.<br>With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`). |
| 2 | In **System Management > Cloning Group**, click **Start Cloning Group Creation Wizard**.<br>The **Cloning Group Creation Wizard** opens. |
| 3 | Select **Cloning group follows ClusterXL**.<br>■ Enter the Cloning Group name.<br>■ Enter a password for the Cloning Group administration account (*cadmin*). |
| 4 | Click **Next** for the **Wizard Summary**. |
| 5 | Click **Finish**. |
| 6 | Repeat Steps 1-5 for all members of the cluster. |

**Note** - For troubleshooting steps, refer to sk119496.

# Configuring Cloning Groups in Gaia Clish

*In This Section:*



**Note** - When run from the *cadmin* account, these commands apply to all members of the Gaia group.

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-4756).

## Cloning Group Modes

You can create Cloning Groups in either **Manual** mode, or **ClusterXL** mode.

### Creating the first Cloning Group member in Manual mode

| Step | Instructions |
|---|---|
| 1 | Set the cloning group mode to `manual`. |
| 2 | Set the cloning group local IP address. |
| 3 | Set the cloning group password. |
| 4 | Set the cloning group state to `on`. |
| 5 | **Optional:** Set a name for the Cloning Group. |

### Adding other Security Gateways to the Cloning Group in Manual mode

Perform these steps on each of the Security Gateways.

| Step | Instructions |
|---|---|
| 1 | Set the cloning group mode to `manual`. |
| 2 | Set the cloning group local IP address. |
| 3 | Set the cloning group password. |
| 4 | Run the "`join cloning group`" command to join the Cloning Group. |

### Creating Cloning Group members in ClusterXL mode

Perform these steps on all member Security Gateways.

| Step | Instructions |
|---|---|
| 1 | Set the cloning group mode to `ClusterXL`. |
| 2 | Set the cloning group password. |
| 3 | Set the cloning group state to `on`. |

## CLI Syntax

### Creating and configuring a Cloning Group

#### Syntax

```
set cloning-group
      local-ip <IPv4 address>
      mode {manual | cluster-xl}
      name <Name of Cloning Group>
      password <Password>
      state {on | off}
```

### Parameters

| Parameter | Description |
|---|---|
| `local-ip <IPv4 address>` | The IPv4 address used to synchronize shared features between members of the Cloning Group. |
| `mode {manual \| cluster-xl}` | The mode determines whether the Cloning Group is defined manually, or through ClusterXL. |
| `name <Name of Cloning Group>` | Name of the Cloning Group. |
| `password <Password>` | Password for the administrator's (cadmin) account, used to access the Cloning Group configuration in the Gaia Portal, or Gaia Clish. When prompted, enter and confirm the password. |
| `state {on \| off}` | Enables (`on`) or disables (`off`) the Cloning Group feature.<br>**Important** - When you configure the state "`off`", the Security Gateway is removed from the Cloning Group. |

## Adding Shared Features

### Syntax

```
add cloning-group shared-feature <Feature>
```

### Parameters

| Parameter | Description |
|---|---|
| `<Feature>` | The name of the feature to be synchronized between the members of the Cloning Group. |

### List of Shared Features

The features are listed in the same order, in which they are shown in Gaia Clish when you run the "`show cloning-group shared-feature`" command.

Table: Shared Features in Gaia Clish

| Name of Shared Feature | Description |
|---|---|
| `aggregate` | Configure route aggregation - create a supernet network from the combination of networks with a common routing prefix. |
| `bgp` | Configure dynamic routing via the Border Gateway Protocol. |
| `bootp` | Configure IPv4 DHCP Relay - relay of DHCP and BOOTP messages between clients and servers on different IPv4 Networks. |
| `cron` | Configure job scheduler - schedule automated tasks that perform actions at a specific time. |
| `dhcp6relay` | Configure IPv6 DHCP Relay - relay of DHCPv6 messages between clients and servers on different IPv6 Networks. |
| `dns` | Configure DNS servers. |
| `hosts` | Configure known hosts. |
| `igmp` | Establish multicast group memberships via the Internet Group Management Protocol. |
| `inboundfilters` | Configure Inbound Route Filters for RIP, OSPFv2, BGP, and OSPFv3 (supports IPv4 and IPv6). |
| `ipreachdetect` | Configure reachability detection of IP Addresses. |
| `time` | Configure the time and date of the system. |
| `ntp` | Configure Network Time Protocol (NTP) for synchronizing the system's clock over a network. |
| `message` | Configure banner messages. |
| `ospf` | Configure IPv4 dynamic routing via the Open Shortest-Path First v2 protocol. |
| `ospf3` | Configure IPv6 dynamic routing via the Open Shortest-Path First v3 protocol. |
| `password-controls` | Configure password and account policies. |

Table: Shared Features in Gaia Clish (continued)

| Name of Shared Feature | Description |
|---|---|
| `mailrelay` | Configure email address, to which Gaia sends mail notifications. |
| `display-format` | Configure how the system displays time, date and netmask. |
| `http` | Configure session parameters, such as inactivity timeout. |
| `net-access` | Configure network access to Gaia. |
| `users-and-roles` | Configure users and roles settings. |
| `arp` | Configure static ARP entries and proxy ARP entries, control dynamic ARP entries. |
| `syslog` | Configure system logging settings. |
| `proxy` | Configure proxy settings. |
| `host-access` | Configure which hosts are allowed to connect to the cluster devices. |
| `pbr` | Configure policy based routing (PBR) priority rules and action tables. |
| `pim` | Configure Protocol-Independent Multicast. |
| `prefix` | Configure dynamic routing prefix lists and trees. |
| `redistribution` | Configure route redistribution - advertisement of routing information from one protocol to another (supports IPv4 and IPv6). |
| `rip` | Configure IPv4 dynamic routing via the Routing Information Protocol. |
| `ripng` | Configure IPv6 dynamic routing via the Routing Information Protocol. |
| `routemap` | Configure dynamic routing route maps. |
| `routingoptions` | Configure protocol ranks and trace (debug) options. |
| `static` | Configure static routes. |

Table: Shared Features in Gaia Clish (continued)

| Name of Shared Feature | Description |
|---|---|
| `static-mroute` | Configure static multicast routes. |
| `snmp` | Configure SNMP. |
| `backup` | Configure Gaia scheduled backups. |

### Deleting Shared Features

#### Syntax

```
delete cloning-group shared-feature <Feature>
```

#### Parameters

| Parameter | Description |
|---|---|
| *<Feature>* | The name of the feature to be deleted from the list of shared features.<br>To see the list of the enabled Shared Features:<br>a. Enter:<br>`delete cloning-group shared-feature`<br>b. Press <SPACE> and <TAB>. |

### Joining an existing Cloning Group

#### Syntax

```
join cloning-group remote-ip <IPv4 address of Cloning Group>
```

#### Parameters

| Parameter | Description |
|---|---|
| *<IPv4 address of Cloning Group>* | The IPv4 address of the Cloning Group member, to which you join.<br>**Note** - This option is not available, if you are logged into the *cadmin* account. |

### Removing a member from a Cloning Group

```
leave cloning-group
```

### Removing an inaccessible Cloning Group member

#### Syntax

```
delete cloning-group disconnected-member <IPv4 address of Member>
```

#### Parameters

| Parameter | Description |
|---|---|
| *<IPv4 address of Member>* | The IPv4 address of the Cloning Group member that became inaccessible. |

**Important** - Use this command only for troubleshooting purposes, when the remote Cloning Group member is not accessible. A normal way to remove a member from a Cloning Group is to run the "`leave cloning-group`" command on that member.

**Notes:**

- The Cloning Group configuration on the remote member itself does not change, and as soon as the device regains connectivity, it joins the Cloning Group again.
- This command can only be run if the Cloning Group is in Manual mode.

### Viewing the Cloning Group configuration

#### Syntax

```
show cloning-group
      local-ip
      members
      mode
      name
      shared-feature
      state
      status
```

### Parameters

| Parameter | Description |
|---|---|
| `local-ip` | The IPv4 address used to synchronize shared features between the members of the Cloning Group. |
| `members` | Shows the members of the Cloning Group. |
| `mode` | Shows the Cloning Group mode - `Manual`, or `Cluster XL` |
| `name` | Shows the name of the Cloning Group |
| `shared-feature` | Lists the shared features that are enabled to be used by all members of the Cloning Group. |
| `state` | Shows the Cloning Group state - enabled, or disabled. |
| `status` | Shows the status of the Cloning Group member.<br>**Note** - This option is not available, if you are logged into the *cadmin* account. |

## Synchronizing a member in the Cloning Group

```
re-synch cloning-group
```

## Enabling or disabling the Cloning Group management mode

When a user (local or remote) receives Cloning Group management privileges, the user can enable (or disable) the Cloning Group management mode, to create, delete, and edit Cloning Groups.

### Syntax

```
set cloning-group-management {on | off}
```

### Parameters

| Parameter | Description |
|---|---|
| `on` | Enables the Cloning Group management mode. |
| `off` | Disables the Cloning Group management mode. |

# SNMP

*In This Section:*



## Introduction

Simple Network Management Protocol (SNMP) is an Internet standard protocol. SNMP is used to send and receive management information to other network devices. SNMP sends messages, called protocol data units (PDUs), to different network parts. SNMP-compliant devices, called agents, keep data about themselves in Management Information Bases (MIBs) and resend this data to the SNMP requesters.

Through the SNMP protocol, network management applications can query a management agent using a supported MIB. The Check Point SNMP implementation lets an SNMP manager monitor the system and modify selected objects only. You can define and change one read-only community string and one read-write community string. You can set, add, and delete trap receivers and enable or disable various traps. You can also enter the location and contact strings for the system.

**Notes:**

- The Check Point implementation also supports the User-based Security model (USM) portion of SNMPv3.
- The Gaia implementation of SNMP is built on NET-SNMP.
  Changes were made to the first version to address security and other fixes.
  For more information, see *Net-SNMP*.
- Scalable Platform Security Groups support only this SNMP OID branch:
  OID 1.3.6.1.4.1.2620.1.48
  `iso.org.dod.internet.private.enterprise.checkpoint.products.asg`
  To see VPN status, you can use the `tunnelTable` branch (OID 1.3.6.1.4.1.2620.500.9002.1).
- Scalable Platform Security Groups support only this SNMP trap:
  OID 1.3.6.1.4.1.2620.1.2001
  `iso.org.dod.internet.private.enterprise.checkpoint.products.asg Trap`

**Warning** - If you use SNMP, we recommend that you change the community strings for security purposes. If you do not use SNMP, disable SNMP or the community strings.

To view detailed information about each MIB that the Check Point implementation supports (also, see sk90470):

| MIB | Location |
|---|---|
| Standard MIBs | `/usr/share/snmp/mibs/*.txt` |
| Check Point MIBs | `$CPDIR/lib/snmp/chkpnt.mib`<br>`$CPDIR/lib/snmp/chkpnt-trap.mib` |
| Check Point Gaia trap MIB | `/etc/snmp/GaiaTrapsMIB.mib` |

SNMP, as implemented on Check Point platforms, enables an SNMP manager to monitor the device using `GetRequest`, `GetNextRequest`, `GetBulkRequest`, and a select number of traps.

The Check Point implementation also supports using `SetRequest` to change these attributes: `sysContact`, `sysLocation`, and `sysName`. You must configure read-write permissions for set operations to work.

Check Point Gaia supports SNMP v1, v2, and v3.

Use Gaia to run these tasks:

- Define and change one read-only community string.
- Define and change one read-write community string.
- Enable and disable the SNMP daemon.
- Create SNMP users.
- Change SNMP user accounts.
- Add or delete trap receivers.
- Enable or disable the various traps.
- Enter the location and contact strings for the device.

# SNMP v3 - User-Based Security Model (USM)

Gaia supports the user-based security model (USM) component of SNMPv3 to supply message-level security. With USM (described in RFC 3414), access to the SNMP service is controlled based on user identities. Each user has a name, an authentication pass phrase (used for identifying the user), and an optional privacy pass phrase (used for protection against disclosure of SNMP message payloads).

The system uses the MD5 hashing algorithm to supply authentication and integrity protection and DES to supply encryption (privacy).

**Best Practice** - Use authentication and encryption. You can use them independently by specifying one or the other with your SNMP manager requests. The Gaia responds accordingly.

SNMP users are maintained separately from system users. You can create SNMP user accounts with the same names as existing user accounts or different. You can create SNMP user accounts that have no corresponding system account. When you delete a system user account, you must separately delete the SNMP user account.

# Enabling SNMP

The SNMP daemon is disabled by default.

If you choose to use SNMP, enable and configure it according to your security requirements.

At minimum, you must change the default community string to something other than public.

You can choose to use all versions of SNMP (v1, v2, and v3) on your system, or to grant SNMPv3 access only.

**Best Practice** - If your SNMP management station supports SNMP v3, select only SNMP v3 on Gaia. SNMPv3 limits community access. Only requests from users with enabled SNMPv3 access are allowed, and all other requests are rejected.

**Note** - If you do not plan to use SNMP to manage the network, disable it. Enabling SNMP opens potential attack vectors for surveillance activity. It lets an attacker learn about the configuration of the device and the network.

# SNMP Agent Address

An SNMP Agent address is a specified IP address, on which the SNMP agent listens and reacts to requests.

The default behavior is for the SNMP agent to listen to and react to requests on all interfaces. If you specify one or more agent addresses, the system SNMP agent listens and responds only on those interfaces.

You can use the agent address as a different method to limit SNMP access. For example: you can limit SNMP access to one secure internal network that uses a specified interface. Configure that interface as the only agent address.

# SNMP Traps

Managed devices use trap messages to report events to the Network Management Station (NMS).

When some types of events occur, the platform sends a trap to the management station.

The Gaia proprietary traps are defined in the `/etc/snmp/GaiaTrapsMIB.mib` file.

Gaia supports these types of SNMP traps:

Table: SNMP Traps in Gaia

| Type of Trap | Description |
|---|---|
| `coldStart` | Notifies when the SNMPv2 agent is re-initialized. |
| `linkUpLinkDown` | Notifies when one of the links changes state to up or down. |
| `authorizationError` | Notifies when an SNMP operation is not properly authenticated. |
| `configurationChange` | Notifies when a change to the system configuration is applied. |
| `configurationSave` | Notifies when a permanent change to the system configuration occurs. |
| `lowDiskSpace` | Notifies when space on the system disk is low.<br>Sent if the disk space utilization in the `/` partition has reached 80 percent or more of its capacity. |
| `powerSupplyFailure` | Notifies when a power supply for the system fails.<br>This trap is supported only on platforms with two power supplies installed and running. |
| `fanFailure` | Notifies when a CPU or chassis fan fails. |
| `overTemperature` | Notifies when the temperature rises above the threshold. |
| `highVoltage` | Notifies if one of the voltage sensors exceeds its maximum value. |
| `lowVoltage` | Notifies if one of the voltage sensors falls below its minimum value. |

Table: SNMP Traps in Gaia (continued)

| Type of Trap | Description |
|---|---|
| `raidVolumeState` | Notifies if the raid volume state is not optimal.<br>This trap works only if RAID is supported on the Gaia computer.<br>To make sure that RAID monitoring is supported, run the command `raid_diagnostic` and confirm that it shows the RAID status. |
| `biosFailure` | Notifies when the Primary BIOS failure is detected.<br>Sent once the event occurs. Applies to computers with Dual BIOS. |
| `vrrpv2AuthFailure` | Notifies when the VRRP Cluster Member has packet an authentication failure in VRRPv2 (IPv4) and VRRPv3 (IPv6).<br>Sent each polling interval. |
| `vrrpv2NewMaster` | Notifies when the VRRP Cluster Member transitioned to VRRP Master state in VRRPv2 (IPv4).<br>Sent each polling interval. |
| `vrrpv3NewMaster` | Notifies when the VRRP Cluster Member transitioned to VRRP Master state in VRRPv3 (IPv6).<br>Sent each polling interval. |
| `vrrpv3ProtoError` | Notifies when the VRRP Cluster Member has a protocol error in VRRPv2 (IPv4) and VRRPv3 (IPv6).<br>Sent each polling interval. |

**Important** - For Scalable Platforms, see the *R82 Scalable Platforms Administration Guide*.

# Configuring SNMP in Gaia Portal

For detailed information, see sk90860: How to configure SNMP on Gaia OS.

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Enabling SNMP

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **SNMP**. |
| 2 | Select **Enable SNMP Agent**. |
| 3 | In the **Version** drop down list, select the version of SNMP to run:<br>■ **1/v2/v3 (any)**<br>Select this option if your SNMP management station does not support SNMPv3.<br>■ **v3-Only**<br>Select this option if your SNMP management station supports v3.<br>SNMPv3 provides a higher level of security than v1 or v2. |
| 4 | In **SNMP Location String**, enter a string that contains the location for the system.<br>The maximum length for the string is 128 characters.<br>That includes letters, numbers, spaces, special characters<br>For example: `Bldg 1, Floor 3, WAN Lab, Fast Networks, Speedy, CA` |
| 5 | In **SNMP Contact String**, enter a string that contains the contact information for the device.<br>The maximum length for the string is 128 characters.<br>That includes letters, numbers, spaces, special characters.<br>For example: `John Doe, Network Administrator, (111) 222-3333` |
| 6 | Click **Apply**. |

### Configuring an SNMP Agent interface

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **SNMP**.<br>The SNMP Addresses table shows the applicable interfaces and their IP addresses. |
| 2 | By default, all interfaces are selected. You can select the individual interfaces. |

**Note** - If you do not specify agent addresses, the SNMP protocol responds to requests from all interfaces.

### Configuring the SNMP community strings

| Step | Instructions |
|---|---|
| 1 | In the **V1/V2 Settings** section, in **Read Only Community String**, set a string other than **public**.<br>You must always use this is a basic security precaution. |
| 2 | Optional.<br>Set a **Read-Write Community String**.<br>**Warning** - Set a read-write community string only if you have reason to enable set operations, and if your network is secure. |

## Configuring USM users

### Adding a USM user

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **SNMP**. |
| 2 | In the **V3 - User-Based Security Model (USM)** section, click **Add**.<br>The **Add New USM User** window opens. |
| 3 | In the **User Name**, enter the applicable user name.<br>This can be the same as a user name for system access.<br>**Notes:**<br>■ This string must contain alphanumeric characters with no spaces, backslash, or colon characters.<br>■ The length of this string is between 1 and 31 characters on Management Server, Log Servers, and Security Gateways that run in the Gateway mode with MDPS disabled.<br>■ The length of this string is between 1 and 26 characters on Security Gateways that run in the VSX mode or with MDPS enabled. |
| 4 | In the **Security Level**, select one of these options from the drop-down list:<br>■ **authPriv** - The user has authentication and privacy pass phrases and can connect with privacy encryption.<br>■ **authNoPriv** - The user has only an authentication pass phrase and can connect only without privacy encryption. |
| 5 | In the **User Permissions**, select one of these options from the drop-down list:<br>■ **read-only**<br>■ **read-write** |
| 6 | In the **Authentication Protocol**, select one of these options from the drop-down list:<br>■ **SHA256**<br>■ **SHA512**<br>The default is **SHA512**.<br>**Note** - When you change the configured **Authentication Protocol** of an existing SNMPv3 USM user, Gaia OS requires you to change the **Authentication Pass Phrase** because the previous password is not valid anymore. |

| Step | Instructions |
|---|---|
| 7 | In the **Authentication Pass Phrase**, enter a password for the user that is between 8 and 128 characters in length. |
| 8 | In the **Privacy Protocol**, select:<br>▪ **DES**<br>▪ **AES**<br>▪ **AES256**<br>The default is **DES**.<br>**Note** - When you change the configured **Privacy Protocol** of an existing SNMPv3 USM user, Gaia OS requires you to change the **Privacy Pass Phrase** because the previous password is not valid anymore. |
| 9 | In the **Privacy Pass Phrase**, enter a pass phrase that is between 8 and 128 characters in length.<br>Used for protection against disclosure of SNMP message payloads. |
| 10 | Click **Save**.<br>The new user shows in the table. |

### Editing a USM user

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **SNMP**. |
| 2 | In the **V3 - User-Based Security Model (USM)** section, select the user and click **Edit**.<br>The **Edit USM User** window opens. |
| 3 | You can change the **Security Level**, **User Permissions**, the **Authentication Protocol**, the **Authentication Passphrase**, or the **Privacy Protocol**. |
| 4 | Click **Save**. |

### Deleting a USM user

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **SNMP**. |
| 2 | In the **V3 - User-Based Security Model (USM)** section, select the user and click **Remove**.<br>The **Deleting USM User Entry** window opens. |
| 3 | The window shows this message:<br>**Are you sure you want to delete "username" entry?**.<br>Click **Yes**. |

### Enabling or disabling SNMP trap types

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **SNMP**. |
| 2 | In the **Enabled Traps** section, click **Set**.<br>The **Add New Trap Receiver** window opens.<br>■ To enable a trap:<br>Select it from the **Disabled Traps** list, and click **Add>**<br>■ To disable a trap:<br>Select it from the **Enabled Traps** list, and click **Remove>** |
| 3 | Click **Save**. |
| 4 | Add a USM user.<br>You must do this even if you use only SNMPv1 or SNMPv2.<br>In the **Trap User**, select an SNMP user. |
| 5 | In **Polling Frequency**, specify the number of seconds between polls. |
| 6 | Click **Apply**. |

## Configuring SNMP trap receivers

### Adding an SNMP trap receiver

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **SNMP**. |
| 2 | In the **Trap Receivers Settings** section, click **Add**.<br>The **Add New Trap Receiver** window opens. |
| 3 | In the **IPv4 Address**, enter the IP address of an SNMP receiver. |
| 4 | In the **Version**, select the SNMP Version for the specified receiver. |
| 5 | In the **Community String**, enter the SNMP community string for the specified receiver. |
| 6 | Click **Save**. |

### Editing an SNMP trap receiver

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **SNMP**. |
| 2 | In the **Trap Receivers Settings** section, select the SNMP receiver and click **Edit**.<br>The **Edit Trap Receiver** window opens. |
| 3 | You can change the SNMP version or the SNMP community string. |
| 4 | Click **Save**. |

### Deleting an SNMP trap receiver

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **SNMP**. |
| 2 | In the **Trap Receivers Settings** section, select the SNMP trap receiver and click **Remove**.<br>The **Deleting Trap Receiver Entry** window opens. |
| 3 | The window shows this message: **Are you sure you want to delete "IPv4 address" entry?**<br>Click **Yes**. |

## Configuring custom SNMP traps

**Adding a custom SNMP trap**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **SNMP**. |
| 2 | In the **Custom Traps** section, click **Add**.<br>The **Add New Custom Trap** window opens. |
| 3 | In the **Trap Name**, enter the name of an SNMP trap.<br>Range: 1 - 128 characters. |
| 4 | In the **OID**, enter the SNMP OID to query.<br>■ The OID value can contain only numbers and periods (sub-identifiers separated by periods).<br>■ The OID value can contain from 2 to 128 sub-identifiers: from `X.X` to `X.X.` (124 sub-identifiers more)<br>■ Number range of each sub-identifier: 0 - 4294967295.<br>■ The first sub-identifier must be one of these numbers:<br>• `0`<br>In this case, the second sub-identifier must be between 0-39: `0.<0-39>.` (other applicable sub-identifiers)<br>• `1`<br>In this case, the second sub-identifier must be between 0-39: `1.<0-39>.` (other applicable sub-identifiers)<br>• `2`<br>`2.X.` (other applicable sub-identifiers) |
| 5 | In the **Operator** field, select the applicable operator to examine the value the SNMP OID to query returns:<br>■ **Equal** - The returned value is equal to the value in the **Threshold** field.<br>■ **Not_Equal** - The returned value is not equal to the value in the **Threshold** field.<br>■ **Less_Than** - The returned value is less than the value in the **Threshold** field.<br>■ **Greater_Than** - The returned value is greater than the value in the **Threshold** field.<br>■ **Changed** - The returned value is different than the returned value in the previous SNMP OID query. |
| 6 | In the **Threshold**, enter an integer value to which Gaia operating system compares the value returned in the SNMP OID query.<br>Range: 1 - 128 characters. |

| Step | Instructions |
|---|---|
| 7 | In the **Frequency**, enter the interval (in seconds) between the SNMP OID queries.<br>Range: 1 - 4294967295. |
| 8 | In the **Message**, enter the applicable text.<br>This is the message you get in the SNMP Trap packets the Gaia operating system sends.<br>Range: 1 - 128 characters. |
| 9 | Click **Save**. |

### Editing a custom SNMP trap

For explanations, see the section "Adding a custom SNMP trap".

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **SNMP**. |
| 2 | In the **Custom Traps** section, select the custom SNMP trap and click **Edit**.<br>The **Edit Custom Trap** window opens. |
| 3 | Configure the applicable settings. |
| 6 | Click **Save**. |

### Deleting a custom SNMP trap

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **SNMP**. |
| 2 | In the **Custom Traps** section, select the custom SNMP trap and click **Remove**. |
| 3 | The window shows this message: **Are you sure you want to delete "<Name of Custom Trap>" entry?**<br>Click **Yes**. |

## Working with SNMP Traps on Scalable Platforms

See the *R82 Scalable Platforms Administration Guide*.

# Configuring SNMP in Gaia Clish

For detailed information, see sk90860: How to configure SNMP on Gaia OS.

**Important:**

- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- Scalable Platforms do **not** support the "`set snmp traps`" command.
  You must use the "`asg alert`" configuration wizard to configure SNMP traps in Gaia gClish.
- After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

**Best Practice:**
For commands that include "`auth-pass-phrase`", "`privacy-pass-phrase`", or both, use the hashed commands.
To get the hashed password, run the "`show configuration snmp`" command.

### Syntax for the 'add' commands

**Note** - To see all available commands:

1. Enter:
   `add snmp`
2. Press <SPACE>
3. Press <ESC><ESC>

### Syntax

```
add snmp interface <Name of Interface>
```

```
add snmp traps receiver <IPv4 address> version {v1 | v2 | v3}
community <String>
add snmp custom-trap <Custom Trap Name> oid <Value> operator
<Logical Operator> threshold <Value> frequency <Value> message
"<Text>"
```

```
add snmp usm user <UserName> security-level authPriv auth-pass-
phrase <Pass Phrase> privacy-pass-phrase <Privacy Pass Phrase>
privacy-protocol {DES | AES} authentication-protocol {MD5 |
SHA1}
add snmp usm user <UserName> security-level authPriv auth-pass-
phrase-hashed <Hashed Pass Phrase> privacy-pass-phrase <Privacy
Pass Phrase> privacy-protocol {DES | AES} authentication-
protocol {MD5 | SHA1}
add snmp usm user <UserName> security-level authNoPriv auth-
pass-phrase <Pass Phrase> authentication-protocol {MD5 | SHA1}
add snmp usm user <UserName> security-level authNoPriv auth-
pass-phrase-hashed <Hashed Pass Phrase>
```

## Description of commands

| Command | Description |
|---|---|
| `add snmp custom-trap ...` | Adds a custom SNMP trap:<br>■ `<Custom Trap Name>`<br>Specifies the name of the custom trap.<br>Range: 1 - 128 characters.<br>■ `oid <Value>`<br>Specifies the SNMP OID to query.<br>• The OID value can contain only numbers and periods (sub-identifiers separated by periods).<br>• The OID value can contain from 2 to 128 sub-identifiers:<br>from `X.X` to `X.X.` (124 sub-identifiers more)<br>• Number range of each sub-identifier: 0 - 4294967295.<br>• The first sub-identifier must be one of these numbers:<br>◦ `0`<br>In this case, the second sub-identifier must be between 0-39:<br>`0.<0-39>.` (other applicable sub-identifiers)<br>◦ `1`<br>In this case, the second sub-identifier must be between 0-39:<br>`1.<0-39>.` (other applicable sub-identifiers)<br>◦ `2`<br>`2.X.` (other applicable sub-identifiers)<br>■ `operator <Logical Operator>`<br>Specifies the operator to examine the value the SNMP OID to query returns:<br>• `Equal` - The returned value is equal to the value in the "`threshold`" parameter.<br>• `Not_Equal` - The returned value is not equal to the value in the "`threshold`" parameter.<br>• `Less_Than` - The returned value is less than the value in the "`threshold`" parameter.<br>• `Greater_Than` - The returned value is greater than the value in the "`threshold`" parameter.<br>• `Changed` - The returned value is different than the returned value in the previous SNMP OID query.<br>■ `threshold <Value>`<br>Specifies an integer value to which Gaia operating system compares the value returned in the SNMP OID query.<br>Range: 1 - 128 characters.<br>■ `frequency <Value>` |

| Command | Description |
|---|---|
| | Specifies the interval (in seconds) between the SNMP OID queries.<br>Range: 1 - 4294967295.<br>■ `message "<Text>"`<br>Specifies the applicable text.<br>This is the message you get in the SNMP Trap packets the Gaia operating system sends.<br>Range: 1 - 128 characters. |
| `add snmp interface ...` | Adds a local interface to the list of local interfaces, on which the SNMP daemon listens. |
| `add snmp traps receiver ...` | Adds a SNMP Trap Sink. |
| `add snmp usm user ...` | Adds an SNMPv3 USM user.<br>**Notes:**<br>■ This string must contain alphanumeric characters with no spaces, backslash, or colon characters.<br>■ The length of this string is between 1 and 31 characters on Management Server, Log Servers, and Security Gateways that run in the Gateway mode with MDPS disabled.<br>■ The length of this string is between 1 and 26 characters on Security Gateways that run in the VSX mode or with MDPS enabled. |

### Syntax for the 'set' commands

**Note** - To see all available commands:

1. Enter:
   `set snmp`
2. Press <SPACE>
3. Press <ESC><ESC>

### Syntax

```
set snmp agent {on | off}
set snmp agent-version {any | v3-Only}
```

| |
|---|
| set snmp clear-trap interval <*Value*> retries <*Value*><br>set snmp custom-trap <*Custom Trap Name*> oid <*Value*> operator <*Logical Operator*> threshold <*Value*> frequency <*Value*> message "<*Text*>"<br>set snmp traps coldStart-threshold <*Seconds*><br>set snmp traps polling-frequency <*Seconds*><br>set snmp traps receiver <*IPv4 address*> version {v1 \| v2 \| v3} community <*String*><br>set snmp traps trap {authorizationError \| biosFailure \| coldStart \| configurationChange \| configurationSave \| fanFailure \| highVoltage \| linkUpLinkDown \| lowDiskSpace \| lowVoltage \| overTemperature \| powerSupplyFailure \| raidVolumeState \| vrrpv2AuthFailure \| vrrpv2NewMaster \| vrrpv3NewMaster \| vrrpv3ProtoError}<br>set snmp traps trap-user <*UserName*> |
| set snmp community <*String*> {read-only \| read-write} |
| set snmp contact <*Contact Information*><br>set snmp location <*Location Information*> |
| set snmp mode {default \| vs} |
| set snmp usm user <*UserName*> security-level authPriv auth-pass-phrase <*Pass Phrase*> privacy-pass-phrase <*Privacy Pass Phrase*> privacy-protocol {DES \| AES \| AES256} authentication-protocol {SHA256 \| SHA512}<br>set snmp usm user <*UserName*> security-level authPriv auth-pass-phrase-hashed <*Hashed Pass Phrase*> privacy-pass-phrase <*Privacy Pass Phrase*> privacy-protocol {DES \| AES \| AES256} authentication-protocol {SHA256 \| SHA512}<br>set snmp usm user <*UserName*> security-level authNoPriv auth-pass-phrase <*Pass Phrase*> authentication-protocol {SHA256 \| SHA512}<br>set snmp usm user <*UserName*> security-level authNoPriv auth-pass-phrase-hashed <*Hashed Pass Phrase*><br>set snmp usm user <*UserName*> {usm-read-only \| usm-read-write}<br>set snmp usm user <*UserName*> vsid {all \| <*IDs of allowed Virtual Devices*> } |
| set snmp vs-direct-access {on \| off} |

### Description of commands

| Command | Description |
|---|---|
| `set snmp agent-version {any \| v3-Only}` | Configures the supported SNMP version:<br>■ `all` - Support SNMP v1, v2 and v3.<br>■ `v3-Only` - Support SNMP v3 only. |
| `set snmp agent {on \| off}` | Enables (`on`) or disables (`off`) the SNMP Agent. |
| `set snmp clear-trap ...` | Configures the indication of a custom SNMP trap termination. |
| `set snmp community <String> {read-only \| read-write}` | Configures the SNMP community password and if this password lets you only read the values of SNMP objects (`read-only`), or set the values as well (`read-write`). |
| `set snmp contact ...` | Configures the contact name for the SNMP community. |
| `set snmp custom-trap ...` | Configures the settings of an existing custom SNMP trap. See the explanations in the "`add snmp custom-trap`" command. |
| `set snmp location ...` | Configures the contact location for the SNMP community. |
| `set snmp mode {default \| vs}` | Configures how to run the SNMP daemon:<br>■ `default`<br>• On non-VSX Gateway, this is the only supported mode.<br>• On VSX Gateway, SNMP daemon runs only in the context of VS0.<br>■ `vs`<br>• For VSX Gateway only.<br>• Each Virtual Device has a separate SNMP daemon running in the context of that Virtual Device. |
| `set snmp traps coldStart-threshold <Seconds>` | Configures the threshold for the SNMP `coldStart` trap. |

| Command | Description |
|---|---|
| `set snmp traps polling-frequency <Seconds>` | Configures the polling interval for the SNMP traps. |
| `set snmp traps receiver ...` | Configures the IPv4 address of the SNMP Trap Sink. |
| `set snmp traps trap-user <UserName>` | Configures the user, which will generate the SNMP traps. |
| `set snmp traps trap ...` | Configures the Gaia built-in SNMP traps. |
| `set snmp usm user <UserName> ...` | Configures the SNMPv3 USM user.<br>**Notes**:<br>■ When you change the configured **Authentication Protocol** of an existing SNMPv3 USM user, Gaia OS requires you to change the **Authentication Pass Phrase** because the previous password is not valid anymore.<br>■ When you change the configured **Privacy Protocol** of an existing SNMPv3 USM user, Gaia OS requires you to change the **Privacy Pass Phrase** because the previous password is not valid anymore. |
| `set snmp vs-direct-access {on \| off}` | Enables (`on`) and disables (`off`) the SNMP direct queries on the IP address of a Virtual System (not only VS0), or Virtual Router.<br>This mode works only when SNMP `vs` mode is enabled.<br>See the *R82 VSX Administration Guide*. |

### Syntax for the '`delete`' commands

**Note** - To see all available commands:

1. Enter:
   `delete snmp`
2. Press <SPACE>
3. Press <ESC><ESC>

### Syntax

| |
|---|
| `delete snmp clear-trap`<br>`delete snmp traps coldStart-threshold`<br>`delete snmp traps polling-frequency`<br>`delete snmp traps receiver <IPv4 address>`<br>`delete snmp traps trap-user <UserName>`<br>`delete snmp custom-trap <Custom Trap Name>` |
| `delete snmp community <String>` |
| `delete snmp contact <Contact Information>`<br>`delete snmp location <Location Information>` |
| `delete snmp interface <Name of Interface>` |
| `delete snmp usm user <UserName>` |

### Description of commands

| Command | Description |
|---|---|
| `delete snmp clear-trap` | Removes the indication of a custom SNMP trap termination. |
| `delete snmp community <String>` | Removes the SNMP community password. |
| `delete snmp contact ...` | Removes the contact name for the SNMP community. |
| `delete snmp custom-trap <Custom Trap Name>` | Removes the custom SNMP trap. |
| `delete snmp interface <Name of Interface>` | Removes the local interface from the list of local interfaces, on which the SNMP daemon listens. |
| `delete snmp location ...` | Removes the contact location for the SNMP community. |
| `delete snmp traps coldStart-threshold` | Removes the threshold for the SNMP `coldStart` trap. |
| `delete snmp traps polling-frequency` | Removes the polling interval for the SNMP traps. |
| `delete snmp traps receiver <IPv4 address>` | Removes the IPv4 address of the SNMP Trap Sink. |

| Command | Description |
|---|---|
| `delete snmp traps trap-user <UserName>` | Removes the user, which will generate the SNMP traps. |
| `delete snmp usm user <UserName>` | Removes the SNMPv3 USM user. |

### Working with SNMP Traps on Scalable Platforms

See the *R82 Scalable Platforms Administration Guide*.

# Interpreting SNMP Error Messages

This section lists and explains certain common error status values that can appear in SNMP messages.

## SNMP PDU

Within the SNMP PDU, the **third** field can include an error-status integer that refers to a specific problem.

The integer zero (0) means that no errors were detected.

When the error field is anything other than 0, the next field includes an error-index value that identifies the variable, or object, in the variable-bindings list that caused the error.

This table lists the error status codes and their meanings:

| Error status code | Meaning | | Error status code | Meaning |
|---|---|---|---|---|
| 0 | `noError` | | 10 | `wrongValue` |
| 1 | `tooBig` | | 11 | `noCreation` |
| 2 | `NoSuchName` | | 12 | `inconsistentValue` |
| 3 | `BadValue` | | 13 | `resourceUnavailable` |
| 4 | `ReadOnly` | | 14 | `commitFailed` |
| 5 | `genError` | | 15 | `undoFailed` |
| 6 | `noAccess` | | 16 | `authorizationError` |
| 7 | `wrongType` | | 17 | `notWritable` |
| 8 | `wrongLength` | | 18 | `inconsistentName` |
| 9 | `wrongEncoding` | | | |

**Note** - You might not see the codes. The SNMP manager or utility interprets the codes and then logs the appropriate message.

Within the SNMP PDU, the **fourth** field, contains the error index when the error-status field is nonzero.

That is, when the error-status field returns a value other than zero, which indicates that an error occurred. The error-index value identifies the variable, or object, in the variable-bindings list that caused the error. The first variable in the list has index 1, the second has index 2, and so on.

Within the SNMP PDU, the **fifth** field, is the variable-bindings field.

This field consists of a sequence of pairs:

- The first element in a pair is the identifier.
- The second element in a pair is one of these options: `value`, `unSpecified`, `noSuchOjbect`, `noSuchInstance`, or `EndofMibView`.

This table describes the elements:

| Variable-bindings element | Description |
|---|---|
| `value` | Value that is associated with each object instance. This value is specified in a PDU request. |
| `unSpecified` | A NULL value is used in retrieval requests. |
| `noSuchObject` | Indicates that the agent does not implement the object, to which it refers by this object identifier. |
| `noSuchInstance` | Indicates that this object does not exist for this operation. |
| `endOfMIBView` | Indicates an attempt to reference an object identifier that is beyond the end of the MIB at the agent. |

## GetRequest

This table lists possible value field sets in the response PDU or error-status messages when performing an SNMP `GetRequest`.

| Value Field Set | Description |
|---|---|
| `noSuchObject` | If a variable does not have an `OBJECT IDENTIFIER` prefix that exactly matches the prefix of any variable accessible by this request, its value field is set to `noSuchObject`. |
| `noSuch Instance` | If the variable's name does not exactly match the name of a variable, its value field is set to `noSuchInstance`. |
| `genErr` | If the processing of a variable fails for any other reason, the responding entity returns `genErr` and a value in the error-index field that is the index of the problem object in the variable-bindings field. |
| `tooBig` | If the size of the message that encapsulates the generated response PDU exceeds a local limitation or the maximum message size of the request's source party, then the response PDU is discarded and a new response PDU is constructed. The new response PDU has an error-status of `tooBig`, an `error-index` of zero, and an empty `variable-bindings` field. |

## GetNextRequest

The only values that can be returned as the second element in the variable-bindings field to a `GetNextRequest` when an error-status code occurs are `unSpecified` or `endOfMibView`.

## GetBulkRequest

The `GetBulkRequest` minimizes the number of protocol exchanges and lets the SNMPv2 manager request that the response is large as possible.

The `GetBulkRequest` PDU has two fields that do not appear in the other PDUs: non-repeaters and max-repetitions. The non-repeaters field specifies the number of variables in the variable-bindings list, for which a single-lexicographic successor is to be returned. The max-repetitions field specifies the number of lexicographic successors to be returned for the remaining variables in the variable-bindings list.

If at any point in the process, a lexicographic successor does not exist, the `endofMibView` value is returned with the name of the last lexicographic successor, or, if there were no successors, the name of the variable in the request.

If the processing of a variable name fails for any reason other than `endofMibView`, no values are returned. Instead, the responding entity returns a response PDU with an error-status of `genErr` and a value in the error-index field that is the index of the problem object in the variable-bindings field.

# Job Scheduler

You can schedule regular jobs.

You can configure the jobs to run at the dates and times that you specify, or at startup.

# Configuring Job Scheduler in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Scheduling new jobs

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **Job Scheduler**. |
| 2 | Click **Add**.<br>The **Add A New Scheduled Job** window opens. |
| 3 | In the **Job Name**, enter the name of the job.<br>Use alphanumeric characters only, and no spaces. |
| 4 | In the **Command to Run**, enter the name of the command.<br>**Important:**<br>■ The command must be a Linux command.<br>■ If you wish to run a Check Point command or use a Check Point environment variable, then use this syntax (see *"Running Check Point Commands in Shell Scripts" on page 758*):<br>• On a Security Management Server / Log Server / SmartEvent Server:<br>`source /etc/profile.d/CP.sh ; <Applicable Check Point Command>`<br>• On a Multi-Domain Server / Multi-Domain Log Server:<br>`source /etc/profile.d/CP.sh ; source $MDSDIR/scripts/MDSprofile.sh ; source $MDS_SYSTEM/shared/mds_environment_utils.sh ; source $MDS_SYSTEM/shared/sh_utilities.sh ; <Applicable Check Point Command>`<br>• On a Security Gateway / Cluster Members (non-VSX):<br>`source /etc/profile.d/CP.sh ; <Applicable Check Point Command>`<br>• On a VSX Gateway / VSX Cluster Members:<br>`source /etc/profile.d/CP.sh ; source /etc/profile.d/vsenv.sh ; <Applicable Check Point Command>` |
| 5 | Below the **Schedule**, select the frequency (**Minute Interval**, **Hourly**, **Daily**, **Weekly**, **Monthly**, **During Boot**) for this job.<br>Where applicable, enter the **Time** of day for the job, in the 24-hour clock format (HH:MM). |
| 6 | Click **OK**.<br>The job shows in the **Scheduled Jobs** table. |

| Step | Instructions |
|---|---|
| 7 | In the **E-mail Notification**, enter the e-mail address, to which Gaia should send the notifications.<br>**Note** - You must also configure a Mail Server (see *"Mail Notification" on page 380*). |
| 8 | Click **Apply**. |

### Editing the scheduled jobs

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **Job Scheduler**. |
| 2 | In the scheduled Jobs table, select the job that you want to edit. |
| 3 | Click **Edit**.<br>The **Edit Scheduled Job** opens. |
| 4 | Enter the changes. |
| 5 | Click **OK**. |

### Deleting the scheduled jobs

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **Job Scheduler**. |
| 2 | In the **Scheduled Jobs** table, select the job to delete. |
| 3 | Click **Delete**. |
| 4 | Click **OK** to confirm.<br>(Click **Cancel** to abort.) |

# Configuring Job Scheduler in Gaia Clish

## Description

Use these commands to configure Gaia to schedule jobs. The jobs run on the dates and times you specify.

You can define an email address, to which Gaia sends the output of the scheduled job.

**Important:**

- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Syntax

### Adding new scheduled jobs

```
add cron job <Job Name> command "<Command>" recurrence
      daily time <HH:MM>
      hourly hours {all | <0-23> | <HH1>,<HH2>,...,<HHn>} at <1-
59>
      interval <1-59>
      monthly month <1-12> days <1-31> time <HH:MM>
      weekly days <0-6> time <HH:MM>
      system-startup
```

### Editing the existing scheduled jobs

```
set cron job <Job Name>
      command "<Command>"
      recurrence
            daily time <HH:MM>
            hourly hours {all | <0-23> | <HH1>,<HH2>,...,<HHn>}
at <1-59>
            interval <1-59>
            monthly month <1-12> days <1-31> time <HH:MM>
            weekly days <0-6> time <HH:MM>
            system-startup
```

```
set cron mailto <Email Address>
```

### Viewing the existing scheduled jobs

```
show cron
      job <Job Name>
            command
            recurrence
      jobs
      mailto
```

### Deleting the existing scheduled jobs

```
delete cron
      all
      job <Job Name>
      mailto
```

**Note** - Only the `show` commands provide an output.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| *<Job Name>* | The name of the job to schedule. |

| Parameter | Description |
|---|---|
| "<*Command*>" | The command to run.<br>**Important:**<br>■ The command must be a Linux command.<br>■ You must enclose the syntax in quotes:<br>• If the command contains variables (`$NameOfVariable`), then use double quotes.<br>• If the command does not contain variables, you can use single quotes.<br>■ If you wish to run a Check Point command or use a Check Point environment variable, then use this syntax (see *"Running Check Point Commands in Shell Scripts" on page 758*):<br>• On a Security Management Server / Log Server / SmartEvent Server:<br>`source /etc/profile.d/CP.sh ; <Applicable Check Point Command>`<br>• On a Multi-Domain Server / Multi-Domain Log Server:<br>`source /etc/profile.d/CP.sh ; source $MDSDIR/scripts/MDSprofile.sh ; source $MDS_SYSTEM/shared/mds_environment_utils.sh ; source $MDS_SYSTEM/shared/sh_utilities.sh ; <Applicable Check Point Command>`<br>• On a Security Gateway / Cluster Members (non-VSX):<br>`source /etc/profile.d/CP.sh ; <Applicable Check Point Command>`<br>• On a VSX Gateway / VSX Cluster Members:<br>`source /etc/profile.d/CP.sh ; source /etc/profile.d/vsenv.sh ; <Applicable Check Point Command>` |

| Parameter | Description |
|---|---|
| `recurrence daily time <HH:MM>` | Specifies that the job should run once a day - every day, at specified time.<br>Enter the time of day in the 24-hour clock format - `<Hours>:<Minutes>`.<br>Example: `14:35` |
| `recurrence hourly hours {all \| <0-23> \| <HH1>,<HH2>,...,<HHn>} at <1-59>` | Specifies that the job should run every day at a specified hour and minute:<br>■ `all at <1-59>`<br>Run each hour at the specified minute<br>Example (run every day at <HH>:15): `all at 15`<br>■ `<0-23> at <1-59>`<br>Run at a specific hour and at the specified minute<br>Example (run every day at 14:15): `14 at 15`<br>■ `<HH1>,<HH2>,...,<HHn> at <1-59>`<br>Run at specific hours and at the specified minute<br>Example (run every day at 10:15, 12:15, and 14:15): `10,12,14 at 15` |
| `recurrence interval <1-59>` | Specifies that the job should run every number of minutes.<br>Example (run every 15 minutes): `15` |
| `recurrence monthly month <1-12> days <1-31> time <HH:MM>` | Specifies that the job should run once a month - on specified months, on specified dates, and at specified time.<br>Months are specified by numbers from 1 to 12:<br>■ January = 1<br>■ February = 2<br>■ ...<br>■ December = 12<br>Dates of month are specified by numbers from 1 to 31.<br>To specify several consequent months, enter their numbers separate by commas.<br>Example: For January, February, and March, enter `1,2,3`<br>To specify several consequent dates, enter their numbers separate by commas.<br>Example: For 1st, 2nd and 3rd day of the month, enter `1,2,3` |

| Parameter | Description |
|---|---|
| `recurrence weekly days <0-6> time <HH:MM>` | Specifies that the job should run once a week - on specified days of week, and at specified time.<br>Days of week are specified by numbers from 0 to 6:<br>■ Sunday = 0<br>■ Monday = 1<br>■ Tuesday = 2<br>■ Wednesday = 3<br>■ Thursday = 4<br>■ Friday = 5<br>■ Saturday = 6<br>To specify several consequent days of a week, enter their numbers separate by commas.<br>Example: For Sunday, Monday, and Tuesday, enter `0,1,2` |
| `recurrence system-startup` | Specifies that the job should at every system startup. |
| `mailto <Email Address>` | Specifies the email address, to which Gaia sends the jobs' results.<br>Enter one email address for each command. You must also configure a mail server (see *"Mail Notification" on page 380*). |

# Mail Notification

*In This Section:*



## Introduction

Mail notifications (also known as Mail Relay) allow you to send email from the Security Gateway.

You can send email interactively or from a script. The email is relayed to a mail hub that sends the email to the final recipient.

Mail notifications are used as an alerting mechanism when a Firewall rule is triggered. It is also used to email the results of cron jobs to the system administrator.

Gaia supports these mail notification features:

- Presence of a mail client or Mail User Agent (MUA) that can be used interactively or from a script.
- Presence of a Sendmail-like replacement that relays mail to a mail hub by using SMTP.
- Ability to specify the default recipient on the mail hub.

Gaia does not support these mail notification features:

- Incoming e-mail.
- Mail transfer protocols other than outbound SMTP.
- Telnet to port 25.
- E-mail accounts other than *admin* or *monitor*.

# Configuring Mail Notification in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **Mail Notification**. |
| 2 | In the **Mail Server** field, enter the IPv4 Address or Hostname of the mail server.<br>For example: `mail.example.com` |
| 3 | In the **User Name** field, enter the user name.<br>For example: `user@mail.example.com` |
| 4 | Click **Apply**. |

# Configuring Mail Notification in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

### Description

Use this group of commands to configure mail notifications.

### Syntax

- To configure the mail server that receives the mail notifications:

```
set mail-notification server <IPv4 Address or Hostname>
```

- To configure the user on the mail server that receives the mail notifications:

```
set mail-notification username <User Name>
```

- To show the configured mail server and user:

```
show mail-notification
      server
      username
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Parameters

| Parameter | Description |
|---|---|
| `server <IPv4 Address or Hostname>` | The IPv4 address or Hostname of the mail server, to which Gaia sends mail notifications.<br>Example: `mail.company.com` |
| `username <User Name>` | The username on the mail server that receives the `admin` or `monitor` mail notifications.<br>Example: `johndoe` |

### Example

```
gaia> set mail-notification server mail.company.com
gaia> set mail-notification username johndoe
gaia> show mail-notification server
Mail notification server: mail.company.com
gaia> show mail-notification username
Mail notification user: johndoe
```

# Messages

*In This Section:*



You can configure Gaia to show a *Banner Message* and a *Message of the Day* to users when they log in.

## Comparison

| Item | Banner Message | Message of the Day |
|---|---|---|
| Default Message | `This system is for authorized use only` | `You have logged into the system` |
| When shown in Gaia Portal | Browser login page, before logging in | After logging in to the system |
| When shown in Gaia Clish | When logging in, before entering the password | After logging in to the system |
| Default state | Enabled | Disabled |

## Configuring Messages in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **Messages**. |
| 2 | To enter a Banner message, select **Banner message**. |
| 3 | To enter a Message of the Day, select **Message of the day**. |
| 4 | Enter the message text.<br>See the **Limits** section below. |
| 5 | Click **Apply**. |

# Configuring Messages in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

### Syntax for Banner message

- To show if the banner message is enabled or disabled:

```
show message banner status
show message all status
```

- To show the configured banner message:

```
show message banner
show message all
```

- To define a new single-line banner message:

```
set message banner on msgvalue "<Banner Text>"
```

  See the **Limits** section below.

  Example:

```
gaia> set message banner on msgvalue "This system is private
and confidential"
```

- To define a new multi-line banner message:

```
set message banner on line msgvalue "<Banner Text for Line
#1>"
set message banner on line msgvalue "<Banner Text for Line
#2>"
```

- To enable or disable the configured banner message:

```
set message banner on
set message banner off
```

- To delete the configured banner message perform these two steps:

1. Delete the user-defined banner message:

   ```
   delete message banner
   ```

   **Note** - This deletes the configured banner message, and replaces it with the default banner message "`This system is for authorized use only.`"

2. Disable the default banner:

   ```
   set message banner off
   ```

### Syntax for Message of the Day

- To show the configured message of the day:

```
show message motd
show message all
```

- To show if the message of the day is enabled or disabled:

```
show message motd status
show message all status
```

- To define a new single-line message of the day:

```
set message motd on msgvalue "<Message Text>"
```

  See the **Limits** section below.

  Example:

```
gaia> set message motd on msgvalue "Hi all - no changes
allowed today"
```

- To define a new multi-line message of the day:

```
set message motd on line msgvalue "<Message Text for Line
#1>"
set message motd on line msgvalue "<Message Text for Line
#2>"
```

  See the **Limits** section below.

- To enable or disable the configured message of the day:

```
set message motd on
set message motd off
```

- To delete the configured message of the day, perform these two steps:

1. Delete the user-defined message of the day:

   ```
   delete message motd
   ```

   **Note** - This deletes the configured message of the day, and replaces it with the default message of the day "`You have logged into the system.`"

2. Disable the default message of the day:

   ```
   set message motd off
   ```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Limits

| Message type | Maximum supported total number of characters in the message | Maximum supported total number of lines in the message | Maximum supported number of characters in each line |
|---|---|---|---|
| Banner | 1600 | 20 | 80 |
| Message of the day | 1200 | 20 | 400 |

# Display Format

*In This Section:*

On this page, you configure:

- The display format for the Time, Date, and IPv4 netmask on Gaia.
- The keyboard layout for the console connection.

**Configuring Display Format in Gaia Portal**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **Display Format**. |
| 2 | In **Time**, select one of these options:<br>■ **12-hour**<br>■ **24-hour** |
| 3 | In **Date**, select one of these options:<br>■ **dd/mm/yyyy**<br>■ **mm/dd/yyyy**<br>■ **yyyy/mm/dd**<br>■ **dd-mmm-yyyy** |
| 4 | In **IPv4 netmask**, select one of these options:<br>■ **Dotted-decimal notation**<br>■ **CIDR notation** |
| 5 | Click **Apply**. |

## Configuring Display Format in Gaia Clish

### Syntax for the Time

- To show the current time format:

```
show format time
show format all
```

- To configure the time format:

```
set format time
      12-hour
      24-hour
```

### Syntax for the Date

- To show the current date format:

```
show format date
show format all
```

- To configure the date format:

```
set format date
      dd/mm/yyyy
      mm/dd/yyyy
      yyyy/mm/dd
      dd-mmm-yyyy
```

### Syntax for the IPv4 netmask

- To show the current IPv4 netmask format:

```
show format netmask
show format all
```

- To configure the IPv4 netmask format:

```
set format netmask
      dotted
      length
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Configuring Keyboard Layout in Gaia Portal

1. In the left tree, click **System Management** > **Display Format**.
2. In the section **Keyboard Layout**, select the applicable keyboard layout.
3. Click **Apply**.

### Configuring Keyboard Layout in Gaia Clish

To show the current keyboard layout:

```
show keyboard layout
```

To configure a keyboard layout:

```
set keyboard layout <Layout>
```

**Note** - Press the Tab key to see the available layouts.

**Important** - After you add, configure, or delete features, run the `save config` command to save the settings permanently.

# Session

You can manage inactivity timeout for Gaia Portal and Gaia Clish.

## Configuring the Session in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **Session**. |
| 2 | In the **Command Line Shell** section, configure the inactivity timeout for the Gaia Clish. |
| 3 | In the **Web UI** section, configure the inactivity timeout for the Gaia Portal.<br>■ **Range:** 1 - 720 minutes<br>■ **Default:** 10 minutes |

## Configuring the Session in Gaia Clish

**Important:**

- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Syntax

- To configure the timeout:

```
set inactivity-timeout <Timeout>
```

- To show the configured timeout:

```
show inactivity-timeout
```

### Parameters

| Parameter | Description |
|---|---|
| *<Timeout>* | The inactivity timeout (in minutes) for the Gaia Clish.<br>■ **Range:** 1 - 720 minutes<br>■ **Default:** 10 minutes |

# Crash Data

*In This Section:*



## Introduction

A process core dump file contains the recorded status of the working memory of the Gaia computer at the time that a Gaia process terminated abnormally.

When a process terminates abnormally, it produces a core dump file in the `/var/log/dump/usermode/` directory.

If the `/log` partition has less than 200 MB, Gaia OS does not create new core dump files and deletes the existing core dump files to get more free space. This prevents the core dump files from filling the `/log` partition.

**Warning** - The core dump files may contain personal data.
For more information, see sk175504.

## Configuring Core Dumps in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

To configure core dumps, enable the feature and then configure parameters.

**Procedure**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **Crash Data**. |
| 2 | Select **Enable Core Dumps** and configure the parameters. |
| 3 | In the **Total space limit** field, configure the maximum disk space to keep all core dump files.<br>Gaia OS deletes the oldest core dump file if it requires disk space for a new core dump file.<br>Gaia OS enforces the process limit before the space limit.<br>■ **Range**: 1 - 99999 MB<br>■ **Default**:<br>◦ Management Server- 5000 MB<br>◦ Security Gateway in the Kernel Space Firewall (KSFW) mode - 5000 MB<br>◦ Security Gateway in the User Space Firewall (USFW) mode - 15000 MB<br>Based on the enabled features, Gaia OS may change the default value automatically. To see the current value, run this command in Gaia Clish:<br>`show core-dump total` |
| 4 | In the **Dumps per process** field, configure the maximum number of core dump files to keep for each process executable file.<br>A new core dump file overwrites the oldest core dump file.<br>Gaia OS enforces the process limit before the space limit.<br>■ **Range**: 1 - 99999<br>■ **Default**: 2<br>**Example**<br>There are two user space processes "A" and "B", and the limit is 2 core dump files for each process.<br>Process "A" terminates 1 time, and process "B" terminates 3 times.<br>Gaia OS keeps these core dumps:<br>■ 1 core dump for process "A"<br>■ 2 core dumps for process "B"<br>Gaia OS deletes the core dump #3 for process "B" because of the process limit. |
| 5 | Click **Apply**. |

# Configuring Core Dumps in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

### Syntax

- To enable or disable core dump files:

```
set core-dump {enable | disable}
```

- To configure the total disk space limit for all core dump files (in MB):

```
set core-dump total <0-99999>
```

- To configure the number of core dump files for each process:

```
set core-dump per_process <0-99999>
```

- To show the status of this feature:

```
show core-dump status
```

- To show the configured total disk space limit:

```
show core-dump total
```

- To show the configured limit of core dump files for each process:

```
show core-dump per_process
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

**Parameters**

| Parameter | Description |
|---|---|
| `total <0-99999>` | The maximum disk space to keep all core dump files.<br>Gaia OS deletes the oldest core dump file if it requires disk space for a new core dump file.<br>Gaia OS enforces the process limit before the space limit.<br>■ **Range:** 1 - 99999 MB<br>■ **Default:**<br>◦ Management Server - 5000 MB<br>◦ Security Gateway in the Kernel Space Firewall (KSFW) mode - 5000 MB<br>◦ Security Gateway in the User Space Firewall (USFW) mode - 15000 MB<br>Based on the enabled features, Gaia OS may change the default value automatically. To see the current value, run this command in Gaia Clish: `show core-dump total` |
| `per_process <0-99999>` | The maximum number of core dump files to keep for each process executable file.<br>A new core dump file overwrites the oldest core dump file.<br>Gaia OS enforces the process limit before the space limit.<br>■ **Range:** 1 - 99999<br>■ **Default:** 2<br>**Example**<br>There are two user space processes "A" and "B", and the limit is 2 core dump files for each process.<br>Process "A" terminates 1 time, and process "B" terminates 3 times.<br>Gaia OS keeps these core dumps:<br>■ 1 core dump for process "A"<br>■ 2 core dumps for process "B"<br>Gaia OS deletes the core dump #3 for process "B" because of the process limit. |

# System Configuration

*In This Section:*



**Important:**

- R82 does **not** support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313).
- On a Multi-Domain Security Management Server, follow these instructions to configure an IPv6 address - *"Configuring an IPv6 Address on a Multi-Domain Server" on page 710*.To configure an IPv6 address on a Multi-Domain Security Management Server, see the *R82 Gaia Administration Guide*.

**Before you can configure IPv6 addresses and IPv6 static routes, you must:**

| Step | Instructions |
|---|---|
| 1 | Enable the IPv6 support. |
| 2 | Reboot. |
| 3 | To configure IPv6 addresses, see *"Network Interfaces" on page 102*.<br>To configure IPv6 static routes, see *"IPv6 Static Routes" on page 279*. |

**To enforce a Security Policy for IPv6 traffic:**

| Step | Instructions |
|---|---|
| 1 | Enable the IPv6 support in Gaia OS on both the Security Management Server and the Security Gateway (each Cluster Member). |
| 2 | Connect with SmartConsole to the Management Server. |
| 3 | Create the applicable IPv6 objects. |
| 4 | Create the applicable IPv6 rules in the Access Control Policy. |
| 5 | Install the Access Control Policy on the Security Gateway (the Cluster) object. |

# Configuring IPv6 Support in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`). |
| 2 | From the navigation tree, click **System Management** > **System Configuration**. |
| 3 | In the **IPv6 Support** section, select **On**. |
| 4 | Click **Apply**. |
| 5 | When prompted, select **Yes** to reboot.<br>**Important** - IPv6 support is **not** available until you reboot. |

# Configuring IPv6 Support in Gaia Clish

**Important:**

- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

- To configure IPv6 support:

  ```
  set ipv6-state {on | off}
  ```

  **Important** - This change requires reboot.

- To show the state of IPv6 support:

  ```
  show ipv6-state
  ```

**Procedure**

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on Gaia. |
| 2 | Log in to Gaia Clish. |
| 3 | On Scalable Platforms, go to Gaia gClish:<br>Type `gclish` and press Enter. |
| 4 | Enable the IPv6 support:<br>`set ipv6-state on` |
| 5 | Save the changes:<br>`save config` |
| 6 | Reboot:<br>`reboot`<br>**Important** - IPv6 support is **not** available until you reboot. |

# Configuring IPv6 Support with Gaia API

See *"Working with Gaia RESTful API" on page 749*

| Step | Instructions |
|---|---|
| 1 | Enable the IPv6 support.<br>a. In the Gaia API Reference:<br>a. Open the chapter "**Networking**".<br>b. Open the section "**IPv6**".<br>b. Run this API command:<br>`set-ipv6` |
| 2 | Reboot.<br>a. In the Gaia API Reference:<br>Open the chapter "**System**".<br>b. Run this API command:<br>`run-reboot` |
| 3 | Configure IPv6 addresses on the applicable interfaces.<br>a. In the Gaia API Reference:<br>a. Open the chapter "**Interfaces**".<br>b. Open the applicable section.<br>For example, "**Physical Interfaces**".<br>b. Run the applicable API "`set`" command to configure the IPv6 address on the applicable interface.<br>For example:<br>`set-physical-interface` |
| 4 | Configure the applicable IPv6 static routes.<br>See *"IPv6 Static Routes" on page 279*.<br>In this release, Gaia API supports only IPv4 static routes. |

# System Logging

You can configure the settings for the system logs, including sending them to a remote server.

Make sure to configure the remote server to receive the system logs.

# Configuring System Logging in Gaia Portal

This section includes procedures for configuring System Logging and Remote System Logging.

System Logging configures if Gaia sends these logs:

- Gaia syslog messages to its Check Point Management Server
- Gaia audit logs upon successful configuration to its Check Point Management Server
- Gaia audit logs upon successful configuration to Gaia syslog facility

Remote System Logging configures a remote syslog server, to which Gaia sends its syslog messages.

**Note** - There are settings that you can configure only in Gaia Clish.

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

**Configuring the System Logging**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **System Logging**. |
| 2 | In the **System Logging** section, select the applicable options: |
| | ■ **Send Syslog messages to management server**<br>Specifies if the Gaia sends the Gaia system logs to a Check Point Management Server.<br>**Default:** Not selected<br>**Note** - You can configure this option in Gaia Clish with the "`set syslog cplogs {on \| off}`" command. |
| | ■ **Send audit logs to management server upon successful configuration**<br>Specifies if the Gaia sends the Gaia audit logs (for configuration changes that authorized users make) to a Check Point Management Server.<br>**Default:** Selected<br>**Note** - You can configure this option in the Gaia Clish with the "`set syslog mgmtauditlogs {on \| off}`" command. |

| Step | Instructions |
|---|---|
| | ■ **Send audit logs to syslog upon successful configuration**<br>Specifies if the Gaia saves the logs for configuration changes that authorized users make.<br>Otherwise, Gaia uses the default `/var/log/messages` file.<br>**Default:** Selected<br>To specify a Gaia configuration audit log file, run this command:<br>`set syslog filename /<Path>/<File>`<br>**Note** - This option is configured in the Gaia Clish with the "`set syslog auditlog {disable \| permanent}`" command. |
| 3 | Click **Apply**. |

### Configuring the Remote System Logging

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **System Logging**. |
| 2 | In the **Remote System Logging** section, click **Add**. |
| 3 | In the **IP Address** field, enter the IPv4 address of the remote syslog server. |
| 4 | In the **Priority** field, select the severity level of the logs that are sent to the remote server.<br>These are the accepted values (as defined by the RFC 5424 - Section-6.2.1):<br>■ **All** - All messages<br>■ **Debug** - Debug-level messages<br>■ **Info** - Informational messages<br>■ **Notice** - Normal but significant condition<br>■ **Warning** - Warning conditions<br>■ **Error** - Error conditions<br>■ **Critical** - Critical conditions<br>■ **Alert** - Action must be taken immediately<br>■ **Emergency** - System is unusable |
| 5 | Click **OK**. |

**Important** - Do **not** to configure two Gaia computers to send system logs to each other - directly, or indirectly. Such configuration creates a syslog forwarding loop, which causes all syslog message to repeat indefinitely on both Gaia computer.

### Editing the Remote System Logging settings

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **System Logging**. |
| 2 | In the **Remote System Logging** section, select the remote server. |
| 3 | Click **Edit**. |
| 4 | In the **IP Address** field, enter the IPv4 address of the remote syslog server. |
| 5 | In the **Priority** field, select the severity level of the logs that are sent to the remote server. |
| 6 | Click **OK**. |

### Deleting the Remote System Logging settings

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **System Logging**. |
| 2 | In the **Remote System Logging** section, select the remote syslog server. |
| 3 | Click **Delete**. |
| 4 | In the confirmation window, click **Yes**. |

### Syslog configuration files

By default, Gaia Operating System saves the Syslog configuration in these files:

- `/etc/rsyslog.conf`
- `/etc/sysconfig/rsyslog`

If it is necessary to add specific settings manually in these files (that Gaia OS does not have), then it is necessary to make these files immutable, so Gaia OS does not overwrite them:

1. Connect to the command line on Gaia OS.
2. Log in to the Expert mode.
3. Edit the applicable Syslog configuration file as required in your environment.
4. Examine the current attributes on the applicable configuration file you edited:

- `lsattr /etc/rsyslog.conf`
- `lsattr /etc/sysconfig/rsyslog`

5. Add the immutable attribute on the applicable configuration file you edited:
   - `chattr +i /etc/rsyslog.conf`
   - `chattr +i /etc/sysconfig/rsyslog`
6. Examine the current attributes on the applicable configuration file you edited:
   - `lsattr /etc/rsyslog.conf`
   - `lsattr /etc/sysconfig/rsyslog`
7. Restart the Syslog service:

```
service rsyslog restart
```

**Warning** - While the Syslog configuration files are immutable:

- Gaia OS cannot save the changes in the Syslog configuration you make in Gaia Portal or Gaia Clish.
- Gaia OS cannot restore a Gaia Backup.

To remove the immutable attribute from a file, use this command:

```
chattr -i <file>
```

# Configuring System Logging in Gaia Clish

### Description

You can configure the System Logging and Remote System Logging.

System Logging configures the Gaia to sends these logs:

- Gaia syslog messages to its Check Point Management Server
- Gaia audit logs upon successful configuration to its Check Point Management Server
- Gaia audit logs upon successful configuration to Gaia syslog facility

Remote System Logging configures a remote server, to which Gaia sends its syslog messages.

**Note** - There are some command options and parameters, which you cannot configure in the Gaia Portal.

**Important:**

- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Syntax for System Logging configuration

- To send the Gaia system logs to a Check Point Management Server:

```
set syslog cplogs {on | off}
```

- To send the Gaia configuration audit logs to a Check Point Management Server:

```
set syslog mgmtauditlogs {on | off}
```

- To save the Gaia configuration audit logs:

```
set syslog auditlog {disable | permanent}
```

- To configure the file name of the Gaia configuration audit log:

```
set syslog filename /<Path>/<File>
```

- To show the Gaia system logging configuration:

```
show syslog
      all
      auditlog
      cplogs
      filename
      mgmtauditlogs
```

### Syntax for Remote System Logging configuration

- To send Gaia system logs to a remote syslog server:

```
add syslog log-remote-address <IPv4 Address> level
<Severity>
```

- To show the Gaia system logging configuration:

```
show syslog
      all
      log-remote-address <IPv4 Address>
      log-remote-addresses
```

- To stop sending Gaia system logs to the specific remote server:

```
delete syslog log-remote-address <IPv4 Address> [level
<Severity>]
```

### CLI Parameters

| Parameter | Description |
|---|---|
| `cplogs {on \| off}` | Specifies if the Gaia sends the Gaia system logs to a Check Point Management Server:<br>■ `on` - Send Gaia system syslogs<br>■ `off` - Do not send Gaia syslogs<br>**Default:** `off`<br>**Note** - This command corresponds to the **Send Syslog messages to management server** option in the Gaia Portal > **System Management** > **System Logging**. |
| `mgmtauditlogs {on \| off}` | Specifies if the Gaia sends the Gaia audit logs (for configuration changes that authorized users make) to a Check Point Management Server:<br>■ `on` - Send Gaia audit logs<br>■ `off` - Do not send Gaia audit logs<br>**Default:** `on`<br>**Note** - This command corresponds to the **Send audit logs to management server upon successful configuration** option in the Gaia Portal > **System Management** > **System Logging**. |
| `auditlog {disable \| permanent}` | Specifies if the Gaia saves the logs for configuration changes that authorized users make:<br>■ `disable` - Disables the Gaia audit log facility<br>■ `permanent` - Enables the Gaia audit log facility to save information about all successful changes in the Gaia configuration. To specify a destination file, run the `set syslog filename </Path/File>` command (otherwise, Gaia uses the default `/var/log/messages` file).<br>**Default:** `permanent`<br>**Note** - This command corresponds to the **Send audit logs to syslog upon successful configuration** option in the Gaia Portal > **System Management** > **System Logging**. |
| */<Path>/<File>* | Configures the full path and file name of the system log.<br>**Default:** `/var/log/messages`<br>**Note** in Gaia Portal does not let you configure this setting. |

| Parameter | Description |
|---|---|
| `log-remote-address` | Configures Gaia to send system logs to a remote syslog server.<br>**Important** - Do **not** configure two Gaia computers to send system logs to each other - directly, or indirectly. Such configuration creates a syslog forwarding loop, which causes all syslog messages to repeat indefinitely on both Gaia computers.<br>**Note** - This command corresponds to the Gaia Portal > **System Management** > **Remote System Logging**. |
| *<IPv4 Address>* | IPv4 address of the remote syslog server, to which Gaia sends its system logs.<br>■ **Range:** Dotted-quad ([0-255].[0-255].[0-255].[0-255])<br>■ **Default:** No default value |
| *<Severity>* | Syslog severity level for the system logging.<br>These are the accepted values (as defined by the RFC 5424 - Section-6.2.1):<br>■ `emerg` - System is unusable<br>■ `alert` - Action must be taken immediately<br>■ `crit` - Critical conditions<br>■ `err` - Error conditions<br>■ `warning` - Warning conditions<br>■ `notice` - Normal but significant condition<br>■ `info` - Informational messages<br>■ `debug` - Debug-level messages<br>■ `all` - All messages<br>**Notes:**<br>■ Until you configure at least one severity level for a given remote server, Gaia does not send syslog messages.<br>■ If you specify multiple severities, the most general least severe severity always takes precedence. |

### Example

```
gaia> set syslog auditlog permanent

gaia> set syslog filename /var/log/system_logs.txt

gaia> set syslog mgmtauditlogs on

gaia> set syslog cplogs on

gaia> set syslog log-remote-address 192.168.2.1 level all

gaia> show syslog all
Syslog Parameters:
    Remote Address 192.168.2.1
        Levels all
    Auditlog permanent
    Destination Log Filename /var/log/system_logs.txt
gaia>

gaia>show syslog auditlog
permanent
gaia>

gaia> show syslog cplogs
Sending syslog syslogs to Check Point's logs is enabled
gaia>

gaia> show syslog mgmtauditlogs
Sending audit logs to Management Serever is enabled
gaia>

gaia> show syslog filename
/var/log/system_logs.txt
gaia>
```

### Syslog configuration files

By default, Gaia Operating System saves the Syslog configuration in these files:

- `/etc/rsyslog.conf`
- `/etc/sysconfig/rsyslog`

If it is necessary to add specific settings manually in these files (that Gaia OS does not have), then it is necessary to make these files immutable, so Gaia OS does not overwrite them:

1. Connect to the command line on Gaia OS.
2. Log in to the Expert mode.
3. Edit the applicable Syslog configuration file as required in your environment.
4. Examine the current attributes on the applicable configuration file you edited:
    - `lsattr /etc/rsyslog.conf`
    - `lsattr /etc/sysconfig/rsyslog`
5. Add the immutable attribute on the applicable configuration file you edited:

- `chattr +i /etc/rsyslog.conf`
- `chattr +i /etc/sysconfig/rsyslog`

6. Examine the current attributes on the applicable configuration file you edited:
   - `lsattr /etc/rsyslog.conf`
   - `lsattr /etc/sysconfig/rsyslog`
7. Restart the Syslog service:

```
service rsyslog restart
```

**Warning** - While the Syslog configuration files are immutable:

- Gaia OS cannot save the changes in the Syslog configuration you make in Gaia Portal or Gaia Clish.
- Gaia OS cannot restore a Gaia Backup.

To remove the immutable attribute from a file, use this command:

```
chattr -i <file>
```

# Redirecting RouteD System Logging Messages

It is possible to configure the RouteD daemon to write its log messages (for example, OSPF or BGP errors) to one of these log files:

| Log File | Description |
|---|---|
| `/var/log/routed_messages` | Dedicated file that contains only the RouteD log messages.<br>In Gaia versions R80 and higher, the RouteD writes to this file by default. |
| `/var/log/messages` | This file contains log messages from different daemons and from the operating system.<br>In Gaia versions R77.30 and lower, the RouteD writes to this file by default.<br>**Best Practice** - Configure the RouteD to write its log messages to the `/var/log/routed_messages` file. |

**Important:**

- In a Cluster, you must configure all the Cluster Members in the same way.
- When you change this configuration, it is **not** necessary to restart the RouteD daemon, or reboot.

### Configuration in the Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | From the left navigation tree, click **Advanced Routing** > **Routing Options**. |
| 2 | In the **Routing Process Message Logging Options** section, select **Log Routed Separately**. |
| 3 | In the **Maximum File Size** field, enter the size (in megabytes) for each log file.<br>The default size is 1 MB.<br>When the active log file `/var/log/routed_messages` reaches the maximum configured size, the Gaia OS rotates it and creates the new `/var/log/routed_messages` file. |
| 4 | In the **Maximum Number of Files** field, enter the maximum number of log files to keep.<br>The default is to keep 10 log files:<br>■ `/var/log/routed_messages`<br>■ `/var/log/routed_messages.0`<br>■ `/var/log/routed_messages.1`<br>■ ...<br>■ `/var/log/routed_messages.9`<br>If the number of all log files reaches the maximum configured number, the Gaia OS deletes the oldest file, and rotates the existing files.<br>The file names end with a number suffix. The greater the suffix number, the older the file. |
| 5 | Click **Apply**. |

### Configuration in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on Gaia. |
| 2 | Log in to Gaia Clish. |
| 3 | On Scalable Platforms, go to Gaia gClish:<br>Type `gclish` and press Enter. |
| 4 | Enable the logging of RouteD messages to a dedicated log file:<br>`set routedsyslog on` |
| 5 | Configure the size (in megabytes) for each log file:<br>`set routedsyslog size <Number of MB between 1 and 2047>`<br>The default size is 1 MB.<br>When the active log file `/var/log/routed_messages` reaches the maximum configured size, the Gaia OS rotates it and creates the new `/var/log/routed_messages` file. |
| 6 | Configure the maximum number of log files to keep:<br>`set routedsyslog maxnum <Number of Files between 1 and 4294967295>`<br>The default is to keep 10 log files:<br>■ `/var/log/routed_messages`<br>■ `/var/log/routed_messages.0`<br>■ `/var/log/routed_messages.1`<br>■ ...<br>■ `/var/log/routed_messages.9`<br>When the number of log files reaches the maximum configured number, the Gaia OS deletes the oldest log file and rotates the existing log files.<br>The file names end with a number suffix. The greater the suffix number, the older the log file. |
| 7 | Save the configuration:<br>`save config` |

### How to examine the configuration in CLI

Examine the configuration in Gaia Clish, or the Expert mode.

| Shell | Command | Expected output |
|---|---|---|
| Gaia Clish | `show configuration routedsyslog` | ■ If default values were used for "`maxnum`" and "`size`":<br>`set routedsyslog on`<br>■ If custom values were configured for "`maxnum`" and "`size`":<br>`set routedsyslog on`<br>`set routedsyslog maxnum <Configured_Value>`<br>`set routedsyslog size <Configured_Value>` |
| Expert mode | `grep routedsyslog /config/active` | ■ If default values were used for "`maxnum`" and "`size`":<br>`routed:instance:default:routedsyslog t`<br>■ If custom values were configured for "`maxnum`" and "`size`":<br>`routed:instance:default:routedsyslog t`<br>`routed:instance:default:routedsyslog:size <Configured_Value>`<br>`routed:instance:default:routedsyslog:files <Configured_Value>` |

**Important:**

- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in the Expert mode on the applicable Security Group.

# Configuring Log Volume

If there is enough available disk space, you can increase the size of the log partition.

**Note** - Disk space is added to the log volume by subtracting it from the disk space used to store Gaia backup images.

**Important:**
Before you change the size of the log partition, take the Gaia snapshot and export it to an external storage. See *"Snapshot Management" on page 614*.
On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in the Expert mode on the applicable Security Group.

Use the **lvm_manager** tool in the Expert mode.

| Step | Instructions |
|---|---|
| 1 | Connect to the Gaia system **through the console port**. |
| 2 | Reboot:<br>`reboot` |
| 3 | During boot, press any key to enter the **Boot menu**.<br>**Note** - You have approximately 5 seconds. |
| 4 | Select **Start in maintenance mode**. |
| 5 | Enter the Expert mode password. |
| 6 | Use the interactive **lvm_manager** tool as described in the sk95566:<br>`lvm_manager` |
| 7 | Reboot:<br>`reboot` |

### Related information

See *"LVM Overview" on page 701*.

# Network Access

## Introduction

Telnet is **not** recommended for remote login, because it is not secure.

SSH, for example, provides much of the functionality of Telnet with good security.

Network access to Gaia using Telnet is disabled by default. You can allow Telnet access.

## Configuring Telnet Access in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **Network Access**. |
| 2 | Select **Enable Telnet**. |
| 3 | Click **Apply**. |

## Configuring Telnet Access in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

### Syntax

- To configure Telnet access:

```
set net-access telnet {on | off}
```

- To show the configured Telnet access:

```
show net-access telnet
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

# Host Access

You can configure hosts or networks that are allowed to connect to the Gaia Portal or Gaia Clish.

## Configuring Allowed Gaia Clients in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management > Host Access**. |
| 2 | Click **Add**.<br>The **Add a New Allowed Client** window opens. |
| 3 | Select one of these options:<br>■ **Any host** - All remote hosts can access the Gaia Portal, or Gaia Clish.<br>■ **Host** - Enter the IPv4 address of one host.<br>■ **Network** - Enter the IPv4 address of a network and subnet mask. |
| 4 | Click **OK**. |

# Configuring Allowed Gaia Clients in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

### Syntax

- To add an allowed client:

```
add allowed-client
      host
            any-host
            ipv4-address <Host IPv4 Address>
      network ipv4-address <Network IPv4 Address> mask-length
<1-31>
```

- To show the configured allowed clients:

```
show allowed-client all
```

- To delete an allowed client:

```
delete allowed-client
      host
            any-host
            host ipv4-address <Host IPv4 Address>
      network ipv4-address <Network IPv4 Address>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Parameters

| Parameter | Description |
|---|---|
| *<Host IPv4 Address>* | The IPv4 address of the allowed host in dotted decimal format (X.X.X.X) |
| *<Network IPv4 Address>* | The IPv4 address of the allowed network in dotted decimal format (X.X.X.X) |

### Example

```
gaia> add allowed-client host any-host
gaia> show allowed-client all
Type                  Address
Mask Length
Host                  Any
gaia>
```

# LLDP for Management Server and Security Gateway

This section applies to all configured interfaces on these:

- Management Servers, Log Server, SmartEvent Servers
- Security Gateways, Cluster Members

**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-10753).
For a Maestro Orchestrator, see *"LLDP on Maestro Orchestrator" on page 430*.

You can configure Gaia to advertise and receive information from other network devices over the Link Layer Discovery Protocol (LLDP) protocol.

The LLDP is a vendor-neutral link layer protocol that network devices use to advertise their identity, capabilities (and so on) and to receive information about their neighbors on a local area network based on IEEE 802 standard.

The gathered information may include:

- System Name
- System Description
- System Capabilities (switching, routing, etc.)
- Port Description
- Management Address

**Important** - By default, LLDP is *disabled* in the Gaia operating system.

## Configuring LLDP in Gaia Portal on a Management Server / Security Gateway

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **LLDP**. |

| Step | Instructions |
|---|---|
| 2 | In the **Type Length Value (TLV)** section, select which information to send in the LLDP packets, and click **Apply**:<br>■ **System Name**<br>To send the Gaia "<*Hostname*>.<*Domainname*>".<br>Note - To configure the domain name, see *"System Name" on page 253*.<br>■ **System Description**<br>To send the formatted output of the "`uname -msr`" command (which contains the kernel name, kernel release, and kernel machine hardware name).<br>■ **System Capabilities**<br>To send the string "`station`" (regardless of the Check Point configuration).<br>■ **Port Description**<br>To send the name of the interface.<br>■ **Management Address**<br>• Select **Send Management interface IP** to send the IP address of the Gaia Management interface only.<br>• Select **Send Configured interface IP** to send the IP address of each selected interface. |
| 3 | In the **Timers** section, configure the applicable values, and click **Apply**:<br>■ **Transmit Interval**<br>This interval controls how frequently Gaia To send LLDP packets on the selected interfaces.<br>Enter a value between 8 and 32768 (default is 30) seconds.<br>■ **Hold Time Multiplier**<br>This multiplier controls the Time-to Live (TTL) of the LLDP packets:<br>TTL = (Transmit Interval) x (Hold Time Multiplier).<br>This TTL is the duration, for which the receiving neighbor stores the LLDP information in its database.<br>Enter a value between 2 and 10 (default is 4).<br>**Note** - These values are global and apply to all selected interfaces. |

| Step | Instructions |
|---|---|
| 4 | In the **Interfaces** section, add the applicable interfaces.<br>■ To add all interfaces:<br>a. Click **Add All**.<br>b. Click **Yes** to confirm.<br>c. The default LLDP mode for all interfaces is **Transmit and Receive**.<br>To change the LLDP mode:<br>i. Select an interface.<br>ii. Click **Edit**.<br>iii. Select the applicable LLDP mode.<br>iv. Click **Save**.<br>■ To add a specific interface:<br>a. Click **Add**.<br>b. In the **Interface Name** field, select an interface.<br>c. In the **Mode** field, select the applicable LLDP mode.<br>d. Click **Save**.<br>The available LLDP modes are:<br>■ **Transmit and Receive**<br>The interface transmits and receives the LLDP packets.<br>■ **Transmit only**<br>The interface only transmits the LLDP packets, but does not receive the LLDP packets.<br>■ **Receive only**<br>The interface only receives the LLDP packets, but does not transmit the LLDP packets. |
| 5 | In the **LLDP Configuration** section:<br>a. Select **Enable LLDP**.<br>b. Click **Apply**. |

# Configuring LLDP in Gaia Clish on Management Server / Security Gateway

**Workflow:**

| Step | Instructions |
|---|---|
| 1 | Enable the LLDP:<br>`set lldp state on` |
| 2 | Configure the required LLDP settings with the "`set lldp`" command. |
| 3 | Save the changes in the Gaia database:<br>`save config` |

**Syntax**

- To configure LLDP:

```
set lldp
      hold-time-multiplier <2-10>
      interface <Name of Interface>
            receive {on | off}
            transmit {on | off}
            transmit-and-receive {on | off}
      state {on | off}
      tlv
            port-description {on | off}
            system-name {on | off}
            system-description {on | off}
            system-capabilities {on | off}
            management-address {on from {configured-interface
| mgmt-interface} | off}
      transmit-interval <8-32768>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

- To show the LLDP configuration:

```
show lldp
      peers
      status
            interface <Name of Interface>
            timers
            tlv
```

### Parameters

| Parameter | Description |
|---|---|
| `hold-time-multiplier` | This multiplier controls the Time-to Live (TTL) of the LLDP packets:<br>TTL = (Transmit Interval) x (Hold Time Multiplier).<br>This TTL is the duration, for which the receiving neighbor stores the LLDP information in its database.<br>Enter a value between 2 and 10 (default is 4). |
| `interface <Name of Interface>` | Specifies the name of an interface, which sends or receives the LLDP packets. |
| `interface <Name of Interface> receive {on \| off}` | Enables (`on`) and disables (`off`) the LLDP mode on the interface as "receive only".<br>The interface only receives the LLDP packets, but does not transmit the LLDP packets. |
| `interface <Name of Interface> transmit {on \| off}` | Enables (`on`) and disables (`off`) the LLDP mode on the interface as "transmit only".<br>The interface only transmits the LLDP packets, but does not receive the LLDP packets. |
| `interface <Name of Interface> transmit-and-receive {on \| off}` | Enables (`on`) and disables (`off`) the LLDP mode on the interface as "transmit and receive".<br>The interface transmits and receives the LLDP packets. |
| `state {on \| off}` | Enables (`on`) and disables (`off`) the LLDP on the specified interface. |
| `tlv port-description {on \| off}` | Enables (`on`) and disables (`off`) the LLDP-enabled interface to send the Port Description information in the LLDP packets.<br>Sends the name of the interface. |
| `tlv system-name {on \| off}` | Enables (`on`) and disables (`off`) the LLDP-enabled interface to send the System Name information in the LLDP packets.<br>Sends the Gaia "`<Hostname>.<Domainname>`".<br>Note - To configure the domain name, see *"System Name" on page 253*. |

| Parameter | Description |
|---|---|
| `tlv system-description {on \| off}` | Enables (`on`) and disables (`off`) the LLDP-enabled interface to send the System Description information in the LLDP packets.<br>Sends the formatted output of the "`uname -msr`" command<br>(which contains kernel name, kernel release, and kernel machine hardware name). |
| `tlv system-capabilities {on \| off}` | Enables (`on`) and disables (`off`) the LLDP-enabled interface to send the System Capabilities information in the LLDP packets.<br>Sends the string "`station`" (regardless of the Check Point configuration). |
| `tlv management-address {on \| off}` | Enables (`on`) and disables (`off`) the LLDP-enabled interface to send the Management Address information in the LLDP packets.<br>■ `from mgmt-interface` - Sends the IP address of the Gaia Management interface only.<br>■ `from configured-interface` - Sends the IP address of each LLDP-enabled interface. |
| `transmit-interval <8-32768>` | This interval controls how frequently the LLDP-enabled interface sends the LLDP packets.<br>Enter a value between 8 and 32768 (default is 30) seconds. |
| `timers` | Shows the configured LLDP timers:<br>■ Hold Time Multiplier<br>■ Transmit Interval |

### Example - Viewing the LLDP status

```
MyGaia> show lldp status
LLDP server  enabled
Interfaces
eth0 - receive
eth1 - receive and transmit
eth2 - transmit
Optional Information
port-description off
system-name on
system-description off
system-capabilities on
management-address on
Timers
Hold time multiplier 5
Transmit interval 20
MyGaia>
```

# LLDP on Maestro Orchestrator

This section applies only to external interfaces (Management ports and Uplink ports) on the Maestro Orchestrator.

**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-10753).

You can configure Gaia to advertise and receive information from other network devices over the Link Layer Discovery Protocol (LLDP) protocol.

The LLDP is a vendor-neutral link layer protocol that network devices use to advertise their identity, capabilities (and so on) and to receive information about their neighbors on a local area network based on IEEE 802 standard.

The gathered information may include:

- System Name
- System Description
- System Capabilities (switching, routing, etc.)
- Port Description
- Management Address

**Important** - By default, LLDP is **disabled** in the Gaia operating system.

**Notes** - In a Maestro environment:

- The Security Appliances send LLDP packets to the Orchestrator.
  Based on these LLDP packets, the Orchestrator maintains the internal database of the Security Appliances and the Orchestrator ports, to which they are connected.
- After you assign Security Appliances to a Security Group, the Orchestrator sends the LLDP packets to the assigned Security Appliances.
  These LLDP packets contain the required Security Group ID and the Security Group Member ID.
- If you change the state of the LLDPD daemon to "`off`" on the Orchestrator, it stops the LLDPD daemon from transmitting and processing LLDP PDUs on the Orchestrator's external interfaces (Management ports and Uplink ports).
  However, the LLDPD daemon continues to transmit and process LLDP PDUs on the Orchestrator's Downlink ports. It is not support to disable LLDP PDUs on the Orchestrator's Downlink ports.
- The external ports appear in the Gaia OS on the Orchestrator with these names:
  - `eth<X>-Mgmt<X>`
    Management ports
  - `eth<X>-<XX>`
    Uplink ports
  - `eth<X>-Sync-<X>-<YZ>`
    Ports for the internal synchronization and the external synchronization
- The port for the external synchronization between Maestro Sites ("`site_sync`") on each Orchestrator appears in the Gaia OS with this interface name:
  `eth<Orchestrator_Member_ID>-Sync-E-<Port_Logical_ID>`
  Example: `eth1-Sync-E-121`
- The port for the internal synchronization on the same Maestro Site ("`ssm_sync`") on each Orchestrator appears in the Gaia OS with this interface name:
  `eth<Orchestrator_Member_ID>-Sync-I-<Port_Logical_ID>`
  Example: `eth1-Sync-I-125`

# Configuring LLDP in Gaia Portal on an Orchestrator

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **System Management** > **LLDP**. |

| Step | Instructions |
|---|---|
| 2 | In the **Type Length Value (TLV)** section, select which information to send in the LLDP packets, and click **Apply**:<br>■ **System Name**<br>To send the Gaia "<*Hostname*>.<*Domainname*>".<br>Note - To configure the domain name, see *"System Name" on page 253*.<br>■ **System Description**<br>To send the formatted output of the "`uname -msr`" command (which contains the kernel name, kernel release, and kernel machine hardware name).<br>■ **System Capabilities**<br>To send the string "`station`" (regardless of the Check Point configuration).<br>■ **Port Description**<br>To send the name of the interface.<br>■ **Management Address**<br>• Select **Send Management interface IP** to send the IP address of the Gaia Management interface only.<br>• Select **Send Configured interface IP** to send the IP address of each selected interface. |
| 3 | In the **Timers** section, it is not supported to change the default values:<br>■ **Transmit Interval**<br>This interval controls how frequently Gaia To send LLDP packets on the selected interfaces.<br>Default: 8 seconds.<br>■ **Hold Time Multiplier**<br>This multiplier controls the Time-to Live (TTL) of the LLDP packets:<br>TTL = (Transmit Interval) x (Hold Time Multiplier).<br>This TTL is the duration, for which the receiving neighbor stores the LLDP information in its database.<br>Default: 3.<br>**Note** - These values are global and apply to all selected interfaces. |

| Step | Instructions |
|---|---|
| 4 | In the **Interfaces** section, add the applicable interfaces.<br>By default, Gaia OS selects the ports for the internal synchronization and the the internal synchronization.<br><br>■ To add all interfaces:<br>a. Click **Add All**.<br>b. Click **Yes** to confirm.<br>c. The default LLDP mode for all interfaces is **Transmit and Receive**.<br>To change the LLDP mode:<br>i. Select an interface.<br>ii. Click **Edit**.<br>iii. Select the applicable LLDP mode.<br>iv. Click **Save**.<br>■ To add a specific interface:<br>a. Click **Add**.<br>b. In the **Interface Name** field, select an interface.<br>c. In the **Mode** field, select the applicable LLDP mode.<br>d. Click **Save**.<br><br>The available LLDP modes are:<br><br>■ **Transmit and Receive**<br>The interface transmits and receives the LLDP packets.<br>■ **Transmit only**<br>The interface only transmits the LLDP packets, but does not receive the LLDP packets.<br>■ **Receive only**<br>The interface only receives the LLDP packets, but does not transmit the LLDP packets. |
| 5 | In the **LLDP Configuration** section:<br><br>a. Select **Enable LLDP on external interfaces**.<br>b. Click **Apply**. |

# Configuring LLDP in Gaia Clish on an Orchestrator

By default, Gaia OS selects the ports for the internal synchronization and the the internal synchronization.

**Workflow:**

| Step | Instructions |
|---|---|
| 1 | Enable the LLDP on the external ports:<br>`set lldp state on` |
| 2 | Configure the required LLDP settings with the "`set lldp`" command. |
| 3 | Save the changes in the Gaia database:<br>`save config` |

**Syntax**

- To configure LLDP on Orchestrator:

```
set lldp
      hold-time-multiplier <2-10>
      interface <Name of Interface>
            receive {on | off}
            transmit {on | off}
            transmit-and-receive {on | off}
      state {on | off}
      tlv
            port-description {on | off}
            system-name {on | off}
            system-description {on | off}
            system-capabilities {on | off}
            management-address {on from {configured-interface
| mgmt-interface} | off}
      transmit-interval <8-32768>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

- To show the LLDP configuration on Orchestrator:

```
show lldp
      peers
      status
            interface <Name of Interface>
            timers
            tlv
```

### Parameters

| Parameter | Description |
|---|---|
| `hold-time-multiplier` | This multiplier controls the Time-to Live (TTL) of the LLDP packets:<br>TTL = (Transmit Interval) x (Hold Time Multiplier).<br>This TTL is the duration, for which the receiving neighbor stores the LLDP information in its database.<br>Default: 3.<br>**Note** - It is not supported to change the default value. |
| `interface <Name of Interface>` | Specifies the name of an interface, which sends or receives the LLDP packets. |
| `interface <Name of Interface> receive {on \| off}` | Enables (`on`) and disables (`off`) the LLDP mode on the interface as "receive only".<br>The interface only receives the LLDP packets, but does not transmit the LLDP packets. |
| `interface <Name of Interface> transmit {on \| off}` | Enables (`on`) and disables (`off`) the LLDP mode on the interface as "transmit only".<br>The interface only transmits the LLDP packets, but does not receive the LLDP packets. |
| `interface <Name of Interface> transmit-and-receive {on \| off}` | Enables (`on`) and disables (`off`) the LLDP mode on the interface as "transmit and receive".<br>The interface transmits and receives the LLDP packets. |
| `state {on \| off}` | Enables (`on`) and disables (`off`) the LLDP on the specified interface. |
| `tlv port-description {on \| off}` | Enables (`on`) and disables (`off`) the LLDP-enabled interface to send the Port Description information in the LLDP packets.<br>Sends the name of the interface. |
| `tlv system-name {on \| off}` | Enables (`on`) and disables (`off`) the LLDP-enabled interface to send the System Name information in the LLDP packets.<br>Sends the Gaia "`<Hostname>.<Domainname>`".<br>Note - To configure the domain name, see *"System Name" on page 253*. |

| Parameter | Description |
|---|---|
| `tlv system-description {on \| off}` | Enables (`on`) and disables (`off`) the LLDP-enabled interface to send the System Description information in the LLDP packets.<br>Sends the formatted output of the "`uname -msr`" command<br>(which contains kernel name, kernel release, and kernel machine hardware name). |
| `tlv system-capabilities {on \| off}` | Enables (`on`) and disables (`off`) the LLDP-enabled interface to send the System Capabilities information in the LLDP packets.<br>Sends the string "`station`" (regardless of the Check Point configuration). |
| `tlv management-address {on \| off}` | Enables (`on`) and disables (`off`) the LLDP-enabled interface to send the Management Address information in the LLDP packets.<br>■ `from mgmt-interface` - Sends the IP address of the Gaia Management interface only.<br>■ `from configured-interface` - Sends the IP address of each LLDP-enabled interface. |
| `transmit-interval <8-32768>` | This interval controls how frequently the LLDP-enabled interface sends the LLDP packets.<br>Default: 8 seconds.<br>**Note** - It is not supported to change the default value. |
| `timers` | Shows the configured LLDP timers:<br>■ Hold Time Multiplier<br>■ Transmit Interval |

### Example - Viewing the LLDP status

```
MHO_1_1> show lldp status
LLDP is enabled on external interfaces
Interfaces
Mgmt1 - transmit and receive
eth1-05 - transmit and receive
eth1-09 - transmit and receive
eth1-17 - transmit and receive
eth1-21 - transmit and receive
eth1-25 - transmit and receive
eth1-29 - transmit and receive
eth1-33 - transmit and receive
eth1-37 - transmit and receive
eth1-41 - transmit and receive
eth1-45 - transmit and receive
eth1-49 - transmit and receive
eth1-53 - transmit and receive
eth1-57 - transmit and receive
eth1-61 - transmit and receive
eth1-Mgmt1 - transmit and receive
eth1-Sync-E-121 - transmit and receive
eth1-Sync-I-125 - transmit and receive
Optional Information
port-description off
system-name on
system-description off
system-capabilities off
management-address on from configured-interface
Timers
Hold time multiplier 3
Transmit interval 8
MHO_1_1>
```

# Configuring LLDP in the Expert mode on an Orchestrator

You can configure advanced LLDP settings in the Expert mode.

**To control the automatic LLDP configuration "transmit-and-receive on" on any new port with the type "ssm_sync" (internal sync) and "site_sync" (external sync):**

By default, this feature is enabled.

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on the Orchestrator. |
| 2 | Log in. |
| 3 | If your default shell is Gaia Clish, then go to the Expert mode:<br>`expert` |
| 4 | Add the required configuration in the Gaia database:<br>■ To enable this feature (this is the default), run:<br>`dbset maestro:lldp:set_lldp_rx_and_tx_to_on_upon_sync_interface_creation true`<br>■ To disable this feature, run:<br>`dbset maestro:lldp:set_lldp_rx_and_tx_to_on_upon_sync_interface_creation` |
| 5 | Save the changes in the Gaia database:<br>`dbset :save` |

**To control the automatic LLDP configuration "transmit-and-receive on" of any new port:**

By default, this feature is disabled.

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on the Orchestrator. |
| 2 | Log in. |
| 3 | If your default shell is Gaia Clish, then go to the Expert mode:<br>`expert` |

| Step | Instructions |
|---|---|
| 4 | Add the required configuration in the Gaia database:<br>■ To enable this feature, run:<br>`dbset maestro:lldp:set_lldp_rx_and_ tx_to_on_upon_interface_creation true`<br>■ To disable this feature (this is the default), run:<br>`dbset maestro:lldp:set_lldp_rx_and_ tx_to_on_upon_interface_creation` |
| 5 | Save the changes in the Gaia database:<br>`dbset :save` |

# Advanced Routing

Dynamic Routing is fully integrated into the Gaia Portal and Gaia Clish.

BGP, OSPF and RIP are supported.

Dynamic Multicast Routing is supported, with PIM (Sparse Mode (SM), Dense Mode (DM), Source-Specific Multicast (SSM), and IGMP.

To learn about dynamic routing, see the *R82 Gaia Advanced Routing Administration Guide*.

# User Management

This chapter describes how to manage passwords, user accounts, roles, authentication servers, system groups, and Gaia Portal clients.

**Note** - When a user logs in to Gaia, the Gaia Portal navigation tree displayed and Gaia Clish commands that are available depend on the role or roles assigned to the user. If the user's roles do not provide access to a feature, the user does not see the feature in the Gaia Portal navigation tree or in the list of commands. If the user has read-only access to a feature, they can see the Gaia Portal page, but the controls are disabled. Similarly, the user can run "`show` commands, but not "`set`", "`add`" or "`delete`" commands.

# Authentication

This section describes:

- How to change your Gaia login password.
- How to enable and configure Two-Factor Authentication for Gaia login.

## Changing Your Gaia Login Password

A Gaia user can change their Gaia login password - in Gaia Portal or Gaia Clish.

**Changing your password in Gaia Portal**

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`).<br>**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group. |
| 1 | In the navigation tree, click **User Management** > **Authentication**.<br>Refer to the section **Change Password**. |
| 2 | In the **Old Password** field, enter your old password. |
| 3 | In the **New Password** field, enter the new password. |
| 4 | In the **Confirm New Password** field, enter the new password again. |
| 5 | Click **Apply**. |

### Changing your password in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

#### Description

Change your Gaia login password in an interactive dialog.

#### Syntax

```
set selfpasswd
```

**Warning** - We do not recommend to use this command:

```
set selfpasswd oldpass <Old Password> passwd <New Password>
```

This is because the passwords are stored as plain text in the command history. Instead, use the "`set selfpasswd`" command.

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

# Two-Factor Authentication for Gaia Login

Two-Factor Authentication (2FA) adds an additional authentication factor to the Gaia login flow using a time-based authentication app.

When enabled, 2FA protects all logins to the Gaia operating system:

- Gaia Portal.
- All CLI shells for a remote login (over SSH or Telnet) and the local login (through a console port or LOM Card):

  For more information about these CLI shells, see *"Users" on page 469*.

  **Important** - 2FA protects only the **Normal** boot mode and the **Debug** boot mode. 2FA does not protect the **Maintenance** boot mode to make sure you can access the operating system to troubleshoot various issues.

  - Gaia Clish (`/bin/cli.sh`).
  - Gaia gClish (`/usr/bin/gclish`, `/bin/clish`) on Scalable Platforms.
  - Expert mode - Bourne Again shell (`/bin/bash`).
  - C shell (`/bin/csh`).
  - Turbo C shell (`/bin/tcsh`).
  - Bourne shell (`/bin/sh`).
  - Terminal shell from Gaia Portal.
- RESTful API access.

You can configure the Two-Factor Authentication settings in these ways:

- In Gaia Portal (described below).
- In Gaia Clish (described below).
- With Gaia RESTful API (see *"Working with Gaia RESTful API" on page 749* > in the API reference, see the chapter "*Users Management*" > sections "*Users*" and "*Passwords Control*").

# Enabling Two-Factor Authentication for Specific Users

### Part 1 of 2 - Forcing Two-Factor Authentication for specific users

Follow the applicable procedure in Gaia Portal or Gaia Clish / Gaia gClish.

#### Procedure in Gaia Portal to force Two-Factor Authentication for a specific user

An administrator can force Two-Factor Authentication for specific users.

Each of these users generates the authentication keys during their next login. See Part 2 of 2 below.

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`).<br>Log in with credentials of an administrator.<br>**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group. |
| 2 | In the navigation tree, click **User Management** > **Users**. |
| 3 | Select the applicable user. |
| 4 | From the top toolbar, click **Edit**. |
| 5 | Select **Force to use Two-Factor Authentication**. |
| 6 | Click **OK**. |

### Procedure in Gaia Clish to force Two-Factor Authentication for a specific user

An administrator can enable Two-Factor Authentication for specific users.

Each of these users generates the authentication keys during their next login. See Part 2 of 2 below.

| Step | Instructions |
|---|---|
| 1 | Connect to the command line.<br>Log in with credentials of an administrator.<br>**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group. |
| 2 | If your default shell is the Expert mode, then go to Gaia Clish:<br>`clish`<br>On Scalable Platforms, go to Gaia gClish:<br>Type `gclish` and press Enter. |
| 3 | Force Two-Factor Authentication for the specific user:<br>`set user <username> force-two-factor-authentication yes` |
| 4 | Save the changes:<br>`save config` |
| 5 | Examine the status of the forced Two-Factor Authentication for the user:<br>`show user <username> force-two-factor-authentication` |
| 6 | Examine the state of Two-Factor Authentication for the user:<br>`show user <username> two-factor-authentication state` |

### Procedure in Gaia Portal to force Two-Factor Authentication for all users at the same time (including all administrators)

An administrator can force Two-Factor Authentication for all users at the same time (including all administrators).

Each user generates the authentication keys during their next login. See Part 2 of 2 below.

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`).<br>Log in with credentials of an administrator.<br>**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group. |
| 2 | In the navigation tree, click **User Management** > **Password Policy**. |
| 3 | In the section **Two-Factor Authentication**, select **Force all users to use Two-Factor Authentication**. |
| 4 | Click **Apply**. |
| 5 | Click **Yes** to confirm this prompt:<br>`After performing this operation, you will be logged out and will need to log in again.`<br>`Are you sure you want to proceed?` |

### Procedure in Gaia Clish to force Two-Factor Authentication for all users at the same time (including all administrators)

An administrator can force Two-Factor Authentication for all users at the same time (including all administrators).

Each user generates the authentication keys during their next login. See Part 2 of 2 below.

| Step | Instructions |
|---|---|
| 1 | Connect to the command line.<br>Log in with credentials of an administrator.<br>**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group. |
| 2 | If your default shell is the Expert mode, then go to Gaia Clish:<br>`clish`<br>On Scalable Platforms, go to Gaia gClish:<br>Type `gclish` and press Enter. |
| 3 | Force Two-Factor Authentication for all users in Gaia Password Policy:<br>`set password-controls force-two-factor-authentication yes` |
| 4 | Save the changes:<br>`save config` |
| 5 | Examine the status of the forced Two-Factor Authentication for all users:<br>`show password-controls force-two-factor-authentication` |

### Part 2 of 2 - First login experience of a user with the forced Two-Factor Authentication (or newly generated authentication keys)

This part describes the user experience in these scenarios:

- An administrator forced Two-Factor Authentication for a specific user or all users, and the user did not generate Two-Factor Authentication keys yet.
- An administrator generated new Two-Factor Authentication keys for a specific user.

**First login experience in Gaia Portal of a user with the forced Two-Factor Authentication (or newly generated authentication keys)**

This is the experience of the user during their next login in Gaia Portal:

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`).<br>**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group. |
| 2 | Enter your username and press the Enter key (or click **Next**). |
| 3 | Enter your password and press the Enter key (or click **Login**). |
| 4 | Click **Set Up**.<br>Follow the instructions on the screen to configure an account in the 2FA app on your mobile device. |
| 5 | Install a supported 2FA time-based app on your mobile device. See sk181854. |
| 6 | In the 2FA app:<br>a. Tap the applicable button to add a new account.<br>b. Tap the applicable account type option.<br>c. Scan the QR code you see in Gaia Portal.<br>Alternatively, use the pre-shared key you see in Gaia Portal. |
| 7 | Click **Next**. |
| 8 | Save the 2FA backup keys.<br>You can copy them from Gaia Portal or click **Download backup keys**.<br>**Warnings:**<br>■ Gaia Portal shows these backup keys only one time.<br>You can find these backup keys in this file:<br>`/etc/2fa_keys/<username>/.google_authenticator`<br>■ Keep these backup keys in a secure location.<br>■ Do **not** share these backup keys with unauthorized personnel. |
| 9 | Click **Done**. |

| Step | Instructions |
|---|---|
| 10 | If you forgot to save the 2FA backup keys, then click **Cancel** to go to the previous page.<br>If you already saved the 2FA backup keys, then click **OK**. |

**First login experience in CLI of a user with the forced Two-Factor Authentication (or newly generated authentication keys)**

This is the experience of the specific user during their next login in CLI (regardless of their default shell):

| Step | Instructions |
|---|---|
| 1 | Connect to the command line.<br>**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group. |
| 2 | Enter your username and password. |
| 3 | In this prompt, enter "y" and press the Enter key:<br>`Your security administrator requires you to use Two-Factor Authentication. Do you want to proceed? (y/n):` |
| 4 | CLI shell shows this information (and then shows the shell prompt):<br>■ QR Code to create an account in the 2FA app<br>■ Secret key to create an account in the 2FA app<br>■ Emergency scratch codes (2FA backup keys)<br>**Warnings:**<br>• Gaia Clish shows these backup keys only one time. You can find these backup keys in this file: `/etc/2fa_keys/<username>/.google_authenticator`<br>• Keep these backup keys in a secure location.<br>• Do **not** share these backup keys with unauthorized personnel. |
| 5 | Install a supported 2FA time-based app on your mobile device. See sk181854. |
| 6 | In the 2FA app:<br>a. Tap the applicable button to add a new account.<br>b. Tap the applicable account type option.<br>c. Scan the QR code you see in Gaia Clish.<br>Alternatively, use the secret key you see in Gaia Clish. |

# Enabling Two-Factor Authentication for the Current User

### Procedure in Gaia Portal to enable Two-Factor Authentication for the current user only

A user with the required permissions can enable Two-Factor Authentication for their username in the current session.

The current user generates the authentication keys during the current session.

**Warning** - If you started this procedure, but changed your mind in the middle, then you must **not** close Gaia Portal.
If you just close Gaia Portal or let the session time out, then your user will be locked out without any possibility to log in.
You must do one of these:

- Complete the procedure.
- Click **Cancel** > enter your Gaia login password > click **OK** > click **Yes** to confirm.
  This completely disables Two-Factor Authentication.

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`).<br>Log in with credentials of an administrator.<br>**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group. |
| 2 | In the navigation tree, click **User Management** > **Authentication**. |
| 3 | In the section **Two-Factor Authentication Settings**, click **Enable Two-Factor Authentication**. |
| 4 | Install a supported 2FA time-based app on your mobile device. See sk181854. |
| 5 | In the 2FA app:<br>a. Tap the applicable button to add a new account.<br>b. Tap the applicable account type option.<br>c. Scan the QR code you see in Gaia Portal.<br>Alternatively, use the pre-shared key you see in Gaia Portal. |
| 6 | Click **Next**. |

| Step | Instructions |
|---|---|
| 7 | Save the 2FA backup keys.<br>You can copy them from Gaia Portal or click **Download backup keys**.<br>**Warnings:**<br>■ Gaia Portal shows these backup keys only one time.<br>You can find these backup keys in this file:<br>`/etc/2fa_keys/<username>/.google_authenticator`<br>■ Keep these backup keys in a secure location.<br>■ Do **not** share these backup keys with unauthorized personnel. |
| 8 | Click **Done**. |
| 9 | If you forgot to save the 2FA backup keys, then click **Cancel** to go to the previous page.<br>If you already saved the 2FA backup keys, then click **OK**. |

### Procedure in Gaia Clish to enable Two-Factor Authentication for the current user only

A user with the required permissions can enable Two-Factor Authentication for their username in the current session.

The current user generates the authentication keys during their next login.

| Step | Instructions |
|---|---|
| 1 | Connect to the command line.<br>Log in with credentials of an administrator.<br>**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group. |
| 2 | If your default shell is the Expert mode, then go to Gaia Clish:<br>`clish`<br>On Scalable Platforms, go to Gaia gClish:<br>Type `gclish` and press Enter. |
| 3 | Force Two-Factor Authentication for the currently logged in user:<br>`set two-factor-authentication state on` |
| 4 | Save the changes:<br>`save config` |
| 5 | Examine the status of the forced Two-Factor Authentication for the user:<br>`show user <username> force-two-factor-authentication` |
| 6 | Examine the state of the Two-Factor Authentication for the currently logged in user:<br>`show two-factor-authentication state` |

## Generating New Two-Factor Authentication Keys

An administrator can generate new 2FA keys for a specific user.

Follow the applicable procedure in Gaia Portal or Gaia Clish / Gaia gClish.

**Procedure in Gaia Portal to generate new Two-Factor Authentication keys for a specific user - configuration of 2FA keys occurs during the next login**

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`).<br>Log in with credentials of an administrator.<br>**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group. |
| 2 | In the navigation tree, click **User Management** > **Users**. |
| 3 | Select the user.<br>You can select your username of a different username. |
| 4 | From the top toolbar, click **Regenerate Key**. |
| 5 | Click **OK** to confirm. |
| 6 | When a user connects to the Gaia operating system the next time, the user must:<br>a. Enter their username.<br>b. Enter their password.<br>c. Follow the instructions on the screen to continue:<br>▪ In Gaia Portal, click **Set Up**.<br>▪ In Gaia Clish, enter "`y`" in the prompt.<br>d. In the 2FA app, remove the current account.<br>e. In the 2FA app, add a new account. |

**Procedure in Gaia Clish to generate new Two-Factor Authentication keys for a specific user - configuration of 2FA keys occurs during the next login**

| Step | Instructions |
|---|---|
| 1 | Connect to the command line.<br>Log in with credentials of an administrator.<br>**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group. |
| 2 | If your default shell is the Expert mode, then go to Gaia Clish:<br>`clish`<br>On Scalable Platforms, go to Gaia gClish:<br>Type `gclish` and press Enter. |
| 3 | Force the generation of new Two-Factor Authentication keys for the specific user:<br>`set user <username> regenerate-two-factor-authentication` |
| 4 | Save the changes:<br>`save config` |

### Procedure in Gaia Portal to generate new Two-Factor Authentication keys for the current user - configuration of 2FA keys during the current login

An administrator can generate new 2FA keys for their username and force the configuration of the 2FA keys during the current login.

**Warning** - If you started this procedure, but changed your mind in the middle, then you must **not** close Gaia Portal.
If you just close Gaia Portal or let the session time out, then users will be locked out without any possibility to log in.
You must do one of these:

- Complete the procedure.
- Click **Cancel** > enter your Gaia login password > click **OK** > click **Yes** to confirm.
  This completely disables Two-Factor Authentication.

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`).<br>Log in with your credentials.<br>**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group. |
| 2 | In the navigation tree, click **User Management** > **Authentication**.<br>Refer to the section **Two-Factor Authentication Settings**. |
| 3 | Click **Regenerate the Authentication Key**. |
| 4 | Enter your Gaia login password. |
| 5 | In the 2FA app:<br>a. Delete the current account.<br>b. Tap the applicable button to add a new account.<br>c. Tap the applicable account type option.<br>d. Scan the QR code you see in Gaia Portal. |
| 6 | Click **Next**. |

| Step | Instructions |
|---|---|
| 7 | Save the 2FA backup keys.<br>You can copy them from Gaia Portal or click **Download backup keys**.<br>**Warnings:**<br>■ Gaia Portal shows these backup keys only one time.<br>You can find these backup keys in this file:<br>`/etc/2fa_keys/<username>/.google_authenticator`<br>■ Keep these backup keys in a secure location.<br>■ Do **not** share these backup keys with unauthorized personnel. |
| 8 | Click **Done**. |
| 9 | If you forgot to save the 2FA backup keys, then click **Cancel** to go to the previous page.<br>If you already saved the 2FA backup keys, then click **OK**. |

# Disabling Two-Factor Authentication for Specific Users

Follow the applicable procedure in Gaia Portal or Gaia Clish / Gaia gClish.

### Part 1 of 2 - Disabling the forced Two-Factor Authentication for a specific user

#### Procedure in Gaia Portal to disable the forced Two-Factor Authentication for a specific user

An administrator can disable the forced Two-Factor Authentication for specific users.

The specific user must manually disable Two-Factor Authentication.

**Note** - This is possible only if Two-Factor Authentication is not forced for all users by the Gaia Password Policy.

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`).<br>Log in with credentials of an administrator.<br>**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group. |
| 2 | In the navigation tree, click **User Management** > **Users**. |
| 3 | Select the applicable user. |
| 4 | From the top toolbar, click **Edit**. |
| 5 | Clear **Force to use Two-Factor Authentication**. |
| 6 | Click **OK**. |

### Procedure in Gaia Clish to disable the forced Two-Factor Authentication for a specific user

An administrator can disable the forced Two-Factor Authentication for specific users.

The specific user must manually disable Two-Factor Authentication.

**Note** - This is possible only if Two-Factor Authentication is not forced for all users by the Gaia Password Policy.

| Step | Instructions |
|---|---|
| 1 | Connect to the command line.<br>Log in with credentials of an administrator.<br>**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group. |
| 2 | If your default shell is the Expert mode, then go to Gaia Clish:<br>`clish`<br>On Scalable Platforms, go to Gaia gClish:<br>Type `gclish` and press Enter. |
| 3 | Disable Two-Factor Authentication for the specific user:<br>`set user <username> force-two-factor-authentication no` |
| 4 | Save the changes:<br>`save config` |
| 5 | Examine the status of the forced Two-Factor Authentication for the user:<br>`show user <username> force-two-factor-authentication` |
| 6 | Examine the state of the Two-Factor Authentication for the user:<br>`show user <username> two-factor-authentication state` |

## Part 2 of 2 - Disabling Two-Factor Authentication by the specific user

### Procedure

Follow the applicable procedure in the section *"Disabling Two-Factor Authentication for the Current User" on page 465*.

# Disabling Two-Factor Authentication for All Users

Follow the applicable procedure in Gaia Portal or Gaia Clish / Gaia gClish.

### Part 1 of 2 - Disabling the forced Two-Factor Authentication for all users

#### Procedure in Gaia Portal to disable the forced Two-Factor Authentication for all users

An administrator can disable the forced Two-Factor Authentication for all users.

Each user must manually disable Two-Factor Authentication.

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`).<br>Log in with credentials of an administrator.<br>**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group. |
| 2 | In the navigation tree, click **User Management** > **Password Policy**. |
| 3 | In the section **Two-Factor Authentication**, clear **Force all users to use Two-Factor Authentication**. |
| 4 | Click **Apply**. |
| 5 | In the navigation tree, click **User Management** > **Users**. |
| 6 | For each user with the state **Enabled** in the column **Two-Factor Authentication**:<br>a. Select the user.<br>b. From the top toolbar, click **Edit**.<br>c. Clear **Force to use Two-Factor Authentication**.<br>d. Click **OK**. |

### Procedure in Gaia Clish to disable the forced Two-Factor Authentication for all users

An administrator can disable the forced Two-Factor Authentication for all users.

Each user must manually disable Two-Factor Authentication.

| Step | Instructions |
|---|---|
| 1 | Connect to the command line.<br>Log in with credentials of an administrator.<br>**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group. |
| 2 | If your default shell is the Expert mode, then go to Gaia Clish:<br>`clish`<br>On Scalable Platforms, go to Gaia gClish:<br>Type `gclish` and press Enter. |
| 3 | Disable Two-Factor Authentication for all users in Gaia Password Policy:<br>`set password-controls force-two-factor-authentication no` |
| 4 | Save the changes:<br>`save config` |
| 5 | Examine the list of users:<br>`show users` |
| 6 | Examine the state of Two-Factor Authentication for each user:<br>`show user <username> two-factor-authentication state` |
| 7 | Disable Two-Factor Authentication for each user, for whom it is currently enabled:<br>`set user <username> force-two-factor-authentication no` |
| 8 | Save the changes:<br>`save config` |

### Part 2 of 2 - Disabling Two-Factor Authentication by the specific user

#### Procedure

Follow the applicable procedure in the section *"Disabling Two-Factor Authentication for the Current User" below*.

## Disabling Two-Factor Authentication for the Current User

Follow the applicable procedure in Gaia Portal or Gaia Clish / Gaia gClish.

#### Procedure in Gaia Portal to disable Two-Factor Authentication for the current user only

A user can disable Two-Factor Authentication for their username in the current session.

**Note** - This is possible only if Two-Factor Authentication is not forced in these places:

- For all users by the Gaia Password Policy.
- For the current user in their user object.

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`).<br>Log in with your credentials and a Two-Factor Authentication key.<br>**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group. |
| 2 | In the navigation tree, click **User Management** > **Authentication**. |
| 3 | In the section **Two-Factor Authentication Settings**, click **Disable Two-Factor Authentication**. |
| 4 | Enter your Gaia login password. |
| 5 | Click **OK**. |
| 6 | Click **Yes** to confirm. |
| 7 | In the navigation tree, click **User Management** > **Users**. |
| 8 | In the row for your username, the column **Two-Factor Authentication** must show **Disabled**. |

### Procedure in Gaia Clish to disable Two-Factor Authentication for the current user only

A user can disable Two-Factor Authentication for their username in the current session.

**Note** - This is possible only if Two-Factor Authentication is not forced in these places:

- For all users by the Gaia Password Policy.
- For the current user in their user object.

| Step | Instructions |
|---|---|
| 1 | Connect to the command line.<br>Log in with your credentials and a Two-Factor Authentication key.<br>**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group. |
| 2 | If your default shell is the Expert mode, then go to Gaia Clish:<br>`clish`<br>On Scalable Platforms, go to Gaia gClish:<br>Type `gclish` and press Enter. |
| 3 | Examine the status of the forced Two-Factor Authentication for the user:<br>`show user <your username> force-two-factor-authentication` |
| 4 | Examine the state of the Two-Factor Authentication for the currently logged in user:<br>`show two-factor-authentication state` |
| 5 | Disable Two-Factor Authentication for the currently logged in user:<br>`set two-factor-authentication state off` |
| 6 | Save the changes:<br>`save config` |

## Gaia Clish / Gaia gClish Syntax for Two-Factor Authentication

The applicable procedures appear above in the corresponding sections.

**Syntax**

**Syntax to force Two-Factor Authentication for specific users:**

```
set user <username> force-two-factor-authentication {yes | no}
show user <username> force-two-factor-authentication
show user <username> two-factor-authentication state
```

**Syntax to force Two-Factor Authentication for all users:**

```
set password-controls force-two-factor-authentication {yes | no}
show password-controls force-two-factor-authentication
```

**Syntax to enable Two-Factor Authentication for the currently logged-in user:**

```
set two-factor-authentication state {on | off}
show two-factor-authentication state
```

**Syntax to generate new Two-Factor Authentication keys for a specific user (during the next login):**

```
set user <username> regenerate-two-factor-authentication
```

## Troubleshooting

**What to do if you lost your smartphone and do not have 2FA backup codes**

These steps are available:

| Scenario | Available Steps |
|---|---|
| There is at least one Gaia administrator who can log in | ■ An administrator needs to generate new Two-Factor Authentication keys for the affected user.<br>■ An administrator needs to boot into the **Maintenance** boot mode and delete this file for the affected user: `/etc/2fa_keys/<username>/.google_authenticator` |
| There are no Gaia administrators who can log in | ■ Restore the Gaia operating system to Factory Defaults from the Boot Menu.<br>■ Perform a clean install from a bootable device. See sk65205. |

# Users

Use the Gaia Portal and Gaia Clish to manage user accounts.

You can:

- Add users to your Gaia system.
- Edit the home directory of the user.
- Edit the default shell for a user.
- Give a password to a user.
- Give privileges to users.

These users are created by default and **cannot** be deleted:

| User | Description |
|---|---|
| **admin** | Has full read/write capabilities for all Gaia features, from the Gaia Portal and the Gaia Clish.<br>This user has a User ID of 0, and therefore has all of the privileges of a root user. |
| **monitor** | Has read-only capabilities for all features in the Gaia Portal and the Gaia Clish, and can change its own password.<br>You must give a password for this user before the account can be used. |

New users have read-only privileges to the Gaia Portal and the Gaia Clish / Gaia gClish by default.

You must assign one or more roles before the new users can log in.

**Notes:**

- You can assign permissions to all Gaia features or a subset of the features without assigning a user ID of 0.
  If you assign a user ID of 0 to a user account (you can do this only in the Gaia Clish), the user is equivalent to the Admin user and the roles assigned to that account cannot be modified.
- Do not define a new user for external users.
  An external user is one that is defined on an authentication server (such as RADIUS or TACACS), and not on the local Gaia system.

When you create a user, you can add pre-defined roles (privileges) to the user. For more information, see *"Roles" on page 480*.

**Warning** - A user with read and write permission to the Users feature can change the password of another user, or an admin user. Therefore, write permission to the Users feature should be assigned with caution.

# Managing User Accounts in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Viewing the list of all configured users

In the navigation tree, click **User Management** > **Users**.

You can also see your username in the top right corner of the Gaia Portal.

### Adding a new user

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **Users**. |
| 2 | Click **Add**. |
| 3 | In the **Login Name** field, enter the username.<br>The valid characters (between 1 and 32 characters) are alphanumeric characters, dash (-), and underscore (_). |
| 4 | In the **Password** field, enter the user's password.<br>All printable characters are allowed. Length is between 6 and 128 characters.<br>**Important** - Do not use the asterisk (*) character in the password. User with such password will not be able to log in. |
| 5 | In the **Confirm Password** field, enter the user's password again. |
| 6 | In the **Real Name** field, enter the user's real name or other informative text.<br>This is an alphanumeric string that can contain spaces.<br>The default is the user's Login Name with capitalized first letter. |
| 7 | In the **Home Directory** field, enter the user's home directory.<br>This is the full Linux path name of a directory, to which the user will log in.<br>Must be a sub-directory of `/home/` directory.<br>If the sub-directory does not already exist, it is created. |
| 8 | In the **Shell** field, select the user's default login shell.<br>See the explanations in the **"Login Shells"** section below. |

| Step | Instructions |
|---|---|
| 9 | Select **User must change password at next logon**, if you wish to force the user to change the configured password during the next login.<br>**Note** - If the user does not log in within the time limit configured in the Gaia Portal > **User Management** > **Password Policy** page > **Mandatory Password Change** section > **Lockout users after password expiration** > **Lockout user after X days**, the user may not be able to log in at all. |
| 10 | **Optional:** In the **UID** field, enter or select the applicable User ID:<br>■ **0** for administrator users (this is the default option)<br>■ An integer between **103** and **65533** for non-administrator users (for example, for users with the default shell `/usr/bin/scponly` - see sk88981) |
| 11* | In the **Access Mechanisms** section:<br>■ Select **Web** to allow this user to access Gaia Portal.<br>■ Select **Clish Access** to allow this user to access Gaia Clish.<br>■ Select **Gaia API** to allow this user to access Gaia RESTful API (see *Check Point Gaia API Reference*). |
| 12* | In the **Available Roles** list:<br>a. Select the roles you wish to assign to this user.<br>To select several roles:<br>i. Press and hold the **CTRL** key on the keyboard.<br>ii. Left-click the applicable roles. The selected roles become highlighted.<br>b. Click **Add >**. The selected roles move to the **Assigned Roles** list. |
| 13 | Click **OK**. |

* To configure these settings in Gaia Clish, see *"Configuring Roles in Gaia Clish" on page 485*.

**Login Shells**

| Shell | Description |
|---|---|
| `/etc/cli.sh` | This is the default option.<br>Lets the user work with the full Gaia Clish.<br>By default, some basic networking commands (such as `ping`) are also available.<br>The **Extended Commands** in the assigned roles makes it possible to add more Linux commands that can be used (see *"List of Available Extended Commands in Roles" on page 511*).<br>User can run the `expert` command to enter the Bash shell (Expert mode). |
| `/bin/bash` | BASH Linux shell.<br>Lets the user work with the Expert mode.<br>User can run the `clish` command to enter the Gaia Clish. |
| `/bin/csh` | CSH Linux shell.<br>User can run the `clish` command to enter the Gaia Clish. |
| `/bin/sh` | SH Linux shell.<br>User can run the `clish` command to enter the Gaia Clish. |
| `/bin/tcsh` | TCSH Linux shell.<br>User can run the `clish` command to enter the Gaia Clish. |
| `/usr/bin/scponly` | User is not allowed to log in to Gaia.<br>User can only connect to Gaia over SCP and transfer files to and from the system.<br>Other commands are forbidden. |
| `/sbin/nologin` | User is not allowed to log in to Gaia. |

**Changing the user configuration**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **Users**. |
| 2 | Select the user. |
| 3 | Click **Edit**. |
| 4 | In the **Real Name** field, enter the user's real name or other informative text. |

| Step | Instructions |
|---|---|
| 5 | In the **Home Directory** field, enter the user's home directory. |
| 6 | In the **Shell** field, select the user's default login shell. |
| 7 | Select **User must change password at next logon**, if you wish to force the user to change the configured password during the next login. |
| 8 | In the **Available Roles** list, select the roles you wish to assign to this user and click **Add >**. |
| 9 | In the **Assigned Roles** list, select the roles you wish to remove from this user and click **Remove >**. |
| 10 | Click **OK**. |

**Note** - For the default users **admin** and **monitor**, you can only change the Shell and Roles.

### Deleting a user

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **Users**. |
| 2 | Select the user. |
| 3 | Click **Delete**. |
| 4 | Click **OK** to confirm. |

**Note** - You cannot delete the default users **admin** and **monitor**.

# Managing User Accounts in Gaia Clish

**Important:**

- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

**Note** - You can use the "`add user`" command to add new users, but you must use the "`set user <username> password`" command to configure the password and allow the user to log on to the system.

## Syntax

### Adding a local user account

```
add user <UserName> uid <User ID> homedir <Path>
```

### Adding a RADIUS user account

```
add user <UserName> uid 0 homedir <Path>
```

### Editing a user account

```
set user <UserName>
      force-password-change {yes | no}
      gid <System Group ID>
      homedir <Path>
      lock-out off
      newpass <Password>
      password
      password-hash <Password Hash>
      realname <Name>
      shell <Login Shell>
      uid <User ID>
```

**Note** - For the default users **admin** and **monitor**, you can only change the Shell and Roles.

### Viewing the summary information about all users

```
show users
```

### Viewing information about a specific user

```
show user <UserName>
      [force-password-change]
      [gid]
      [homedir]
      [lock-out]
      [realname]
      [shell]
      [uid]
```

### Deleting a configured user

```
delete user <User ID>
```

**Note** - You cannot delete the default users **admin** and **monitor**.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| `user <UserName>` | Configures unique login username - an alphanumeric string, from 1 to 32 characters long, that can contain dashes (-) and underscores (_), but not spaces: `a-z A-Z 0-9 - _` |
| `uid <User ID>` | Optional. Configures unique User ID to identify permissions of the user:<br>▪ `0` for administrator users and RADIUS user account (this is the default option)<br>▪ An integer between `103` and `65533` for non-administrator user<br>**Notes:**<br>• Configure this UID for users with the default shell `/usr/bin/scponly` - see sk88981.<br>• If you do not enter a value, Gaia OS automatically assigns the next free sequential number. |
| `homedir <Path>` | Configures user's home directory.<br>This is the full Linux path name of a directory, to which the user will log in.<br>Must be a sub-directory of the `/home/` directory.<br>If the sub-directory does not already exist, it is created. |

| Parameter | Description |
|---|---|
| `force-password-change {yes \| no}` | If you wish to force the user to change the configured password during the next login, use the value "`yes`".<br>**Note** - If the user does not log in within the time limit configured by the "`set password-controls expiration-lockout-days`" command, the user may not be able to log in at all. |
| `gid <System Group ID>` | Configures System Group ID (`0-65535`) for the primary group, to which a user belongs.<br>The default is `100`.<br>You can add the user to several groups.<br>Use the "`add group`" and "`set group`" commands to manage the groups. |
| `lock-out off` | Unlocks the user, if the user was locked out.<br>The password expiration date is adjusted, if necessary. |
| `newpass <Password>` | Configures a new password for the user.<br>Gaia does not ask to verify the new password.<br>The password you enter shows on the terminal command line in plain text, and is stored in the command history as plain text. |
| `password` | Configures a password for the new user.<br>The command runs in interactive mode.<br>You must enter the password twice, to verify it.<br>The password you enter is not visible on the terminal command line. |

| Parameter | Description |
|---|---|
| `password-hash <Password Hash>` | The password as an MD5, SHA256, or SHA512 salted hash instead of plain text (the password string must contain at least 6 characters).<br>Use this option when you upgrade or restore using backup scripts.<br>You can generate the hash of the password with the "`cpopenssl`" command (run: `cpopenssl passwd -help`).<br>To configure the default hash algorithm, see:<br>■ *"Password Hashing Algorithm" on page 524* (in Gaia Portal)<br>■ *"Configuring Hashing Algorithm" on page 533* (in Gaia Clish)<br><br>**Best Practice** - Do **not** use MD5 hash because it is not secure.<br><br>**Notes:**<br>■ Format:<br>`$<Hash Standard>$<Salt>$<Encrypted>`<br>■ The length of this hash string must be less than 128 characters.<br>■ *<Hash Standard>*<br>One of these digits:<br>• `1` = MD5<br>• `5` = SHA256<br>• `6` = SHA512<br>■ *<Salt>*<br>A string of these characters:<br>`a-z A-Z 0-9 . / [ ] _ ` ^`<br>The length of this string must be between 2 and 16 characters.<br>■ *<Encrypted>*<br>A string of these characters:<br>`a-z A-Z 0-9 . / [ ] _ ` ^`<br>The length of this string must be:<br>• For MD5, less than 22 characters.<br>• For SHA256, less than 43 characters.<br>• For SHA512, less than 86 characters. |
| `realname <Name>` | Configures user's description - most commonly user's real name.<br>This is an alphanumeric string that can contain spaces.<br>The default is the username with the capitalized first letter. |
| `shell <Login Shell>` | Configures the user's default login shell.<br>See the explanations in the "**Login Shells**" section below. |

**Login Shells**

| Shell | Description |
|---|---|
| `/etc/cli.sh` | This is the default option.<br>Lets the user work with the full Gaia Clish.<br>By default, some basic networking commands (such as `ping`) are also available.<br>The **Extended Commands** in the assigned roles makes it possible to add more Linux commands that can be used (see *"List of Available Extended Commands in Roles" on page 511*).<br>User can run the `expert` command to enter the Bash shell (Expert mode). |
| `/bin/bash` | BASH Linux shell.<br>Lets the user work with the Expert mode.<br>User can run the `clish` command to enter the Gaia Clish. |
| `/bin/csh` | CSH Linux shell.<br>User can run the `clish` command to enter the Gaia Clish. |
| `/bin/sh` | SH Linux shell.<br>User can run the `clish` command to enter the Gaia Clish. |
| `/bin/tcsh` | TCSH Linux shell.<br>User can run the `clish` command to enter the Gaia Clish. |
| `/usr/bin/scponly` | User is not allowed to log in to Gaia.<br>User can only connect to Gaia over SCP and transfer files to and from the system.<br>Other commands are forbidden. |
| `/sbin/nologin` | User is not allowed to log in to Gaia. |

# Roles

Role-based administration (RBA) lets you create administrative roles for users. With RBA, an administrator can allow Gaia users to access specified features by including those features in a role and assigning that role to users. Each role can include a combination of administrative (read/write) access to some features, monitoring (read-only) access to other features, and no access to other features.

You can also specify which access mechanisms (Gaia Portal, or Gaia Clish) are available to the user.

**Note** - When users log in to the Gaia Portal, they see only those features to which they have read-only or read/write access. If they have read-only access to a feature, they can see the settings pages, but cannot change the settings.

Gaia includes these predefined roles:

| Role | Description |
|---|---|
| **adminRole** | Gives the user read/write access to all features. |
| **monitorRole** | Gives the user read-only access to all features. |

**Notes:**

- You **cannot** delete or change the predefined roles.
- Do **not** define a new user for external users.
  An external user is one that is defined on an authentication server (such as RADIUS or TACACS), and not on the local Gaia system.

# Configuring Roles in Gaia Portal

You define roles on the **User Management** > **Roles** page of the Gaia Portal.

This page also shows a list of existing roles.

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Adding a new role

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **Roles**. |
| 2 | Click **Add**. |
| 3 | In the **Role Name** field, enter the applicable name.<br>The role name must start with a letter and can be a combination of letters, numbers and the underscore (_) character. |
| 4 | On the **Features** tab:<br>In the **R/W** column, click the **?** icon near the feature you wish to configure in this role and select the permission: **None**, **Read Only**, or **Read / Write**.<br>**Important** - A user with **Read/Write** permission to the **User Management** feature can change a user password, including that of the **admin** user. Be careful when assigning roles that include this permission!<br>See *"List of Available Features in Roles" on page 490*. |
| 5 | On the **Extended Commands** tab:<br>Select the commands you wish to configure in this role.<br>■ To select several commands:<br>a. Press and hold the **CTRL** key on the keyboard.<br>b. Left-click the applicable commands (in the **Name**, **Description**, or **Path** column).<br>The selected commands become highlighted.<br>c. In the top right corner, select the option **Check selected as**.<br>The checkboxes of the selected commands become checked.<br>■ To clear several selected commands:<br>a. Press and hold the **CTRL** key on the keyboard.<br>b. Left-click the applicable commands (in the **Name**, **Description**, or **Path** column).<br>The selected commands become highlighted.<br>c. In the top right corner, clear the option **Check selected as**.<br>The checkboxes of the selected commands become cleared.<br>See *"List of Available Extended Commands in Roles" on page 511*. |

| Step | Instructions |
|---|---|
| 6 | Click **OK**. |

**Changing features and commands in the existing role**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **Roles**. |
| 2 | Select the role. |
| 3 | Click **Edit**. |
| 4 | On the **Features** tab:<br>In the **R/W** column, click the **?** icon near the feature you wish to configure in this role and select the permission: **None**, **Read Only**, or **Read / Write**.<br>**Important** - A user with **Read/Write** permission to the **User Management** feature can change a user password, including that of the **admin** user. Be careful when assigning roles that include this permission! |
| 5 | On the **Extended Commands** tab:<br>Select the commands you wish to configure in this role.<br>■ To select several commands:<br>a. Press and hold the **CTRL** key on the keyboard.<br>b. Left-click the applicable commands (in the **Name**, **Description**, or **Path** column).<br>The selected commands become highlighted.<br>c. In the top right corner, select the option **Check selected as**.<br>The checkboxes of the selected commands become checked.<br>■ To clear several selected commands:<br>a. Press and hold the **CTRL** key on the keyboard.<br>b. Left-click the applicable commands (in the **Name**, **Description**, or **Path** column).<br>The selected commands become highlighted.<br>c. In the top right corner, clear the option **Check selected as**.<br>The checkboxes of the selected commands become cleared. |
| 6 | Click **OK**. |

### Deleting a role

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **Roles**. |
| 2 | Select the role. |
| 3 | Click **Delete**. |
| 4 | Click **OK** to confirm. |

**Note** - You cannot delete the default roles **adminRole** and **monitorRole**.

### Assigning users to a role

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **Roles**. |
| 2 | Select the role. |
| 3 | Click **Assign Members**. |
| 4 | In the **Available Users** list, left-click the user you wish to add to the role.<br>To select several users:<br>a. Press and hold the **CTRL** key on the keyboard.<br>b. Left-click the applicable commands. The selected users become highlighted. |
| 5 | Click **Add >**.<br>The selected users move to the **Users with Role** list. |
| 6 | Click **OK**. |

### Removing users from a role

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **Roles**. |
| 2 | Select the role. |
| 3 | Click **Assign Members**. |
| 4 | In the **Users with Role** list, left-click the user you wish to remove from the role.<br>To select several users:<br>a. Press and hold the **CTRL** key on the keyboard.<br>b. Left-click the applicable commands. The selected users become highlighted. |
| 5 | Click **Remove >**.<br>The selected users move to the **Available Users** list. |
| 6 | Click **OK**. |

**Note** - You can assign a user to many roles on the **Users** page (see *"Users" on page 469*).

# Configuring Roles in Gaia Clish

You can:

- Add, change, or delete roles.
- Add or remove users to or from existing roles.
- Add or remove access mechanism permissions for a specified user.

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

## Syntax

### Adding an RBA role

```
add rba role <New Role Name> domain-type System
      all-features
      readonly-features <List of RO Features>
      readwrite-features <List of RW Features>}
```

**Note** - You can add "`readonly-features`" and "`readwrite-features`" in the same command.

### Choosing which VSX Virtual Systems this role can access

```
add rba role <Existing Role Name>
      virtual-system-access 0
      virtual-system-access all
      virtual-system-access VSID1,VSID2,...,VSIDn
```

### Assigning Gaia access mechanisms to a user

```
add rba user <User Name>
      access-mechanisms Web-UI
      access-mechanisms CLI
      access-mechanisms Web-UI,CLI
      access-mechanisms Gaia-API
```

### Assigning an RBA role to a user

```
add rba user <User Name> roles <Role1,Role2,...,RoleN>
```

### Viewing the RBA roles information

```
show rba
      all
      role <Role Name>
      roles
      user <User Name>
      users
```

### Deleting an entire RBA role

```
delete rba role <Role Name>
```

### Deleting features from an RBA role

```
delete rba role <Role Name>
      readonly-features <List of RO Features>
      readwrite-features <List of RW Features>
```

**Note** - You can delete "`readonly-features`" and "`readwrite-features`" in the same command.

### Removing Gaia access mechanisms from a user

```
delete rba user <User Name>
      access-mechanisms Web-UI
      access-mechanisms CLI
      access-mechanisms Web-UI,CLI
      access-mechanisms Gaia-API
```

### Removing an RBA role from a user

```
delete rba user <User Name> roles <Role1,Role2,...,RoleN>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

**Notes:**

- There are no "`set`" commands for configured roles.
- You cannot delete the default roles **adminRole** or **monitorRole**.

### Parameters

#### CLI Parameters

| Parameter | Description |
|---|---|
| `role <Role Name>` | Role name as a character string that contains letters, numbers or the underscore (_) character.<br>The role name must start with a letter. |
| `domain-type System` | Reserved for future use. |
| `virtual-system-access {0 \| all \| VSID1, VSID2, ..., VSIDn}` | Specifies which VSX Virtual Systems this role can access:<br>■ `0` - Access only to VSX Gateway (VSX Cluster Member) itself (context of VS0).<br>■ `all` - Access to all Virtual Systems.<br>■ *`VSID1,VSID2,...,VSIDn`* - Access only to specified Virtual Systems. This is a comma-separated list of Virtual Systems IDs (spaces are **not** allowed in this syntax). |
| `all-features` | Grants read-write permissions to all features.<br>**Important** - This is equivalent to the **admin** role! |
| `readonly-features <List of RO Features>` | A comma-separated list of Gaia features that have read-only permissions in the specified role.<br>See:<br>■ *"List of Available Features in Roles" on page 490*<br>■ *"List of Available Extended Commands in Roles" on page 511*<br>**Notes:**<br>■ Press <SPACE><TAB> to see the list of available features.<br>■ You can add read-only and read-write feature lists in the same "`add rba role <Role Name> domain-type System ...`" command. |

| Parameter | Description |
|---|---|
| `readwrite-features <List of RW Features>` | A comma-separated list of Gaia features that have read-write permissions in the specified role.<br>See:<br>■ *"List of Available Features in Roles" on page 490*<br>■ *"List of Available Extended Commands in Roles" on page 511*<br>**Notes:**<br>■ Press <SPACE><TAB> to see the list of available features.<br>■ You can add read-only and read-write feature lists in the same "`add rba role <Role Name> domain-type System ...`" command.<br>**Important** - A user with read/write permission to the **user** feature can change a user password, including that of the **admin** user. Be careful when assigning roles that include this permission! |
| `user <User Name>` | User, to which access mechanism permissions and roles are assigned.* |
| `roles <Role1,Role2,...,RoleN>` | Comma-separated list of role names that are assigned to or removed from the specified user (spaces are **not** allowed in this syntax).* |
| `access-mechanisms {Web-UI \| CLI \| Web-UI,CLI \| Gaia-API}` | Defines the access mechanisms that users can work with to manage Gaia:*<br>■ `Web-UI` - Access only to Gaia Portal<br>■ `CLI` - Access only to Gaia Clish<br>■ `Web-UI,CLI` - Access to both Gaia Portal and Gaia Clish (spaces are not allowed in this syntax)<br>■ `Gaia-API` - Access only to Gaia RESTful API (see *Check Point Gaia API Reference*) |

* To configure these settings in Gaia Portal, see *"Managing User Accounts in Gaia Portal" on page 471*.

### Example

```
gaia> add rba role NewRole domain-type System readonly-features vpn,ospf,rba readwrite-
features snmp

gaia> show rba role NewRole
Role
    NewRole
    domain-type System
    read-write-feature snmp
    read-only-feature vpn,ospf,rba
gaia>

gaia> add rba user John roles NewRole

gaia> add rba user John access-mechanisms Web-UI,CLI

gaia> show rba user John
User
    John
    access-mechanism CLI
    access-mechanism Web-UI
    role NewRole
gaia>

gaia> delete rba user John roles NewRole

gaia> delete rba role NewRole
```

# List of Available Features in Roles

**Important:**

- Read the Known Limitations for R82 in sk181128.
- Read the Known Limitations for Scalable Platforms in sk181128.

Table: List of Available Features in Roles

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| Authentication Servers | `aaa-servers` | Configure authentication through external RADIUS or TACACS+ server. | `set aaa radius-servers *`<br>`set aaa tacacs-servers *`<br>`delete aaa radius-servers *`<br>`delete aaa tacacs-servers *`<br>`add aaa radius-servers *`<br>`add aaa tacacs-servers *`<br>`show aaa radius-servers *`<br>`show aaa tacacs-servers *` |
| Advanced VRRP | `adv-vrrp` | Configure the Advanced Virtual Router Redundancy Protocol (VRRP) | `set vrrp *`<br>`show vrrp *` |
| Appliance Maintenance | `prod-maintain` | Overview page for Appliance Maintenance. | |
| ARP | `arp` | Control static ARP entries and proxy ARP entries. Control dynamic ARP entries. | `add arp *`<br>`delete arp *`<br>`set arp *`<br>`show arp *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| Banner Messages | `message` | Control Banner Message and Message of the Day. | `set message *`<br>`delete message *`<br>`show message *` |
| BGP | `bgp` | Configure dynamic routing through the Border Gateway Protocol (BGP). | `set as *`<br>`set router-id *`<br>`set bgp *`<br>`show route bgp *`<br>`show as *`<br>`show router-id *`<br>`show bgp *` |
| Blades Summary | `blades` | Show summary for enabled Software Blades. | |
| cdt | `cdt` | Central Deployment Tool | `show cdt *`<br>`set cdt *`<br>`start cdt *` |
| Certificate Authority | `certificate_ authority` | Control Certificate Authority. | `cpca_client` |
| Change My Password | `selfpasswd` | Change your user account password. | `set selfpasswd *` |
| Cloning Group | `CloningGroup` | Control Gaia Cloning Groups. | `set cloning-group *`<br>`add cloning-group *`<br>`delete cloning-group *`<br>`join cloning-group *`<br>`re-synch cloning-group *`<br>`leave cloning-group *`<br>`show cloning-group *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| Cloning Group Management | `CloningGroupManagement` | Control management of Gaia Cloning Groups. | `set cloning-group-management *` |
| Cloud Config | `cloud-config` | Control of Zero Touch. | `show cloud-config *`<br>`set cloud-config *`<br>`delete cloud-config *` |
| Cluster | `cluster` | Control clustering. | `add cluster *`<br>`set cluster *`<br>`delete cluster *`<br>`show cluster *` |
| Core Dump | `core-dump` | Control core dumps. | `set core-dump *`<br>`show core-dump *` |
| DHCP Relay | `bootp` | Control Relay of IPv4 DHCP and IPv4 BOOTP messages between DHCP clients and DHCP servers on different IPv4 Network. | `set bootp *`<br>`show bootp *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| DHCP Server | `dhcp` | Control DHCP Server on Gaia. | `set dhcp service *`<br>`delete dhcp service *`<br>`set dhcp client *`<br>`delete dhcp client *`<br>`add dhcp client *`<br>`set dhcp server *`<br>`delete dhcp server *`<br>`add dhcp server *`<br>`show dhcp service *`<br>`show dhcp client *`<br>`show dhcp server *` |
| DHCPv6 Relay | `dhcp6relay` | Control Relay of DHCPv6 messages between DHCP clients and DHCP servers on different IPv6 Network. | `set ipv6 dhcp6relay *`<br>`show ipv6 dhcp6relay *` |
| Display Configuration | `configuration` | Save and show Gaia configuration. | `save configuration *`<br>`show configuration *` |
| Display Format | `format` | Control how the system displays time, date and netmask. | `set format *`<br>`show format *` |
| DNS | `dns` | Control DNS servers on Gaia. | `set dns *`<br>`delete dns *`<br>`show dns *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| Domain Name | `domainname` | Control the domain name on Gaia. | `set domainname *`<br>`delete domainname`<br>`show domainname` |
| Download SmartConsole | `smart-console` | Download SmartConsole from Gaia Portal. | N / A |
| Expert Mode | `expert` | Access to the Expert mode shell. | `expert` |
| Expert Password | `expert-password` | Change the Expert mode password (interactive). | `set expert-password` |
| Expert Password Hash | `expert-password-hash` | Change the Expert mode password using password hash. | `set expert-password-hash *` |
| Extended Commands | `command` | Control the ability to define additional Extended Commands for the Gaia Clish. | `add command *`<br>`delete command *`<br>`show command *`<br>`show commands`<br>`show extended *` |
| Factory Defaults | `fcd` | Restore Gaia OS to Factory Defaults. | `set fcd *`<br>`show fcd *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| Firewall Management | `firewall_ management` | Control Login and Logout from Management Server. | `mgmt *` |
| Front Panel | `lcd` | Control the front panel LCD display available on some Check Point appliances. | `set lcd *`<br>`show lcd *` |
| Hardware Health | `hw-monitor` | Hardware sensor monitoring. | `show sysenv all`<br>`cpstat -f sensors os` |
| High Availability | `high-avail-group` | Overview page for High Availability. | |
| Host Access | `host-access` | Control which hosts are allowed to connect to Gaia. | `add allowed-client *`<br>`delete allowed-client *`<br>`show allowed-client *` |
| Host Address | `host` | Control known hosts and their IP addresses on Gaia. | `add host *`<br>`set host *`<br>`delete host *`<br>`show host *` |
| Host Name | `hostname` | Control the Gaia hostname. | `set hostname *`<br>`show hostname *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| IGMP | `igmp` | Control multicast group memberships through the Internet Group Management Protocol (IGMP). | `set igmp *`<br>`show igmp *` |
| Inactivity timeout | `inactto` | Control inactivity timeout for Gaia Portal and Gaia Clish. | `set inactivity-timeout *`<br>`show inactivity-timeout *` |
| Inbound Route Filters | `import` | Configure IPv4 Inbound Route Filters for RIP, OSPFv2, and BGP IPv4. | `set inbound-route-filter *` |
| Inbound Route Filters | `import6` | Configure IPv6 Inbound Route Filters for RIPng, OSPFv3, and BGP IPv6. | `set ipv6 inbound-route-filter *` |
| Installation | `ftw` | Run the Gaia First Time Configuration Wizard. | |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| Interface Naming | `interface-name` | Set a different name for an existing interface (requires a reboot and reconfiguration of the interface) | `set interface-name *` |
| IP Broadcast Helper | `iphelper` | Control forwarding of UDP broadcast traffic to other interfaces. | `set iphelper *`<br>`show iphelper *` |
| IP Reachability Detection | `ipreachdetect` | Control reachability of IP Addresses. | `set ip-reachability-detection *`<br>`show ip-reachability-detection *` |
| IPv4 Static Routes | `static-route` | Configure IPv4 static routes on Gaia. | `set static-route *`<br>`show route static *` |
| IPv6 Router Discovery | `ipv6rdisc6` | Control IPv6 router discovery. | `set ipv6 rdisc6 *`<br>`show ipv6 rdisc6 *` |
| IPv6 State | `ipv6-state` | Control IPv6 stack on Gaia. | `set ipv6-state *`<br>`show ipv6-state` |
| IPv6 Static Routes | `static6` | Control IPv6 static routes on Gaia. | `set ipv6 static-route *`<br>`show ipv6 route static *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| IPv6 VRRP | `vrrp6` | Control the IPv6 Virtual Router Redundancy Protocol (VRRPv3). | `set ipv6 vrrp6 *`<br>`show ipv6 vrrp6 *` |
| Job Scheduler | `cron` | Control scheduled automated tasks that perform actions at a specific time. | `add cron *`<br>`set cron *`<br>`delete cron *`<br>`show cron *` |
| License Activation | `license_ activation` | Access to "Activate Licenses". | `cplic` |
| License Configuration | `license` | Access to "Manage License". | `cplic` |
| Lights Out Management (LOM) Configuration | `lom` | Show Lights Out Management (LOM) Configuration. | `show lom *` |
| Mail Notification | `ssmtp` | Control mail notifications sent by Gaia. | `set mail-notification *`<br>`show mail-notification *` |
| Maintenance | `maintenance-group` | Overview page for Maintenance. | N / A |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| Management Interface | `management_interface` | Control which interface is used for management (main interface). | `set management *`<br>`show management *` |
| NDP | `neighbor` | Control IPv6 Neighbor Discovery Protocol. | `add neighbor-entry *`<br>`set neighbor *`<br>`delete neighbor-entry *`<br>`show neighbor *` |
| NetFlow Export | `netflow` | Control NetFlow Export on Gaia. | `add netflow *`<br>`set netflow *`<br>`delete netflow *`<br>`show netflow *` |
| Network Access | `netaccess` | Control TELNET access to Gaia. | `set net-access *`<br>`show net-access *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| Network Interfaces | `interface` | Control Physical interfaces, Aliases, Bridges, Bonds, VLANs, PPPoE. | `set interface *`<br>`add interface *`<br>`delete interface *`<br>`add bonding *`<br>`set bonding *`<br>`delete bonding *`<br>`add bridging *`<br>`set bridging *`<br>`delete bridging *`<br>`add pppoe *`<br>`delete pppoe *`<br>`set pppoe *`<br>`add gre *`<br>`delete gre *`<br>`show interface *`<br>`show interfaces`<br>`show bonding *`<br>`show bridging *`<br>`show pppoe *`<br>`show gre *` |
| Network Management | `interface-group` | Overview page for Network Management. | `show interface *`<br>`show interfaces *`<br>`set interface *` |
| NTP | `ntp` | Control Network Time Protocol for synchronizing the Gaia clock. | `add ntp *`<br>`set ntp *`<br>`delete ntp *`<br>`show ntp *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| OSPF | `ospf` | Control IPv4 dynamic routing through the Open Shortest-Path First protocol (OSPFv2). | `set ospf *`<br>`show ospf *`<br>`show route ospf *` |
| OSPF v3 | `ospf3` | Control IPv6 dynamic routing through the Open Shortest-Path First protocol v3 (OSPFv3). | `set ipv6 ospf3 *`<br>`set router-id *`<br>`show ipv6 ospf3 *`<br>`show ipv6 route ospf3 *`<br>`show router-id *` |
| Password Policy | `password-controls` | Control password and account policies on Gaia. | `set password-controls *`<br>`show password-controls *` |
| Performance Optimization | `perf` | Control Multi-Queue on Security Gateway. | `set multi-queue *`<br>`show multi-queue *` |
| PIM | `pim` | Control Protocol-Independent Multicast (PIM). | `set pim *`<br>`show pim *`<br>`show mfc *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| Policy Based Routing | `pbr-combine-static` | Control policy based routing rules and action tables. | `set pbr *`<br>`set pbrroute *`<br>`show pbr *`<br>`show pbrroute *` |
| Policy Routing | `pbr-routing-group` | Overview page for Policy Based Routing. | `set pbr *`<br>`set pbrroute *`<br>`show pbr *`<br>`show pbrroute *` |
| Prefix Lists and Prefix Trees | `prefix` | Control Prefix Lists and Prefix Trees used in routing policy. | `set prefix-tree *`<br>`set prefix-list *` |
| Proxy Settings | `proxy` | Control Proxy server on Gaia. | `set proxy *`<br>`delete proxy *`<br>`show proxy *` |
| RAID Monitoring | `raid-monitor` | Overview page for RAID volumes monitoring. | `raidconfig`<br>`raid_diagnostic` |
| RIP | `rip` | Control dynamic routing through the Routing Information Protocol for IPv4 (RIP). | `set rip *`<br>`show rip *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| RIPng | `ripng` | Control dynamic routing through the Routing Information Protocol for IPv6 (RIPng). | `set ipv6 ripng *`<br>`show ipv6 ripng *` |
| Roles | `rba` | Control user roles on Gaia. | `add rba *`<br>`delete rba *`<br>`show rba *` |
| Route | `route` | Show IPv4 and IPv6 routing table on Gaia. | `show route *`<br>`show ipv6 route *` |
| Route Aggregation | `aggregate` | Create a supernet network from the combination of networks with a common routing prefix. | `set aggregate *`<br>`show route aggregate *` |
| Route Injection Mechanism | `route-injection` | Control the Route Injection Mechanism (RIM) on Gaia. | `set kernel-routes *`<br>`show route kernel *` |
| Route Map | `routemap` | Configure route maps on Gaia. | `set routemap *`<br>`show routemap *`<br>`show routemaps *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| Route Redistribution | `export` | Control advertisement of IPv4 routing information from one protocol to another. | `set route-redistribution *` |
| Route Redistribution | `export6` | Control advertisement of IPv6 routing information from one protocol to another. | `set ipv6 route-redistribution *` |
| Routed ClusterXL | `routed-cluster` | Control how RouteD daemon interacts with ClusterXL on Gaia. | `set routed-clusterxl *`<br>`show routed-clusterxl *` |
| Router Discovery | `rdisc` | Control ICMP Router Discovery on Gaia. | `set rdisc *`<br>`show rdisc *` |
| Router Service | `router-service-group` | Overview page for Routing Services. | |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| Routing Monitor | `show-route-all` | View summary information about routes on Gaia. | `show route *` |
| Routing Options | `route-options` | Configure protocol ranks and trace (debug) options on Gaia. | `set routedsyslog *`<br>`set trace *`<br>`set tracefile *`<br>`set max-path-splits *`<br>`set nexthop-selection *`<br>`set protocol-rank *`<br>`set router-options *`<br>`show trace *`<br>`show routed *`<br>`show protocol-rank *`<br>`show router-options *` |
| SAM (Accelerator Card) | `sam` | Deprecated - SAM card is not supported. Monitor Security Acceleration Module for information on usage and connections. | `show sam *` |
| Scheduled Backup | `scheduled_backup` | Create scheduled backups of the Gaia for events of data loss. | `add backup-scheduled *`<br>`set backup-scheduled *`<br>`delete backup-scheduled *`<br>`show backup-scheduled` |
| Scratchpad Configuration | `scratchpad` | Control Scratchpad in Gaia Portal. | N / A |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| Security Management GUI Clients | `mgmt-gui-clients` | Control allowed Security Management GUI Clients. | |
| Shutdown | `reboot_halt` | Shut down and reboot the Gaia. | `halt *`<br>`reboot *` |
| Snapshot | `snapshot` | Create full backups (snapshots) of the Gaia. | `add snapshot *`<br>`set snapshot *`<br>`delete snapshot *`<br>`show snapshots`<br>`show snapshot *` |
| SNMP | `snmp` | Control Gaia monitoring through the Simple Network Management Protocol (SNMP). | `add snmp *`<br>`set snmp *`<br>`delete snmp *`<br>`show snmp *` |
| Software Updates Policy Management | `installer_conf` | CPUSE - Manage deployment policy and mail notifications for software updates. | For more information, see sk92449.<br>`installer restore_policy *`<br>`set installer *`<br>`set installer download_mode *`<br>`set installer install_mode *`<br>`set installer download_mode schedule *`<br>`set installer install_mode schedule *` |
| Static Multicast Routes | `static-mroute` | Configure multicast static routes on Gaia. | `set static-mroute *`<br>`show static-mroute *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| System Asset | `asset` | Show hardware asset summary. | `show asset *` |
| System Backup | `backup` | Create backup of the Gaia system for events of data loss. | `add backup *`<br>`set backup *`<br>`backup *`<br>`restore *`<br>`delete backup *`<br>`show backups`<br>`show backup *`<br>`show restore *` |
| System Configuration | `sysconfig` | System Configuration. | `show configuration *` |
| System Groups | `group` | Control Gaia OS user groups, for advanced management of privileges. | `add group *`<br>`set group *`<br>`delete group *`<br>`show groups`<br>`show group *` |
| System Logging | `syslog` | Control system logging on Gaia. | `add syslog *`<br>`set syslog *`<br>`delete syslog *`<br>`show syslog *` |
| System Management | `system-group` | Overview page for System Management. | |
| System Status | `sysenv` | Hardware sensor monitoring. | `show sysenv *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| TACACS_ Enable | `tacacs_enable` | Control TACACS+ mechanism on Gaia. | `tacacs_enable *`<br>`show tacacs_enable *` |
| Time | `clock-date` | Configure the time and date of the Gaia system. | `set clock *`<br>`set date *`<br>`set time *`<br>`set timezone *`<br>`show clock *`<br>`show date *`<br>`show time *`<br>`show timezone *` |
| Upgrade | `upgrade` | Upgrade the Gaia. Deprecated - use the CPUSE instead. | `upgrade *`<br>`add upgrade *`<br>`delete upgrade *`<br>`show upgrade *` |
| Upgrades (CPUSE) | `installer` | CPUSE - Show the update packages status and manage package downloads and installations on Gaia. | For more information, see sk92449.<br>`show installer *`<br>`add installer *`<br>`installer *`<br>`set installer *` |
| Upgrades (CPUSE) | `software-updates-group` | Overview page for CPUSE. | For more information, see sk92449.<br>`show installer *`<br>`set installer *`<br>`installer agent *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| User Management | `security-access-group` | Overview page for User Management. | |
| Users | `user` | Control user accounts on Gaia. | `add user *`<br>`set user *`<br>`delete user *`<br>`show user *`<br>`show users *` |
| Version | `version` | Shows the version of the installed Check Point product, and Gaia build and kernel. | `show version *` |
| Virtual-System | `virtual-system` | Control VSX Virtual Systems (CLI only). You must configure all Virtual Systems in SmartConsole only. | `add virtual-system *`<br>`set virtual-system *`<br>`delete virtual-system *`<br>`show virtual-system *` |
| VPNT | `vpnt` | Control VPN Tunneling on Gaia. | `add vpn *`<br>`set vpn *`<br>`delete vpn *` |

Table: List of Available Features in Roles (continued)

| Feature name in Gaia Portal | Feature name in Gaia Clish | Description | Affected commands in Gaia Clish |
|---|---|---|---|
| VRRP | `vrrp` | Control the IPv4 Virtual Router Redundancy Protocol (VRRPv2) - Monitored Circuit/Simplified VRRP. | `set vrrp *`<br>`add mcvr *`<br>`set mcvr *`<br>`delete mcvr *`<br>`show vrrp *`<br>`show mcvr *` |
| VSX | `vsx` | Enable or Disable the VSX mode (to be used only by Check Point Support only). | `set vsx *`<br>`show vsx *` |
| Web configuration | `web` | Control Gaia Portal. | `set web *`<br>`generate web *`<br>`show web *` |

# List of Available Extended Commands in Roles

**Important:**

- Read the Known Limitations for R82 in sk181128.
- Read the Known Limitations for Scalable Platforms in sk181128.

| Command name in Gaia Portal | Command name in Gaia Clish / Gaia gClish | Description |
|---|---|---|
| api | ext_api | Starts, stops, or checks the status of the API server |
| config_system | ext_config_system | Runs the Gaia First Time Configuration tool in Expert mode. |
| cp_conf | ext_cp_conf | Runs the Check Point configuration utility for some local settings. |
| cpca | ext_cpca | Runs the Check Point Internal Certificate Authority (ICA). |
| cpca_client | ext_cpca_client | Controls the Check Point Internal Certificate Authority (ICA). |
| cpca_create | ext_cpca_create | Creates the Check Point Internal Certificate Authority (ICA) database. |
| cpca_dbutil | ext_cpca_dbutil | Controls the Check Point Internal Certificate Authority (ICA) database. |
| cpconfig | ext_cpconfig | Runs the Check Point Configuration Tool for Security Management Server and Security Gateway. |
| cphaprob | ext_cphaprob | Access to clustering commands. |
| cphastart | ext_cphastart | Enables the clustering feature on Security Gateway. |
| cphastop | ext_cphastop | Disables the clustering feature on Security Gateway. |
| cpinfo | ext_cpinfo | Collects the Check Point diagnostics information. |
| cplic | ext_cplic | Controls the Check Point licenses. |

| Command name in Gaia Portal | Command name in Gaia Clish / Gaia gClish | Description |
|---|---|---|
| cpshared_ver | ext_cpshared_ver | Shows the Check Point SVN Foundation version. |
| cpstart | ext_cpstart | Starts the installed Check Point products. |
| cpstat | ext_cpstat | Shows the Check Point statistics history information for Software Blades and Gaia. |
| cpstop | ext_cpstop | Stops the installed Check Point products. |
| cpview | ext_cpview | Shows the advanced Check Point statistics information for Software Blades and Gaia in real-time. |
| cpwd_admin | ext_cpwd_admin | Controls the Check Point WatchDog administration tool. |
| diag | ext_diag | Sends the system diagnostics information. |
| dtps | ext_dtps | Controls the Endpoint Policy Server commands. |
| etmstart | ext_etmstart | Starts the QoS Software Blade. |
| etmstop | ext_etmstop | Stops the QoS Software Blade. |
| fgate | ext_fgate | Controls the QoS Software Blade. |
| fips | ext_fips | Controls the FIPS mode. |
| fw | ext_fw | Access to Security Gateway commands for IPv4. |
| fw6 | ext_fw6 | Access to Security Gateway commands for IPv6. |
| fwaccel | ext_fwaccel | Access to SecureXL commands for IPv4. |
| fwaccel6 | ext_fwaccel6 | Access to SecureXL commands for IPv6. |
| fwm | ext_fwm | Access to Security Management commands. |
| ifconfig | ext_ifconfig | Deprecated. Use "show interface", or "set interface" commands instead. |

| Command name in Gaia Portal | Command name in Gaia Clish / Gaia gClish | Description |
|---|---|---|
| ips | ext_ips | Controls the IPS Software Blade. |
| lomipset | ext_lomipset | Configures the LOM Card IP address. |
| LSMcli | ext_LSMcli | Access to SmartProvisioning command line. |
| LSMenabler | ext_LSMenabler | Enables the SmartProvisioning. |
| mds_backup | ext_mds_backup | Creates backup of the Multi-Domain Server. |
| mds_restore | ext_mds_restore | Restores the backup of the Multi-Domain Server. |
| mdscmd | ext_mdscmd | Access to Multi-Domain Server command line. |
| mdsconfig | ext_mdsconfig | Runs the Check Point Configuration Tool for Multi-Domain Server. |
| mdsstart | ext_mdsstart | Starts the Multi-Domain Server. |
| mdsstart_ customer | ext_mdsstart_ customer | Starts a specific Domain Management Server. |
| mdsstat | ext_mdsstat | Shows the status of the Multi-Domain Server and all Domain Management Servers. |
| mdsstop | ext_mdsstop | Stops the Multi-Domain Server. |
| mdsstop_ customer | ext_mdsstop_ customer | Stops a specific Domain Management Server. |
| netstat | ext_netstat | Shows network connections, routing tables, and interface statistics. |
| ping | ext_ping | Sends pings to a host using IPv4. |
| ping6 | ext_ping6 | Sends pings to a host using IPv6. |
| raid_diagnostic | ext_raid_ diagnostic | Access to RAID Monitoring tool. |

| Command name in Gaia Portal | Command name in Gaia Clish / Gaia gClish | Description |
|---|---|---|
| raidconfig | ext_raidconfig | Access to RAID Configuration and Monitoring tool. |
| rtm | ext_rtm | Controls the Monitoring Software Blade. |
| rtmstart | ext_rtmstart | Starts the Monitoring Software Blade. |
| rtmstop | ext_rtmstop | Stops the Monitoring Software Blade. |
| rtmtopsvc | ext_rtmtopsvc | Monitors top services using the Monitoring Software Blade. |
| SDSUtil | ext_SDSUtil | Access to Software Distribution Server utility. |
| sim | ext_sim | Access to SecureXL SIM device commands for IPv4. |
| SnortConvertor | ext_ SnortConvertor | Access to the IPS Snort conversion tool. |
| tecli | ext_tecli | Access to the Threat Emulation Software Blade shell. |
| top | ext_top | Shows the most active system processes. |
| traceroute | ext_traceroute | Runs the trace tool. |
| vpn | ext_vpn | Controls the VPN kernel module for IPv4. |
| vpn6 | ext_vpn6 | Controls the VPN kernel module for IPv6. |
| vsx_util | ext_vsx_util | Controls the managed VSX Gateways and VSX Clusters on a Management Server. |

# Password Policy

This section explains how to configure your platform:

- To enforce creation of strong passwords.
- To monitor and prevent use of already used passwords.
- To force users to change passwords at regular intervals.

One of the important elements of securing your Check Point cyber security platform is to set user passwords and create a good *password policy*.

**Note** - The password policy does not apply to non-local users that authentication servers such as RADIUS manage their login information and passwords. In addition, it does not apply to non-password authentication, such as the public key authentication supported by SSH.

To set and change user passwords, see *"Users" on page 469* and *"User Management" on page 442*.

### Password Strength

Strong, unique passwords that use a variety of character types and require password changes, are key factors in your overall cyber security.

### Password History Checks

The *password history* feature prevents users from using a password they have used before when they change their password.

The number of already used passwords that this feature checks against is defined by the *history length*.

Password history check is enabled by default.

The password history check:

- Applies to user passwords set by the administrator and to passwords set by the user.
- Does not apply to SNMPv3 USM user pass phrases.

These are some considerations when using password history:

- The password history for a user is updated only when the user successfully changes password.

  If you change the history length, for example: from ten to five, the stored passwords number does not change.

  Next time the user changes password, the new password is examined against all stored passwords, maybe more than five.

  After the password change succeeds, the password file is updated to keep only the five most recent passwords.
- The password history is only stored if the password history feature is enabled when the password is created.
- The new password is checked against the previous password, even if the previous password is not stored in the password history.

### Mandatory Password Change

The *mandatory password change* feature requires users to use a new password at defined intervals.

Forcing users to change passwords regularly is important for a strong security policy.

You can set user passwords to expire after a specified number of days.

When a password expires, the user is forced to change the password the next time the user logs in.

This feature works together with the password history check to get users to use new passwords at regular intervals.

The mandatory password change feature does not apply to SNMPv3 USM user pass phrases.

### Denying Access to Unused Accounts

You can deny access to unused accounts. If there were no successful login attempts within a set time, the user is locked out and cannot log in.

You can also configure the allowed number of days of non-use before a user is locked-out.

### Denying Access After Failed Login Attempts

You can deny access after too many failed login attempts. The user cannot log in during a configurable time.

You can also allow access again after a user was locked out.

In addition, you can configure the number of failed login attempts that a user is allowed before being locked out.

When one login attempt succeeds, counting of failed attempts stops, and the count is reset to zero.

# Configuring Password Policy in Gaia Portal

*In This Section:*



## Procedure

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **Password Policy**. |
| 2 | Configure the password policy options:<br>■ **Password Strength** (see *"Password Strength" on the next page*)<br>■ **Password History** (see *"Password History" on page 520*)<br>■ **Mandatory Password Change** (see *"Mandatory Password Change" on page 521*)<br>■ **Deny Access to Unused Accounts** (see *"Denying Access to Unused Accounts" on page 522*)<br>■ **Deny Access After Failed Login Attempts** (see *"Denying Access After Failed Login Attempts" on page 523*)<br>■ **Password hashing algorithm** (see *"Password Hashing Algorithm" on page 524*) |
| 3 | Click **Apply**. |

## Password Strength

| Parameter | Description |
|---|---|
| **Minimum Password Length** | The minimum number of characters in a Gaia user, or an SNMP user password.<br>Does not apply to passwords that were already configured.<br>■ **Range**: 6 - 128<br>■ **Default**: 6 |
| **Disallow Palindromes** | A palindrome is a sequence of letters, numbers, or characters that can be read the same in each direction.<br>■ **Default**: Selected |
| **Password Complexity** | The required number of character types:<br>■ `1` - Don't check<br>■ `2` - Require two character types (default)<br>■ `3` - Require three character types<br>■ `4` - Require four character types<br>Character types are:<br>■ Upper case alphabetic (A-Z)<br>■ Lower case alphabetic (a-z)<br>■ Digits (0-9)<br>■ Other (everything else)<br>Changes to this setting do not affect existing passwords. |

## Password History

| Parameter | Description |
|---|---|
| **Check for Password Reuse** | Check for reuse of passwords for all users.<br>Enables or disables password history checking and password history recording.<br>When a user's password is changed, the new password is checked against the recent passwords for the user.<br>An identical password is not allowed. The number of passwords kept in the record is set by **History Length**.<br>Does not apply to SNMP passwords.<br>■ **Default:** Selected |
| **History Length** | The number of former passwords to keep and check against when a new password is configured for a user.<br>■ **Range**: 1 - 1000<br>■ **Default**: 10 |

## Mandatory Password Change

| Parameter | Description |
|---|---|
| **Password Expiration** | The number of days, for which a password is valid. After that time, the password expires.<br>The count starts when the user changes the password.<br>Users are required to change an expired password the next time they log in.<br>Does not apply to SNMP users.<br>■ **Range**: `1 - 1827`, or `Passwords never expires`<br>■ **Default**: `Passwords never expires` |
| **Warn users before password expiration** | How many days before the user's password expires to start generating warnings to the user that user must change the password.<br>A user that does not log in, does not see this warning.<br>■ **Range**: 1 - 366<br>■ **Default**: 7 |
| **Lockout users after password expiration** | Lockout users after password expiration.<br>After a user's password has expired, user has this number of days to log in and change it.<br>If a user does not change the password within that number of days, the user is unable to log in - the user is locked out.<br>The administrator can unlock a user that is locked out from the **User Management** > **Users** page.<br>■ **Range**: `1 - 1827`, or `Never lockout users after password expires`<br>■ **Default**: `Never lockout users after password expires` |
| **Force users to change password at first login after password was changed from Users page** | Forces a user to change password at first login, after the user's password was changed using the command "`set user <UserName> password`", or from the Gaia Portal **User Management** > **Users** page.<br>■ **Default**: Not selected |

## Denying Access to Unused Accounts

| Parameter | Description |
|---|---|
| **Deny access to unused accounts** | Denies access to unused accounts.<br>If there were no successful login attempts within a set time, the user is locked out and cannot log in.<br>■ **Default**: Not selected |
| **Days of non-use before lock-out** | Configures the number of days of non-use before locking out the unused account.<br>This only takes effect, if **Deny access to unused accounts** is enabled.<br>■ **Range**: 30 - 1827<br>■ **Default**: 365 |

## Denying Access After Failed Login Attempts

| Parameter | Description |
|---|---|
| **Deny access after failed login attempts** | If the configured limit is reached, the user is locked out (unable to log in) for a configured time.<br>**Warning** - Enabling this leaves you open to a "denial of service" - if an attacker makes unsuccessful login attempts often enough, the affected user account is locked out. Consider the advantages and disadvantages of this option, in light of your security policy, before enabling it.<br>■ **Default**: Not selected |
| **Block admin user** | This option is available only if **Deny access after failed login attempts** is enabled.<br>If the configured limit of failed login attempts for the `admin` user is reached, the `admin` user is locked out (unable to log in) for a configured time. |
| **Maximum number of failed attempts allowed** | This only takes effect if **Deny access after failed attempts** is enabled.<br>The number of failed login attempts that a user is allowed before being locked out.<br>After making that many successive failed attempts, future attempts fail.<br>When one login attempt succeeds, counting of failed attempts stops, and the count is reset to zero.<br>■ **Range**: 2 - 1000<br>■ **Default**: 10 |

| Parameter | Description |
|---|---|
| **Allow access again after time** | This only takes effect, if **Deny access after failed login attempts** is enabled.<br>Allow access again after a user was locked out (due to failed login attempts).<br>The user is allowed access after the configured time, if there were no login attempts during that time.<br>■ **Range**: 60 - 604800 seconds<br>■ **Default**: 1200 seconds (20 minutes)<br>Examples:<br>■ 60 = 1 minute<br>■ 300 = 5 minutes<br>■ 3600 = 1 hour<br>■ 86400 = 1 day<br>■ 604800 = 1 week |

## Password Hashing Algorithm

| Parameter | Description |
|---|---|
| **Password hashing algorithm** | Configures the hashing algorithm to store new passwords in the Gaia database.<br>■ **Range**: `SHA256`, or `SHA512`<br>■ **Default**: `SHA512` |

# Configuring Password Policy in Gaia Clish

*In This Section:*



Use these commands to configure a policy for managing user passwords.

**Important:**

- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Password Strength

### Syntax

- To configure the password strength:

```
set password-controls
      complexity <1-4>
      min-password-length <6-128>
      palindrome-check {on |off}
```

- To show the configured password strength:

```
show password-controls
      complexity
      min-password-length
      palindrome-check
```

```
show password-controls all
```

**Parameters**

| Parameter | Description |
|---|---|
| `complexity <1-4>` | The required number of character types:<br>■ `1` - Don't check<br>■ `2` - Require two character types (default)<br>■ `3` - Require three character types<br>■ `4` - Require four character types<br>Character types are:<br>■ Upper case alphabetic (A-Z)<br>■ Lower case alphabetic (a-z)<br>■ Digits (0-9)<br>■ Other (everything else)<br>Changes to this setting do not affect existing passwords.<br>■ **Range**: 1 - 4<br>■ **Default**: 2 |
| `min-password-length <6-128>` | The minimum number of characters in a Gaia user, or an SNMP user password.<br>Does not apply to passwords that were already configured.<br>■ **Range**: 6 - 128<br>■ **Default**: 2 |
| `palindrome-check {on \| off}` | A palindrome is a sequence of letters, numbers, or characters that can be read the same in each direction.<br>■ **Range**: `on`, or `off`<br>■ **Default**: `on` |

## Password History

### Syntax

- To configure the password history:

```
set password-controls
      history-checking {on | off}
      history-length <1-1000>
```

- To show the configured password history:

```
show password-controls
      history-checking
      history-length
```

```
show password-controls all
```

### Parameters

| Parameter | Description |
|---|---|
| `history-checking {on \| off}` | Check for reuse of passwords for all users.<br>Enables or disables password history checking and password history recording.<br>When a user's password is changed, the new password is checked against the recent passwords for the user. An identical password is not allowed. The number of passwords kept in the record is set by `history-length`.<br>Does not apply to SNMP passwords.<br>■ **Range**: `on`, or `off`<br>■ **Default:** `on` |
| `history-length <1-1000>` | The number of former passwords to keep and check against when a new password is configured for a user.<br>■ **Range**: 1 - 1000<br>■ **Default**: 10 |

## Mandatory Password Change

### Syntax

- To configure the mandatory password change:

```
set password-controls
      expiration-lockout-days <1-1827 | never>
      expiration-warning-days <1-366>
      force-change-when {no | password}
      password-expiration <1-1827 | never>
```

- To show the configured mandatory password change:

```
show password-controls
      expiration-lockout-days
      expiration-warning-days
      force-change-when
      password-expiration
```

```
show password-controls all
```

### Parameters

| Parameter | Description |
|---|---|
| `expiration-lockout-days <1-1827 \| never>` | Lockout users after password expiration.<br>After a user's password has expired, user has this number of days to log in and change it.<br>If a user does not change the password within that number of days, the user is unable to log in - the user is locked out.<br>The administrator can unlock a user that is locked out from the **User Management** > **Users** page.<br>■ **Range**: `1 - 1827`, or `never`<br>■ **Default**: `never` |
| `expiration-warning-days <1-366>` | How many days before the user's password expires to start generating warnings to the user that user must change the password.<br>A user that does not log in, does not see this warning.<br>■ **Range**: 1 - 366<br>■ **Default**: 7 |

| Parameter | Description |
|---|---|
| `force-change-when {no \| password}` | Forces a user to change password at first login, after the user's password was changed using the command "`set user <UserName> password`", or from the Gaia Portal **User Management** > **Users** page.<br>■ **Range**:<br>• `no` - Disables this functionality.<br>• `password` - Forces users to change their password after their password was changed.<br>■ **Default**: `no` |
| `password-expiration <1-1827 \| never>` | The number of days, for which a password is valid. After that time, the password expires.<br>The count starts when the user changes the password.<br>Users are required to change an expired password the next time they log in.<br>Does not apply to SNMP users.<br>■ **Range**: `1-1827`, or `never`<br>■ **Default**: `never` |

**Note** - To see when Gaia OS changed the password for a specific user, run this command in the Expert mode:

```
date -d @"$(dbget passwd:<username>:lastchg)"
```

- The command "`dbget passwd:<username>:lastchg`" returns the time stamp in the Epoch format.
- The command "`date -d @<Epoch Time>`" converts it to the human-readable time stamp.

Example:

```
[Expert@MyGaia:0] date -d @"$(dbget
passwd:admin:lastchg)"
Mon May 24 15:39:46 UTC 2021
[Expert@MyGaia:0]
```

## Denying Access to Unused Accounts

### Syntax

- To configure the denial of access to unused accounts based on the number of days:

```
set password-controls deny-on-nonuse
      allowed-days <30-1827>
      enable {on | off}
```

- To show the configured denial of access to unused accounts:

```
show password-controls deny-on-nonuse
```

```
show password-controls all
```

### Parameters

| Parameter | Description |
|---|---|
| `deny-on-nonuse allowed-days <30-1827>` | Configures the number of days of non-use before locking out the unused account.<br>This only takes effect, if the "`set password-controls deny-on-nonuse enable`" is set to "`on`".<br>■ **Range**: 30 - 1827<br>■ **Default**: 365 |
| `deny-on-nonuse enable {on \| off}` | Denies access to unused accounts. If there were no successful login attempts within a set time, the user is locked out and cannot log in.<br>■ **Range**: `on`, or `off`<br>■ **Default**: `off` |

## Denying Access After Failed Login Attempts

### Syntax

- To configure the denial of access to unused accounts based on the number of failed login attempts:

```
set password-controls deny-on-fail
      allow-after <60-604800>
      block-admin {on | off}
      enable {on | off}
      failures-allowed <2-1000>
```

- To show the configured denial of access to unused accounts:

```
show password-controls deny-on-fail
```

```
show password-controls all
```

### Parameters

| Parameter | Description |
|---|---|
| `allow-after <60-604800>` | Allow access again after a user was locked out (due to failed login attempts).<br>The user is allowed access after the configured time, if there were no login attempts during that time.<br>■ **Range:** 60 - 604800 seconds<br>■ **Default:** 1200 seconds (20 minutes)<br>Examples:<br>■ 60 = 1 minute<br>■ 300 = 5 minutes<br>■ 3600 = 1 hour<br>■ 86400 = 1 day<br>■ 604800 = 1 week |
| `block-admin {on \| off}` | This only takes effect if "`set password-controls deny-on-fail enable`" is set to "`on`".<br>If the configured limit of failed login attempts for the `admin` user is reached, the `admin` user is locked out (unable to log in) for a configured time.<br>■ **Range:** `on`, or `off`<br>■ **Default:** `off` |

| Parameter | Description |
|---|---|
| `enable {on \| off}` | If the configured limit is reached, the user is locked out (unable to log in) for a configured time.<br>**Warning** - Enabling this leaves you open to a "denial of service" - if an attacker makes unsuccessful login attempts often enough, the affected user account is locked out. Consider the advantages and disadvantages of this option, in light of your security policy, before enabling it.<br>■ **Range:** `on`, or `off`<br>■ **Default:** `off` |
| `failures-allowed <2-1000>` | This only takes effect if "`set password-controls deny-on-fail enable`" is set to "`on`".<br>The number of failed login attempts that a user is allowed before being locked out.<br>After making that many successive failed attempts, future attempts fail.<br>When one login attempt succeeds, counting of failed attempts stops, and the count is reset to zero,<br>■ **Range:** 2 - 1000<br>■ **Default:** 10 |

## Configuring Hashing Algorithm

### Syntax

- To configure the hashing algorithm:

```
set password-controls password-hash-type {SHA256 | SHA512}
```

- To show the configured hashing algorithm:

```
show password-controls password-hash-type
```

```
show password-controls all
```

### Parameters

| Parameter | Description |
|---|---|
| `{SHA256 \| SHA512}` | Configures the hashing algorithm to store new passwords in the Gaia database.<br>■ **Range**: `SHA256`, or `SHA512`<br>■ **Default**: `SHA512` |

# Monitoring Password Policy in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

## Syntax

```
show password-controls
      all
      complexity
      deny-on-fail
            allow-after
            block-admin
            enable
            failures-allowed
      deny-on-nonuse
            allowed-days
            enable
      expiration-lockout-days
      expiration-warning-days
      force-change-when
      history-checking
      history-length
      min-password-length
      palindrome-check
      password-expiration
      password-hash-type
```

## Example

```
gaia> show password-controls all

Password Strength
    Minimum Password Length 6
    Password Complexity 2
    Password Palindrome Check on

Password History
    Password History Checking off
    Password History Length 10

Mandatory Password Change
    Password Expiration Lifetime 5
    Password Expiration Warning Days 8
    Password Expiration Lockout Days never
    Force Password Change When no

Configuration Deny Access to Unused Accounts
    Deny Access to Unused Accounts off
    Days Nonuse Before Lockout 365

Configuration Password hash
    Password hashing algorithm MD5
gaia>
```

# Configuring SSH Authentication with RSA Key Files

## Prerequisites

- Console access / LOM access to the Gaia server
- Administrator access to the Gaia server, or an equivalent user with the required permission
- The Gaia server must run version R80.40 with Take 83, or a higher version.

**Notes:**

- For the initial setup, it is necessary to do each step only one time.
- To configure more SSH users, it is necessary to do only steps 1 through 7.

## Procedure

1. Create a pair of SSH keys.

   You can use these tools:

   - On a Windows OS computer - the PuTTYgen tool.
   - On the Gaia server (or on a Linux OS computer) - the "ssh-keygen" command.

   **Important:**
   - To use the "`ssh-keygen`" command on the Gaia server:
     a. Connect to the command line and log in to the Expert mode.
     b. Save the pair of the key files in some directory.
   - Save the private SSH key file on your SSH client computer.
   - You configure the public SSH key on the Gaia server later.

2. Configure a new user on the Gaia server for the SSH connection and assign the administrator role.

   You can create and configure a new user in Gaia Portal or Gaia Clish.

- In Gaia Portal:

  Create a new user with these settings:

  - Default shell: `/bin/bash`
  - Assigned Role: `adminRole` (you can create another more limited role)

  In our example, the username is: `filecopy`

  See:

  - *"Managing User Accounts in Gaia Portal" on page 471*.
  - *"Configuring Roles in Gaia Portal" on page 481*.

- In Gaia Clish:

  a. Create a new user.

     See *"Managing User Accounts in Gaia Clish" on page 475*.

     Example:

```
MyGW> add user filecopy uid 103 homedir
/home/filecopy
WARNING Must set password and a role before user can
login.
- Use 'set user USER password' to set password.
- Use 'add rba user USER roles ROLE' to set a role.
MyGW> set user filecopy password
New password:
Verify new password:

MyGW>
```

  b. Assign the administrator role to the new user.

     See *"Configuring Roles in Gaia Clish" on page 485*.

     Note - You can create another more limited role.

     Example:

```
MyGW> add rba user filecopy roles adminRole
```

  c. Configure the default shell `/bin/bash` for the new user.

     See *"Configuring Roles in Gaia Clish" on page 485*.

     Example:

```
MyGW> set user filecopy shell /bin/bash
```

  d. Save the configuration:

```
MyGW> save config
```

3. Connect with an SSH client to the Gaia server.
4. Log in with the new user.

   In our example, the username is: `filecopy`
5. Make sure you are in the home directory:

```
cd ~ ; pwd
```

6. Configure the required directory "`.ssh`":
   a. Create the directory "`.ssh`":

      ```
      mkdir -v .ssh
      ```

   b. Assign the required permissions to the new directory "`.ssh`":

      ```
      chmod -v u=rwx,g=,o= ~/.ssh
      ```

7. Configure the required file "`authorized_keys`":
   a. Create the required file "`authorized_keys`":

      ```
      touch ~/.ssh/authorized_keys
      ```

   b. Assign the required permissions to the new file "`authorized_keys`":

      ```
      chmod -v u=rw,g=,o= ~/.ssh/authorized_keys
      ```

   c. Edit the "`authorized_keys`" file:

      ```
      vi ~/.ssh/authorized_keys
      ```

   d. Paste the SSH key you created earlier into this file.
   e. Save the changes in the file and exit the editor.
8. Make the required changes in the SSH configuration template for the Gaia operating system:
   a. Back up the `sshd_config.templ` file:

      ```
      cp -v /etc/ssh/templates/sshd_config.templ{,_BKP}
      ```

   b. Edit the `sshd_config.templ` file:

      ```
      vi /etc/ssh/templates/sshd_config.templ
      ```

c. At the bottom of the file, change the line:

from

```
PasswordAuthentication yes
```

to

```
PasswordAuthentication no
```

d. Save the changes in the file and exit the editor.

9. Import the changes from the SSH configuration template into the running Gaia configuration:

```
/usr/bin/sshd_template_xlate < /config/active
```

10. Restart the SSHD process:

```
service sshd restart
```

11. Close the current SSH connection for the new user.
12. Connect with an SSH client to the Gaia server.
13. Log in with the new user with the private SSH key.

In our example, the username is: `filecopy`

Example:

```
login as: filecopy
This system is for authorized use only.
Authenticating with public key "rsa-key-20230207"
Last login: Sun Jul  2 15:08:58 2023 from 172.20.213.71
[Expert@MyGW:0]#
```

# Authentication Servers

You can configure Gaia to authenticate Gaia users even when they are not defined locally.

This is a good way of centrally managing the credentials of multiple Security Gateways.

To define non-local Gaia users, you define Gaia as a client of an authentication server.

Gaia supports these types of authentication servers:

| Server | Description |
|---|---|
| RADIUS | RADIUS (Remote Authentication Dial-In User Service) is a client/server authentication system that supports remote-access applications. User profiles are kept in a central database on a RADIUS authentication server. Client computers or applications connect to the RADIUS server to authenticate users.<br>You can configure your Gaia computer to connect to more than one RADIUS server. If the first server in the list is unavailable, the next RADIUS server in the priority list connects. |
| TACACS+ | The TACACS+ (Terminal Access Controller Access Control System) authentication protocol users a remote server to authenticate users for Gaia. All information sent to the TACACS+ server is encrypted.<br>Gaia supports TACACS+ for authentication only. Challenge-response authentication, such as S/Key, is not supported.<br>You can configure TACACS+ support separately for different services. The Gaia Portal service is one of those, for which TACACS+ is supported and is configured as the HTTP service. When TACACS+ is configured for use with a service, Gaia contacts the TACACS+ server each time it needs to examine a user password. If the server fails or is unreachable, the user is authenticated via local password mechanism. If the user fails to authenticate via the local mechanism, the user is not allowed access.<br>**Note** - For TACACS authentication to work on a Virtual System, see the *R82 VSX Administration Guide*. |

When you configure Gaia OS to use several authentication methods, it uses them in this order:

1. RADIUS
2. TACACS+
3. Local

Authentication flow when a user enters the credentials:

1. Authenticate the user on the configured RADIUS servers.
    - If successful, the user logs in.
    - If failed, go to the next step.
2. Authenticate the user on the configured TACACS+ servers.
    - If successful, the user logs in.
    - If failed, go to the next step.
3. Authenticate the user based on the local configuration.
    - If successful, the user logs in.
    - If failed, deny the login.

# Configuring RADIUS Servers

*In This Section:*



## Configuring RADIUS Servers in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Configuring a RADIUS server

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **Authentication Servers**. |
| 2 | In the **RADIUS Servers** section, click **Add**. |
| 3 | Enter the RADIUS Server parameters:<br>■ **Priority**<br>The RADIUS server priority is an integer between -999 and 999 (default is 0).<br>When there two or more configured RADIUS servers, Gaia connects to the RADIUS server with the highest priority.<br>Low numbers have the higher priority.<br>■ **Host**<br>Host name or IP address (IPv4 or IPv6) of RADIUS server.<br>■ **UDP Port**<br>UDP port used on RADIUS server.<br>The default port is 1812 as specified by the RADIUS standard.<br>The range of valid port numbers is from 1 to 65535.<br>Port 1645 is non-standard, but is commonly used as alternative to port 1812.<br>**Warning** - Firewall software frequently blocks traffic on port 1812. Make sure that you define a Firewall rule to allow traffic on UDP port 1812 between the RADIUS server and Gaia.<br>■ **Shared Secret**<br>Shared secret used for authentication between the RADIUS server and the Gaia client.<br>Enter the shared secret text string up to 256 characters, without any whitespace characters and without a backslash.<br>Make sure that the shared string defined on the Gaia matches the shared string defined on the RADIUS server.<br>RFC 2865 recommends that the secret be at least 16 characters in length.<br>Some RADIUS servers have a maximum string length for shared secret of 15 or 16 characters.<br>See the documentation for your RADIUS server.<br>■ **Timeout in**<br>**Optional:** Enter the timeout in seconds (from 1 to 5), during which Gaia waits for the RADIUS server to respond. The default value is 3.<br>If there is no response after the configured timeout, Gaia tries to connect to a different configured RADIUS server.<br>Set this timeout, so that the sum of all RADIUS server timeouts is less than 50. |

| Step | Instructions |
|---|---|
| 4 | Click **OK**. |
| 5 | **Optional:** Select the **Network Access Server (NAS)** IP address.<br>This setting applies to all configured RADIUS servers.<br>This parameter records the IP address, from which Gaia sends the RADIUS packet.<br>This IP address is stored in the RADIUS packet, even when the packet goes through NAT, or some other address translation that changes the source IP address of the packet.<br>The "NAS-IP-Address" is defined in RFC 2865.<br>If no NAS IP Address is chosen, the IPv4 address of the Gaia Management Interface is used (click **Network Management > Network Interfaces >** see the **Management Interface** section). |
| 6 | **Optional:** Select **RADIUS Users Default Shell** (for details about the shells, see *"Users" on page 469*).<br>This setting applies to all configured RADIUS servers. |
| 7 | **Optional:** Select the **Super User ID** - 0 or 96.<br>This setting applies to all configured RADIUS servers.<br>If the UID is 0, there is no need to run the `sudo` command to get super user permissions (see *"Configuring RADIUS Servers for Non-Local Gaia Users" on page 548*). |
| 8 | Click **Apply**. |

## Editing the RADIUS server

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **Authentication Servers**. |
| 2 | Select the RADIUS server. |
| 3 | Click **Edit**. |
| 4 | You can edit only the **Host**, **UDP Port**, **Shared secret**, and **Timeout**. |
| 5 | Click **OK**. |

## Deleting a RADIUS server

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **Authentication Servers**. |
| 2 | Select the RADIUS server. |
| 3 | Click **Delete**. |
| 4 | Click **OK** to confirm. |

# Configuring RADIUS Servers in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

## Description

Use the "`aaa radius-servers`" commands to add, configure, and delete RADIUS authentication servers.

## Syntax

### Configuring RADIUS settings for use in a single authentication profile

```
add aaa radius-servers priority <Priority> host <Hostname, or IP
Address of RADIUS Server> [port <1-65535>]
      prompt-secret timeout <1-50>
      secret <Shared Secret> timeout <1-50>
```

### Changing the configuration of a specific RADIUS server

```
set aaa radius-servers priority <Priority>
      host <Hostname, or IP Address of RADIUS Server>
      new-priority <New Priority>
      port <1-65535>
      prompt-secret
      secret <Shared Secret>
      timeout <1-50>
```

### Changing the configuration that applies to all configured RADIUS servers

```
set aaa radius-servers
      NAS-IP<SPACE><TAB>
      default-shell<SPACE><TAB>
      super-user-uid <0 | 96>
```

### Viewing a list of all configured RADIUS servers associated with an authentication profile

```
show aaa radius-servers list
```

### Viewing the configuration of a specific RADIUS server

```
show aaa radius-servers priority <Priority>
      host
      port
      timeout
```

**Viewing the configuration that applies to all configured RADIUS servers**

```
show aaa radius-servers
      NAS-IP
      default-shell
      super-user-uid
```

**Deleting a specific RADIUS server**

```
delete aaa radius-servers
      priority <Priority>
```

**Deleting the configuration that applies to all configured RADIUS servers**

```
delete aaa radius-servers
      NAS-IP
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| `priority <Priority>` | Configures the RADIUS server priority. Enter an integer between -999 and 999 (default is 0).<br>When there two or more configured RADIUS servers, Gaia connects to the RADIUS server with the highest priority.<br>Low numbers have the higher priority. |
| `new-priority <New Priority>` | Configures the new priority for the RADIUS server. |
| `host <Hostname, or IP Address of RADIUS Server>` | Configures the Host name or IP address (IPv4 or IPv6) of RADIUS server. |
| `port <1-65535>` | Configures the UDP port used on RADIUS server.<br>The default port is 1812 as specified by the RADIUS standard.<br>The range of valid port numbers is from 1 to 65535. Port 1645 is non-standard, but is commonly used as alternative to port 1812.<br>**Warning** - Firewall software frequently blocks traffic on port 1812. Make sure that you define a Firewall rule to allow traffic on UDP port 1812 between the RADIUS server and Gaia. |

| Parameter | Description |
|---|---|
| `prompt secret` | The system will prompt you to enter the Shared Secret. |
| `secret <Shared Secret>` | Configures the shared secret used for authentication between the RADIUS server and the Gaia.<br>Enter the shared secret text string up to 256 characters, without any whitespace characters and without a backslash.<br>Make sure that the shared string defined on the Gaia matches the shared string defined on the RADIUS server.<br>RFC 2865 recommends that the secret be at least 16 characters in length.<br>Some RADIUS servers have a maximum string length for shared secret of 15 or 16 characters.<br>See the documentation for your RADIUS server. |
| `timeout <1-50>` | Configures the timeout in seconds (from 1 to 5), during which Gaia waits for the RADIUS server to respond.<br>The default value is 3.<br>If there is no response after the configured timeout, Gaia tries to connect to a different configured RADIUS server.<br>Set this timeout, so that the sum of all RADIUS server timeouts is less than 50. |
| `default-shell` <SPACE><TAB> | **Optional:** Configures the default shell for RADIUS Users (for details about the shells, see *"Users" on page 469*). |
| `super-user-uid <0 \| 96>` | **Optional:** Configures the UID for the RADIUS super user.<br>If the UID is 0, there is no need to run the `sudo` command to get super user permissions (see *"Configuring RADIUS Servers for Non-Local Gaia Users" on page 548*). |
| `NAS-IP`<SPACE><TAB> | **Optional:** This parameter records the IP address, from which Gaia sends the RADIUS packet.<br>This IP address is stored in the RADIUS packet, even when the packet goes through NAT, or some other address translation that changes the source IP address of the packet.<br>The "NAS-IP-Address" is defined in RFC2865.<br>If no NAS IP Address is chosen, the IPv4 address of the Gaia Management Interface is used (run the "`show management interface`" command). |

# Configuring Gaia as a RADIUS Client

Gaia acts as a RADIUS client. You must define a role for the RADIUS client, and the features for that role.

To allow login with non-local users to Gaia, you must define a default Gaia role for all non-local users that are configured in the RADIUS server.

The default role can include a combination of:

- Administrative (read/write) access to some features
- Monitoring (read-only) access to other features
- No access to other features.

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

### To configure Gaia as a RADIUS Client

| Step | Instructions |
|---|---|
| 1 | Define the role for the RADIUS client:<br>■ If no group is defined on the RADIUS server for the client, define this role:<br>`radius-group-any`<br>■ If a group is defined on RADIUS server for the client (group `XXX`, for example), define this role:<br>`radius-group-<XXX>` |
| 2 | Define the features for the role. |

### Example for Gaia Clish

```
gaia> add rba role radius-group-any domain-type System readonly-
features arp
```

For instructions, see *"Roles" on page 480*.

**Note** - Do **not** define a new user for external users. An external user is one that is defined on an authentication server (such as RADIUS or TACACS), and not on the local Gaia system.

# Configuring RADIUS Servers for Non-Local Gaia Users

Non-local users can be defined on a RADIUS server and not in Gaia.

When a non-local user logs in to Gaia, the RADIUS server authenticates the user and assigns the applicable permissions.

You must configure the RADIUS server to correctly authenticate and authorize non-local users.

**Important** - If you define a RADIUS user with a null password (on the RADIUS server), Gaia cannot authenticate that user.

### Configuring a RADIUS server for non-local Gaia users

In addition, see sk72940.

| Step | Instructions |
|---|---|
| 1 | Copy the applicable dictionary file to your RADIUS server. |
| | **Example for the "*Steel-Belted RADIUS server*"**<br>a. Copy this file from the Gaia to the RADIUS server:<br>`/etc/radius-dictionaries/checkpoint.dct`<br>b. Add these lines to the `vendor.ini` file on the RADIUS server (keep in alphabetical order with the other vendor products in this file):<br>`vendor-product = Check Point Gaia`<br>`dictionary = nokiaipso`<br>`ignore-ports = no`<br>`port-number-usage = per-port-type`<br>`help-id = 2000`<br>c. Add this line to the `dictiona.dcm` file:<br>`"@checkpoint.dct"` |
| | **Example for the "*FreeRADIUS server*"**<br>a. Copy this file from the Gaia to the RADIUS server to the `/etc/freeradius/` directory:<br>`/etc/radius-dictionaries/dictionary.checkpoint`<br>b. Add this line to the `/etc/freeradius/dictionary` file:<br>`"$INCLUDE dictionary.checkpoint"` |

| Step | Instructions |
|---|---|
| | **Example for the "*OpenRADIUS server*"**<br>a. Copy this file from the Gaia to the RADIUS server to the `/etc/openradius/subdicts/` directory: `/etc/radius-dictionaries/dict.checkpoint`<br>b. Add this line `/etc/openradius/dictionaries` file immediately after the `dict.ascend`: `$include subdicts/dict.checkpoint` |
| 2 | Define the user roles on Gaia.<br>Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:<br>`CP-Gaia-User-Role = "role1,role2,...`<br>For example:<br>`CP-Gaia-User-Role = "adminrole, backuprole, securityrole"` |
| 3 | Define the Check Point users that must have superuser access to the Gaia shell.<br>Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:<br>■ If this user should not receive superuser permissions:<br>`CP-Gaia-SuperUser-Access = 0`<br>■ If this user can receive superuser permissions:<br>`CP-Gaia-SuperUser-Access = 1` |

### Logging in as the superuser

A user with super user permissions can use the Gaia shell to do system-level operations, including working with the file system.

Super user permissions are defined in the Check Point Vendor-Specific Attributes.

Users that have a UID of 0 have super user permissions.

They can run all the commands that the root user can run.

Users that have a UID of 96 must run the `sudo` command to get super user permissions.

The UIDs of all non-local users are defined in the `/etc/passwd` file.

### Getting the superuser permissions (for users that have a UID of 96)

**Important** - On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in the Expert mode on the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on Gaia. |
| 2 | Log in to the Expert mode. |
| 3 | Run:<br>`sudo /usr/bin/su -`<br>The user now has superuser permissions. |

# Configuring TACACS+ Servers

*In This Section:*



## Configuring TACACS+ Servers in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Configuring a TACACS+ server

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **Authentication Servers**. |
| 2 | In the **TACACS+ Configuration** section, select **Enable TACACS+ authentication**.<br>This setting applies to all configured TACACS+ servers. |
| 3 | Click **Apply**. |
| 4 | In the **TACACS+ Servers** section, click **Add**. |

| Step | Instructions |
|---|---|
| 5 | Configure the TACACS+ parameters:<br>■ **Priority**<br>The priority of the TACACS+ server - from 1 to 20.<br>Must be unique for this operating system.<br>Gaia uses the priority:<br>• To determine the order, in which Gaia connects to the TACACS+ servers.<br>First, Gaia connects to the TACACS+ server with the lowest priority number.<br>For example: Three TACACS+ servers have a priority of 1, 5, and 10 respectively.<br>Gaia connects to these TACACS+ servers in that order, and uses the first TACACS+ server that responds.<br>• To identify the TACACS+ server in commands. A command with `priority 1` applies to the TACACS+ server with priority 1.<br>■ **Server**<br>IPv4 address of the TACACS+ server.<br>■ **Shared Key**<br>The Shared Secret used for authentication between the TACACS+ server and Gaia.<br>Enter the shared secret text string up to 256 characters, without any whitespace characters and without a backslash.<br>Make sure that the shared string defined on the Gaia matches the shared string defined on the TACACS+ server.<br>■ **Timeout in Seconds**<br>Enter the timeout in seconds (from 1 to 60), during which Gaia waits for the TACACS+ server to respond.<br>The default value is 5.<br>If there is no response after the configured timeout, Gaia tries to connect to a different configured TACACS+ server. |
| 6 | Click **OK**. |
| 7 | **Optional:** In the **TACACS+ Servers Advanced Configuration** section, select the **User UID** - 0, or 96 and click **Apply**.<br>This setting applies to all configured TACACS+ servers. |

### Disabling TACACS+ authentication

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **Authentication Servers**. |

| Step | Instructions |
|---|---|
| 2 | In the **TACACS+ configuration** section, clear **Enable TACACS+ authentication**.<br>This setting applies to all configured TACACS+ servers. |
| 3 | Click **Apply**. |

### Deleting the TACACS+ server

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **Authentication Servers**. |
| 2 | In the **TACACS+ Servers** section, select a TACACS+ server. |
| 3 | Click **Delete**. |
| 4 | Click **OK** to confirm. |

# Configuring TACACS+ Servers in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

## Syntax

### Configuring a TACACS+ server for use in a single authentication profile

```
add aaa tacacs-servers priority <Priority> server <IPv4 Address
of TACACS+ Server> key <Shared Secret> timeout <1-60>
```

### Changing the configuration of a specific TACACS+ server

```
set aaa tacacs-servers priority <Priority>
      server <IPv4 Address of TACACS+ Server>
      new-priority <New Priority>
      key <Shared Secret>
      timeout <1-60>
```

### Changing the configuration that applies to all configured TACACS+ servers

```
set aaa tacacs-servers
      state {on | off}
      user-uid <0 | 96>
```

### Viewing the list of all configured TACACS+ servers associated with an authentication profile

```
show aaa tacacs-servers list
```

### Viewing the configuration of a specific TACACS+ server

```
show aaa tacacs-servers priority <Priority>
      server
      timeout
```

### Viewing the configuration that applies to all configured TACACS+ servers

```
show aaa tacacs-servers
      state
      user-uid
```

### Deleting a specific TACACS+ server

```
delete aaa tacacs-servers
      priority <Priority>
```

**Deleting the configuration that applies to all configured TACACS+ servers**

```
delete aaa tacacs-servers
      NAS-IP
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| `priority <Priority>` | The priority of the TACACS+ server - from 1 to 20.<br>Must be unique for this operating system.<br>The priority is used:<br>■ To determine the order, in which Gaia connects to the TACACS+ servers.<br>First, Gaia connects to the TACACS+ server with the lowest priority number.<br>For example: Three TACACS+ servers have a priority of 1, 5, and 10 respectively.<br>Gaia connects to these TACACS+ servers in that order, and uses the first TACACS+ server that responds.<br>■ To identify the TACACS+ server in commands. A command with `priority 1` applies to the TACACS+ server with priority 1.<br>Values:<br>■ **Range:** 1 - 20<br>■ **Default:** No default |
| `server <IPv4 Address of TACACS+ Server>` | IPv4 address of the TACACS+ server. |
| `key <Shared Secret>` | The Shared Secret used for authentication between the TACACS+ server and Gaia.<br>Enter the shared secret text string up to 256 characters, without any whitespace characters and without a backslash.<br>Make sure that the shared string defined on the Gaia matches the shared string defined on the TACACS+ server. |

| Parameter | Description |
|---|---|
| `timeout <1-60>` | Enter the timeout in seconds, during which Gaia waits for the TACACS+ server to respond.<br>If there is no response after the configured timeout, Gaia tries to connect to a different configured TACACS+ server.<br>■ **Range:** 1 - 60<br>■ **Default:** 5 |
| `new-priority <`*`New Priority`*`>` | Configures the new priority for the TACACS+ server. |
| `state {on \| off}` | Configures the state of TACACS+ authentication.<br>■ **Range:** `on`, or `off`<br>■ **Default:** `off` |

**Example**

```
gaia> set aaa tacacs-servers priority 2 server 10.10.10.99 key
MySharedSecretKey timeout 10
```

## Checking if the Logged In User is Enabled for TACACS+

**Procedure**

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on Gaia. |
| 2 | Log in to Gaia Clish. |
| 3 | On Scalable Platforms, go to Gaia gClish:<br>Type `gclish` and press Enter. |
| 4 | Run:<br>`show tacacs_enable` |

# Configuring Gaia as a TACACS+ Client

Gaia acts as a TACACS+ client for Gaia users that are defined on the TACACS+ server and are not defined locally on Gaia.

The **admin** user must define a role called `TACP-0` for the TACACS+ users, and the allowed features for the `TACP-0` role.

**Important:**

1. All TACACS+ users must log in to Gaia OS with the password assigned to the default role `TACP-0`.
2. To get their applicable TACP role in Gaia OS, after this initial login, TACACS+ users must log in for the second time with the password assigned to their applicable TACP role.

### Privilege Escalation

The Gaia admin user can define roles that make it possible for Gaia users to get temporarily higher privileges, than their regular privileges.

For example, Gaia user Fred needs to configure the interfaces, but his role does not support interfaces configuration. To configure the interfaces, Fred enters his user name together with a password given him by the admin user. This password lets him change his default role to the role that allows him to configure the interfaces.

There are sixteen different privilege levels (0 - 15) defined in TACACS+.

Each level can be mapped to a different Gaia role.

For example:

- Privilege level 0 - monitor-only
- Privilege level 1 - basic network configuration
- Privilege level 15 - admin user

By default, all non-local TACACS+ Gaia users are assigned the role `TACP-0`.

The Gaia admin can define for them roles with the name `TACP-N` that give them different privileges, where `N` is a privilege level - a number from 1 to 15.

The TACACS+ users can changes their own privileges by moving to another TACP-N role.

To do this, the TACACS+ users need to get a password from the Gaia admin user.

### Configuring Gaia as a TACACS+ Client

| Step | Instructions |
|---|---|
| 1 | Connect to Gaia OS as the `admin` user. |

| Step | Instructions |
|---|---|
| 2 | Define the role `TACP-0`. |
| 3 | Define the features for the role.<br>For instructions, see *"Roles" on page 480*. |
| 4 | **Optional:** Define one or more roles with the name `TACP-N` where `N` is a privilege level - a number from 1 to 15, and define the features for each role. |

### Raising the "TACP" privileges

You can raise the "TACP" privileges in either Gaia Portal, or Gaia Clish.

#### Raising "TACP" privileges in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | In your web browser, connect to Gaia Portal. |
| 2 | Enter the username and password of the TACACS+ user.<br>After the TACACS server authentication, you have the privileges of the TACP-0 role. |
| 3 | To raise the privileges to the `TACP-N` role (`N` is a number from 1 to 15), click **Enable** at the top of the **Overview** page. |
| 4 | Enter the password for the user. |

#### Raising "TACP" privileges in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

| Step | Instructions |
|---|---|
| 1 | Connect to the command line. |
| 2 | Log in to the Gaia Clish using the username and password of the TACACS+ user. |

| Step | Instructions |
|---|---|
| 3 | After you are authenticated by the TACACS server, you get the Gaia Clish prompt.<br>At this point, you have the privileges of the TACP-0 role.<br>Run:<br>`tacacs_enable TACP-<N>`<br>Where *N* is the new TACP role (an integer from 1 to 15). |
| 4 | When prompted, enter the applicable password. |

To go back to the TACP-0 role, press **CTRL+D**, or enter **exit** at the command prompt.

The user automatically exits the current shell and goes back to TACP-0.

**Note** - Do **not** define a new user for external users. An external user is one that is defined on an authentication server (such as RADIUS, or TACACS), and not on the local Gaia system.

**Viewing if the currently logged in user is authenticated by TACACS+**

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on Gaia. |
| 2 | Log in to Gaia Clish. |
| 3 | On Scalable Platforms, go to Gaia gClish:<br>Type `gclish` and press Enter. |
| 3 | Run:<br>`show tacacs_enable` |

# Configuring TACACS+ Servers for Non-Local Gaia Users

You can define Gaia users on a TACACS server instead of defining them on the Gaia computer.

Gaia users that are defined on a TACACS server are called non-local users.

Cisco ACS servers are the most commonly used TACACS+ servers.

For help with the configuration of a Cisco ACS server as a TACACS+ server for Gaia clients, see sk98733 (as an example of best practices and **not** a replacement for the official Cisco documentation).

When a non-local user logs in to Gaia, the TACACS server authenticates the user and assigns the permissions to the user.

You must configure the TACACS server to correctly authenticate and authorize non-local Gaia users.

**Important** - If you define a TACACS user with a null password (on the TACACS server), Gaia cannot authenticate that user.

# Configuring Authentication Access Order

Configure the order of the user authentication methods in Gaia Portal and Gaia Clish.

## The Default Order and State

| Priority | Server Type | State | Note |
|---|---|---|---|
| 1 | TACACS | Off | See:<br>■ *"Configuring TACACS+ Servers" on page 551*<br>■ *"Configuring Gaia as a TACACS+ Client" on page 557*<br>■ *"Configuring TACACS+ Servers for Non-Local Gaia Users" on page 560* |
| 2 | RADIUS | On | See:<br>■ *"Configuring RADIUS Servers" on page 542*<br>■ *"Configuring Gaia as a RADIUS Client" on page 547*<br>■ *"Configuring RADIUS Servers for Non-Local Gaia Users" on page 548* |
| 3 | Local | On | See:<br>■ *"Users" on page 469* |

## Configuration in Gaia Portal

1. From the left tree, click **User Management** > **Authentication Servers**.
2. In the section **Authentication Access Order**, select the applicable server type and click **Edit**.
3. In the **Priority** field, configure the required priority.
4. In the **State** field, select the applicable value ("`On`" or "`Off`").
5. Click **OK**.

## Configuration in Gaia Clish

This command shows the order in which Gaia OS uses the configured AAA servers if you enable them

```
show aaa order
```

Example Output:

```
gaia> show aaa order

Priority     Server Type          State

1            TACACS       Off
2            RADIUS       On
3            Local        On

gaia>
```

To configure the order of authentication access:

```
set aaa order {radius | tacacs | local} priority <1-3>
```

```
set aaa order {radius | tacacs | local} state {on | off}
```

# System Groups

*In This Section:*



## Introduction

You can define and configure groups with Gaia as you can with equivalent Linux-based systems.

This function is retained in Gaia for advanced applications and for retaining compatibility with Linux.

Use groups for these purposes:

- Specify Linux file permissions.
- Control who can log in through SSH.

For other functions that are related to groups, use the role-based administration feature, described in *"Roles" on page 480*.

All users are assigned by default to the `users` group. You can edit a user's primary group ID (using Gaia Clish) to be something other than the default. However, you can still add the user to the `users` group. The list of members of the `users` group includes only users, who are explicitly added to the group. The list of does not include users added by default.

# Configuring System Groups in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Viewing the list of all System Groups

In the navigation tree, click **User Management** > **System Groups**.

### Adding a System Group

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **System Groups**. |
| 2 | Click **Add**. |
| 3 | In the **Group Name** field, enter the applicable unique name - between 1 and 16 alphanumeric characters without spaces. |
| 4 | In the **Group ID** field, enter a unique Group ID number - between 101 and 65530:<br>■ Group ID range 0-100 and range 65531-65535 are reserved for system use.<br>■ Group ID 0 is reserved for users with root permissions.<br>■ Group ID 10 is reserved for the predefined Users groups.<br>If you specify a value in the reserved ranges, an error message is displayed. |
| 5 | Click **OK**. |

### Adding a user to the System Group

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **System Groups**. |
| 2 | Select the System Group. |
| 3 | Click **Edit**. |
| 4 | In the **Available Members** list, select a user.<br>To select several users:<br>a. Press and hold the **CTRL** key on the keyboard.<br>b. Left-click the applicable users.<br>The selected users become highlighted. |

| Step | Instructions |
|---|---|
| 5 | Click **Add >**.<br>The selected users move to the **Members of Group** list. |
| 6 | Click **OK**. |

### Removing a user from the System Group

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **System Groups**. |
| 2 | Select the System Group. |
| 3 | Click **Edit**. |
| 4 | In the **Members of Group** list, select a user.<br>To select several users:<br>a. Press and hold the **Ctrl** key on the keyboard.<br>b. Left-click the applicable users.<br>The selected users become highlighted. |
| 5 | Click **Add >**.<br>The selected users move to the **Available Members** list. |
| 6 | Click **OK**. |

### Deleting the System Group

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management** > **System Groups**. |
| 2 | Select the System Group. |
| 3 | Click **Delete**. |
| 4 | Click **OK** to confirm. |

# Configuring System Groups in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

## Syntax

### Adding a System Group

```
add group <Group Name> gid <Group ID>
```

### Adding a user to the System Group

```
add group <Group Name> member<SPACE><TAB>
add group <Group Name> member <UserName>
```

### Changing the Group ID of a System Group

```
set group <Group Name> gid <Group ID>
```

### Viewing all users in the System Group

```
show group <Group Name>
```

### Viewing all configured System Groups

```
show groups
```

### Removing a user from a System Group

```
delete group <Group Name> member<SPACE><TAB>
delete group <Group Name> member <UserName>
```

### Deleting a System Group

```
delete group <Group Name>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

### CLI Parameters

| Parameter | Description |
|---|---|
| `group <Group Name>` | Unique name of System Group - between 1 and 16 alphanumeric characters without spaces |
| `gid <Group ID>` | Unique Group ID number - between 101 and 65530:<br>■ Group ID range 0-100 and range 65531-65535 are reserved for system use.<br>■ Group ID 0 is reserved for users with root permissions.<br>■ Group ID 10 is reserved for the predefined Users groups.<br>If you specify a value in the reserved ranges, an error message is displayed. |
| `member <UserName>` | Name of an existing user. |

# GUI Clients

*In This Section:*



If this is a Security Management Server, you can configure which computers can connect to this Security Management Server with SmartConsole.

**Note** - This section does **not** appear, if this is a Multi-Domain Server.

## Configuring GUI Clients in Gaia Portal

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **User Management > GUI Clients**. |
| 2 | Click **Add**.<br>The **Add GUI Client** window opens. |
| 3 | Define the GUI clients (trusted hosts).<br>These are the values:<br>■ **Any IP Address**<br>All clients are allowed to log in, regardless of their IP address.<br>This option only shows if **Any** was not defined during the initial configuration.<br>■ **This machine - IP address**<br>■ **Network**<br>■ **Range of IPv4 addresses** |

# Configuring GUI Clients in Command Line

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on the Security Management Server. |
| 2 | Run:<br>`cpconfig`<br>For more information, see the *R82 CLI Reference Guide* > Chapter *Security Management Server Commands* > Section *cpconfig*. |
| 3 | Enter **3** for the **GUI Clients** option. |
| 4 | A list of hosts selected to be GUI clients shows.<br>You can add or delete hosts, or create a new list.<br>You can add new GUI clients in these formats:<br>■ **IP address** - One computer defined by its IPv4 or IPv6 address.<br>■ **Machine name** - One computer defined by its hostname.<br>■ **"Any"** - An IPv4 address without restriction.<br>You must:<br>a. Enter the word **Any** with capital letter "**A**"<br>b. Press the Enter key<br>c. Press the **CTRL+D** keys.<br>■ **IP/Netmask** - A range of IPv4 addresses (for example, `192.168.10.0/255.255.255.0`) or IPv6 addresses (for example, `2001::1/128`).<br>■ **A range of addresses** - A limited range of IPv4 addresses (for example, `192.168.10.8-192.168.10.16`), or IPv6 addresses (for example, `2001::1-2001::10`).<br>■ **Wild cards (IPv4 only)** - A limited range of IPv4 addresses only (for example, `192.168.10.*`). |

# High Availability

*In This Section:*



**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature in Gaia operating system (Known Limitation MBS-2521).
To configure Scalable Platforms in Dual Site, see the *R82 Scalable Platforms Administration Guide*.

# Understanding VRRP

Virtual Routing Redundancy Protocol (VRRP) is a high-availability solution, where two Gaia Security Gateways can provide backup for each other. Gaia offers two ways to configure VRRP:

- **Monitored Circuit/Simplified VRRP** - All the VRRP interfaces automatically monitor other VRRP interfaces.
- **Advanced VRRP** - Every VRRP interface must be explicitly configured to monitor every other VRRP interface.

**Important:**

- You cannot have a Standalone deployment (Security Gateway and Security Management Server on the same computer) in a Gaia VRRP cluster.
- You cannot use both the Monitored Circuit/Simplified VRRP and Advanced VRRP together on the same Cluster Member.

Virtual Router Redundancy Protocol (VRRP) provides dynamic failover of IP addresses from one router to another in the event of failure. This increases the availability and reliability of routing paths through gateway selections on an IP network. Each VRRP router has a unique identifier known as the Virtual Router Identifier (VRID), which is associated with at least one Virtual IP Address (VIP). Neighboring network nodes connect to the VIP as a next hop in a route or as a final destination. Gaia supports VRRP as configured in RFC 3768.

# VRRP Terminology

The conceptual information and procedures in this chapter use standard VRRP terminology.

This glossary contains basic VRRP terminology and a reference to related Check Point ClusterXL terms.

| VRRP Term | ClusterXL Term | Definition |
|---|---|---|
| VRRP Cluster | Cluster | A group of Security Gateways that provides redundancy. |
| VRRP Router | Member | A Security Gateway using the VRRP protocol that is a member of one or more Virtual Router. In this guide, a VRRP Router is commonly called a Security Gateway. |
| Master | Active | The Security Gateway (Security Gateway) that handles traffic to and from a Virtual Router. The Master is the Security Gateway with the highest priority in a group. The Master inspects traffic and enforces the security policy. |
| Backup | Standby | A redundant Security Gateway (Security Gateway) that is available to take over for the Master in the event of a failure. |
| VRID | Cluster name | Unique Virtual Router identifier The VRID is the also last byte of the MAC address. |
| VIP | Cluster Virtual IP address | Virtual IP address assigned to a Virtual Router. VIPs are routable from internal and/or external network resources. The VIP is called **Backup Address** in the Gaia Portal. |
| VMAC | VMAC | Virtual MAC address assigned to a Virtual Router. |
| VRRP Transition | Failover | Automatic change over to a backup Security Gateway when the primary Security Gateway fails or is unavailable. The term 'failover' is used frequently in this guide. |

# VRRP on Gaia OS

On Gaia, VRRP can be used with ClusterXL enabled or with ClusterXL disabled.

| VRRP with ClusterXL | Description |
|---|---|
| VRRP with ClusterXL *enabled* | This is the most common use case.<br>You can deploy only an Active/Backup environments.<br>VRRP supports a maximum of one VRID with one Virtual IP Address (VIP) for each interface.<br>You must configure VRRP, so that the same node is the VRRP Master for all VRIDs. Therefore, you must configure each VRID to monitor every other VRRP-enabled interface.<br>You must also configure *priority deltas* to allow a failover to the VRRP Backup node, when the VRID on any on interface fails over. |
| VRRP with ClusterXL *disabled* | You can deploy an Active/Active environment.<br>You can configure two VRIDs on the same interface, with one VIP for each VRID.<br>This configuration supports only static routes on the VRRP interfaces.<br>You must disable the **VRRP monitoring of the Check Point Firewall** (see *"Preparing a VRRP Cluster" on page 579*). |

# VRRP Configuration Methods

| VRRP Method | Description |
|---|---|
| **Monitored Circuit/Simplified VRRP** | To configure this simplified VRRP method, in the Gaia Portal go to **High Availability > VRRP**.<br>This method contains all of the basic parameters, and is applicable for most environments.<br>You configure each Virtual Router as one unit and configure the same VRID on all interfaces.<br>Monitored Circuit VRRP automatically monitors all VRRP interfaces. This make a complete node failover possible.<br>You can configure only one VRID, which is automatically added to all the VRRP interfaces.<br>If the VRID on any of the VRRP-enabled interfaces fails, the configured priority delta is decremented on the other VRRP-enabled interfaces to allow the VRRP Backup node to take over as the new VRRP Master. |
| **Advanced VRRP** | To configure this advanced VRRP method, in the Gaia Portal go to **High Availability > Advanced VRRP**.<br>This method allows configuration of different VRIDs on different interfaces.<br>You configure a VRID on each interface individually. In addition, each VRRP-enabled interface must be monitored by each VRID together with an appropriate priority delta. This ensures that when one interface fails, all the other VRIDs can transition to VRRP Backup state<br>■ With ClusterXL *enabled*, you must configure each VRID to monitor every other VRRP interface.<br>You must also configure priority deltas that allow complete node failover.<br>Advanced VRRP also makes it possible for a VRID to monitor interfaces that do not run VRRP.<br>■ With ClusterXL *disabled*, you can configure two VRIDs on each interface, with one VIP for each VRID. |

# Monitoring of VRRP Interfaces

The monitoring of all VRRP-enabled interfaces by all VRIDs is important to avoid connection issues with asymmetric routes.

For example, when an external interface fails, the VRRP Master fails over only for the external Virtual Router. The VRRP Master for the internal Virtual Router does not fail over. This can cause connectivity problems when the internal Virtual Router accepts traffic and is unable to connect to the new external VRRP Master.

Another tool for avoiding asymmetric issues during transitions is the VRRP *interface delay* setting. Configure this when the Preempt Mode of VRRP was turned off. This VRRP global setting is useful when the VRRP node with a higher priority is rebooted, but must not preempt the existing VRRP Master that handles the traffic, but is configured with a lower priority. Sometimes, interfaces that come up, take longer than the VRRP timeout to process incoming VRRP Hello packets. The interface delay extends the time that VRRP waits to receive VRRP Hello packets from the existing VRRP Master.

# How VRRP Failover Works

Each Virtual Router (VRRP Group) is identified by a unique *Virtual Router ID* (VRID).

A Virtual Router contains one VRRP *Master* Security Gateway and at least one VRRP *Backup* Security Gateway.

The VRRP Master sends periodic VRRP advertisements (known as VRRP *Hello* messages) to the VRRP Backup Security Gateways.

VRRP advertisements broadcast the operational status of the VRRP Master to the VRRP Backup.

Gaia uses dynamic routing protocols to advertise the VIP of the Virtual Router (Virtual IP address or Backup IP address).

**Notes:**

- Gaia supports OSPF on VPN tunnels that terminate at a VRRP group.
- Active/Backup VRRP environments are supported with ClusterXL enabled. If ClusterXL is disabled, Active/Active environments can be deployed.
- Active/Active VRRP environments support only static routes. In addition, you must disable the monitoring of the Check Point Firewall by VRRP.

If the VRRP Master fails, or its VRRP-enabled interfaces fail, VRRP uses a priority algorithm to make the decision if failover to a VRRP Backup is necessary. Initially, the VRRP Master is the Security Gateway that has the highest configured priority value. You configure a priority for each Security Gateway when you create a Virtual Router or change its configuration. If two VRRP Security Gateways have same priority value, the platform that comes online and broadcasts its VRRP advertisements first becomes the VRRP Master.

Gaia also uses priorities to select a VRRP Backup Security Gateway upon failover (when there is more than one VRRP Backup available). In the event of failover, the Virtual Router priority value is decreased by a predefined *Priority Delta* value to calculate an *Effective Priority* value. The Virtual Router with the highest effective priority becomes the new VRRP Master. The *Priority Delta* value is a Check Point proprietary parameter that you configure when configuring a Virtual Router. If you configure your system correctly, the effective priority will be lower than the VRRP Backup Security Gateway priority in the other Virtual Routers. This causes the problematic VRRP Master to fail over for the other Virtual Routers as well.

**Note** - If the effective priority for the current VRRP Master and VRRP Backup are the same, the Security Gateway with the highest IP address becomes the VRRP Master.

# Typical VRRP Use Cases

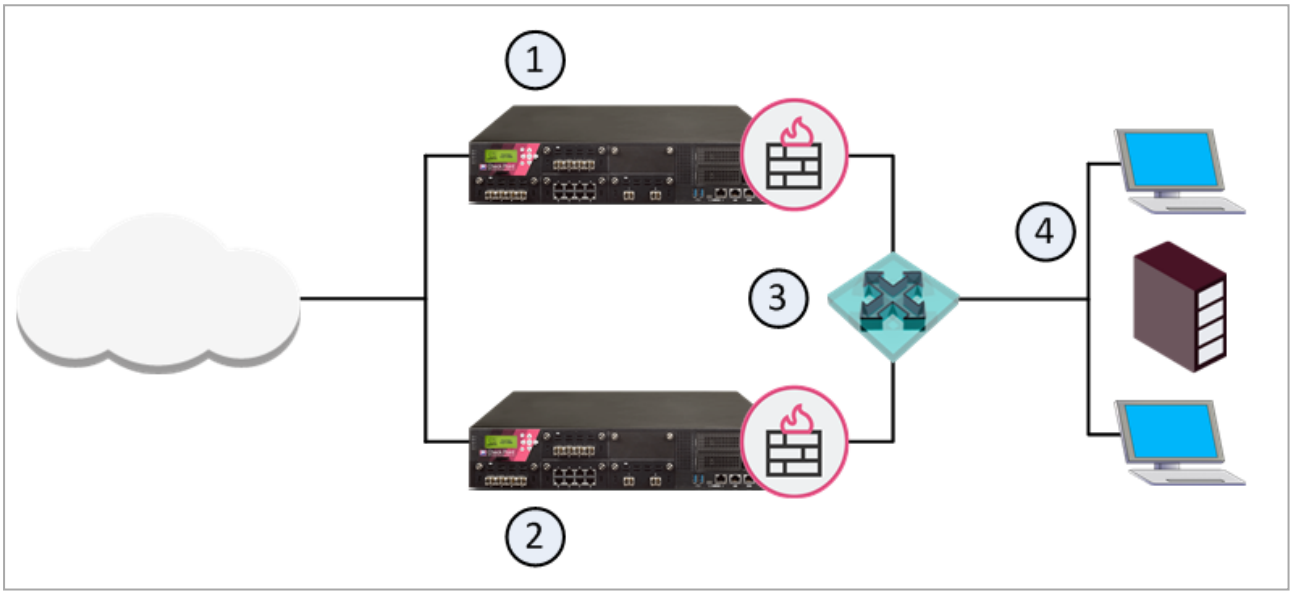
These are examples of some VRRP environments.

### VRRP Use Case 1 - Internal Network High Availability

This is a simple VRRP use case, where Security Gateway 1 is the VRRP Master, and Security Gateway 2 is the VRRP Backup.

Virtual Router redundancy is available only for connections to and from the internal network.

There is no redundancy for external network traffic.




| Item | Description |
|---|---|
| 1 | VRRP Master Security Gateway |
| 2 | VRRP Backup Security Gateway |
| 3 | Virtual Router VRID 5 - Virtual IP Address (Backup Address) is 192.168.2.5 |
| 4 | Internal Network and hosts |

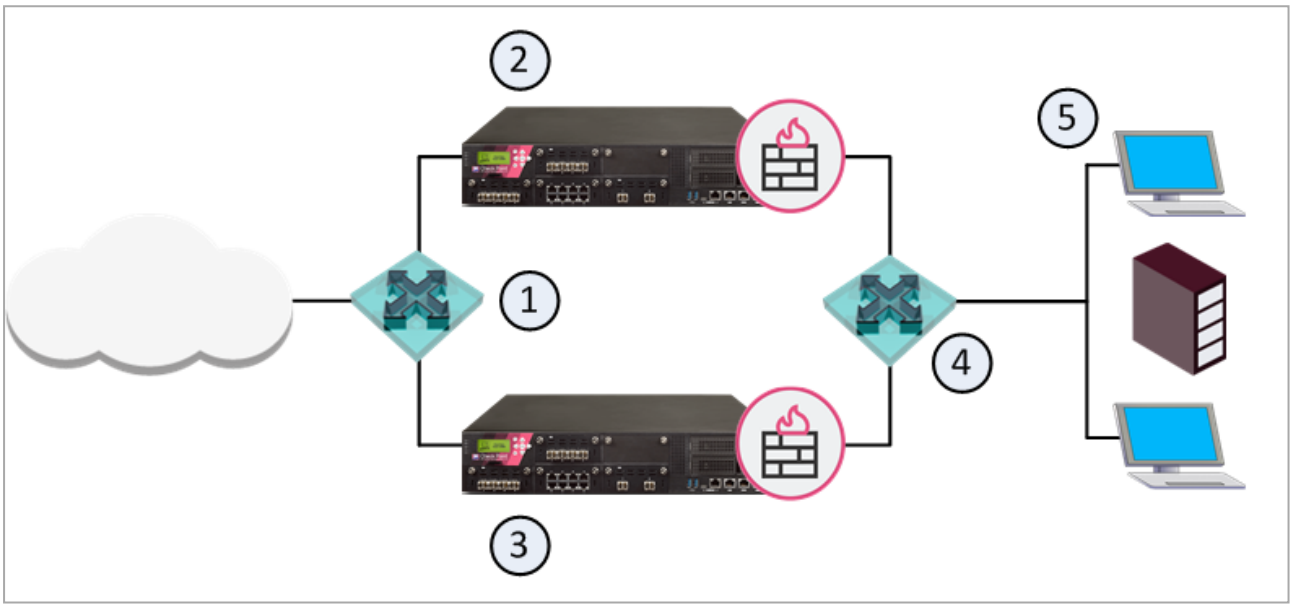
### VRRP Use Case 2 - Internal and External Network High Availability

This use case shows an example of an environment, where there is redundancy for internal and external connections.

Here, you can use Virtual Routers for the two Security Gateways - for internal and for external connections.

The internal and external interfaces must be on different subnets.

Configure one Security Gateway as the VRRP Master and one Security Gateway as the VRRP Backup.




| Item | Description |
|---|---|
| 1 | Virtual Router VRID 5 - External Virtual IP Address (Backup Address) is 192.168.2.5 |
| 2 | VRRP Master Security Gateway |
| 3 | VRRP Backup Security Gateway |
| 4 | Virtual Router VRID 5 - Internal Virtual IP Address (Backup Address) is 192.168.3.5 |
| 5 | Internal network and hosts |

### VRRP Use Case 3 - Internal Network Load Sharing

This use case shows an example of an Active/Active Load Sharing environment for internal network traffic.

This environment gives load balancing, as well as full redundancy.

This configuration is supported with ClusterXL disabled. Only Static Routes are supported.

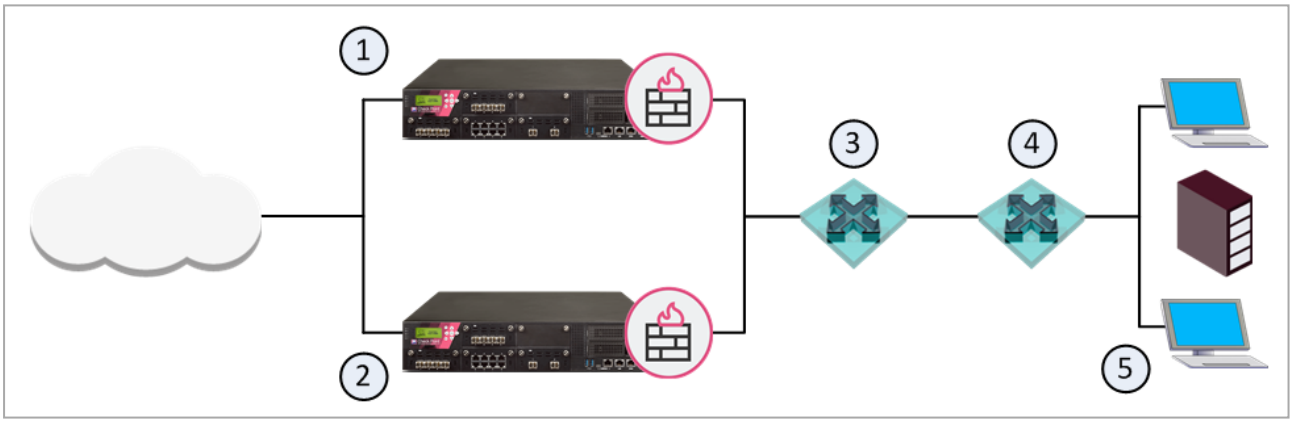
The monitoring of the Check Point Firewall by VRRP must be disabled (it is enabled by default).

A maximum of two VRIDs is supported per interface.

Security Gateway 1 is the VRRP Master for VRID 5, and Security Gateway 2 is the VRRP Backup.

Security Gateway 2 is the VRRP Master for VRID 7, and Security Gateway 1 is the VRRP Backup.

The two Security Gateways are configured to back each other up. If one fails, the other takes over its VRID and IP addresses.




| Item | Description |
|---|---|
| 1 | VRRP Master Security Gateway for VRID 5 and VRRP Backup for VRID 7 |
| 2 | VRRP Backup Security Gateway for VRID 5 and VRRP Master for VRID7 |
| 3 | Virtual Router, VRID 5 Virtual IP Address (Backup Address) is 192.168.2.5 |
| 4 | Virtual Router, VRID 7 Virtual IP Address (Backup Address) is 192.168.2.7 |
| 5 | Internal network and hosts |

# Preparing a VRRP Cluster

*In This Section:*



**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-2521).

## Configuring Network Switches

**Recommendations**

**Best Practice** - If you use the Spanning Tree protocol on Cisco switches connected to Check Point VRRP clusters, we recommend that you enable PortFast. It sets interfaces to the Spanning Tree forwarding state, which prevents them from waiting for the standard forward-time interval.

If you use switches from a different vendor, we recommend that you use the equivalent feature for that vendor. If you use the Spanning Tree protocol without PortFast, or its equivalent, you may see delays during VRRP failover.

## Preparing VRRP Cluster Members

**Procedure**

| Step | Instructions |
|---|---|
| 1 | Install the VRRP Cluster Members<br>See the *R82 Installation and Upgrade Guide* > Chapter *Installing a ClusterXL, VSX Cluster, VRRP Cluster* > Section *Installing a VRRP Cluster*.. |
| 2 | Synchronize the system time on the VRRP Cluster Members.<br>**Best Practice** - Enable NTP (Network Time Protocol) on all Security Gateways (see *"Time" on page 314*).<br>You can also manually change the time and time zone on each Security Gateway to match the other members.<br>In this case, you must synchronize member times to within a few seconds. |
| 3 | **Optional:** Add host names and IP address pairs to the host table on each Security Gateway (see *"Hosts" on page 255*).<br>This lets you use host names as an alternative to IP addresses or DNS servers. |

| Step | Instructions |
|---|---|
| 4 | Enable Virtual Routers:<br>a. With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`).<br>b. In the navigation tree, click **High Availability > VRRP**.<br>c. Configure the VRRP Global Settings.<br>See the section "**Configuring Global Settings for VRRP**" below.<br>d. If the **Disable All Virtual Routers** option is currently selected, clear it.<br>e. Click **Apply Global Settings**. |
| 5 | Configure your Virtual Routers in either Gaia Portal, or Gaia Clish.<br>See:<br>■ *"Configuring Monitored Circuit/Simplified VRRP" on page 582*<br>■ *"Configuring Advanced VRRP" on page 591* |

# Configuring Global Settings for VRRP

This section shows you how to configure the global settings that apply to all Virtual Routers.

**Procedure**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click one of these:<br>■ **High Availability > VRRP**.<br>■ **High Availability >Advanced VRRP**. |

| Step | Instructions |
|---|---|
| 2 | In the **VRRP Global Settings** section:<br>■ **Cold Start Delay** - Configures the delay period in seconds before a Security Gateway joins a Virtual Router. Default = 0.<br>■ **Interface Delay** - Configure this when the Preempt Mode of VRRP was turned off. This is useful when the VRRP node with a higher priority is rebooted, but must not preempt the existing VRRP Master that is handling the traffic, but is configured with a lower priority. Sometimes interfaces that come up take longer than the VRRP timeout to process incoming VRRP Hello packets. The *Interface Delay* extends the time that VRRP waits to receive Hello packets from the existing VRRP Master.<br>■ **Disable All Virtual Routers** - Select this option to disable all Virtual Routers defined on this Gaia system. Clear this option to enable all Virtual Routers. By default, all Virtual Routers are enabled.<br>■ **Monitor Firewall State** - Select this option to let VRRP monitor the Security Gateway and automatically take appropriate action. This is enabled by default, which is the recommended setting when using VRRP with ClusterXL enabled. This must be disabled when using VRRP with ClusterXL disabled.<br>**Important** - If you disable **Monitor Firewall State**, VRRP can assign VRRP Master status to a Security Gateway before it completes the boot process. This can cause more than one Security Gateway in a Virtual Router to have VRRP Master status. |
| 3 | Click **Apply Global Settings**. |

**Notes**

Gaia starts to monitor the Firewall after the cold start delay completes.

This can cause some problems:

- If all the interfaces in a Virtual Router fail, all VRRP Cluster Members become VRRP Backups.

  None of the VRRP Cluster Members can become the VRRP Master and no traffic is allowed.

- If you change the time on any of the VRRP Cluster Members, a VRRP failover occurs automatically.

- In certain situations, installing a policy causes a failover.

  This can happen if it takes a long time to install the policy.

# Configuring Monitored Circuit/Simplified VRRP

*In This Section:*



**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-2521).

This section includes the procedure for configuring Monitored Circuit/Simplified VRRP.

## Configuring Monitored Circuit/Simplified VRRP in Gaia Portal

**Procedure**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **High Availability > VRRP**. |
| 2 | Configure the **VRRP Global Settings**.<br>See *"Preparing a VRRP Cluster" on page 579*. |
| 3 | In the **Virtual Routers** section, click **Add**. |

| Step | Instructions |
|---|---|
| 4 | In the **Add Virtual Router** window, configure these parameters:<br>■ **Virtual Router ID** - Enter a unique ID number for this virtual router. The range of valid values is 1 to 255.<br>■ **Priority** - Enter the priority value, which selects the Security Gateway that takes over in the event of a failure. The Security Gateway with the highest available priority becomes the new VRRP Master. The range of valid values 1 to 254. The default value is 100.<br>■ **Hello Interval** - Optional. Enter or select the number of seconds, after which the VRRP Master sends its VRRP advertisements. The valid range is between 1 (default) and 255 seconds.<br>All VRRP routers on a Security Gateways must be configured with the same hello interval. Otherwise, more than one Security Gateway can be in the VRRP Master state.<br>The Hello interval also defines the failover interval (the time a VRRP Backup router waits to hear from the existing VRRP Master before it takes on the VRRP Master role). The value of the failover interval is three times the value of the Hello interval (default - 3 seconds).<br>■ **Authentication:**<br>• **None** - To disable authentication of VRRP packets<br>• **Simple** - To authenticate VRRP packets using a plain-text password<br>You must use the same authentication method for all Security Gateways in a Virtual Router.<br>■ **Priority Delta** - Enter the value to subtract from the **Priority** to create an effective priority when an interface fails. The range is 1-254.<br>If an interface fails on the VRRP Backup, the value of the priority delta is subtracted from its priority. This gives a higher effective priority to another Security Gateway member.<br>If the effective priority of the current VRRP Master is less than that of the VRRP Backup, the VRRP Backup becomes the VRRP Master for this Virtual Router. If the effective priority for the current VRRP Master and VRRP Backup are the same, the gateway with the highest IP address becomes the VRRP Master.<br>■ **Auto-deactivation** - When an interface is reported as DOWN, a cluster member's Priority value is reduced by the configured Priority Delta amount. If another cluster member exists with a higher Priority, it will then take over as VRRP Master to heal the network.<br>By default, some Cluster Member is elected as VRRP Master, even if all Cluster Members have issues and are reporting a Priority of zero.<br>The auto-deactivation option can be enabled to change this behavior and ensure that no Cluster Member is elected as VRRP Master, if all Cluster Members have a Priority of zero. |

| Step | Instructions |
|---|---|
| | When this option is enabled, Priority Delta should be set equal to the Priority value, so that Priority becomes zero, if an interface goes down. |
| 5 | In the **Backup Addresses** section, click **Add**.<br>Configure these parameters in the **Add Backup Address** window:<br>■ **IPv4 address** - Enter the interface IPv4 address.<br>■ **VMAC Mode** - For each Virtual Router, a Virtual MAC (VMAC) address is assigned to the Virtual IP address. The VMAC address is included in all VRRP packets as the source MAC address. The physical MAC address is not used.<br>Select one of these Virtual MAC modes:<br>• **VRRP** - Sets the VMAC to use the standard VRRP protocol. It is automatically set to the same value on all Security Gateways in the Virtual Router. This is the default setting.<br>• **Interface** - Sets the VMAC to the local interface MAC address. If you define this mode for the VRRP Master and the VRRP Backup, the VMAC is different for each. VRRP IP addresses are related to different VMACs. This is because they are dependent on the physical interface MAC address of the currently defined VRRP Master.<br>**Note** -If you configure different VMACs on the VRRP Master and VRRP Backup, you must make sure that you select the correct proxy ARP setting for NAT.<br>• **Static** - Manually set the VMAC address. Enter the VMAC address in the applicable field.<br>• **Extended** - Gaia dynamically calculates and adds three bytes to the interface MAC address to generate VMAC address that is more random. If you select this mode, Gaia constructs the same MAC address for VRRP Master and VRRP Backups in the Virtual Router.<br>**Note** - If you set the VMAC mode to **Interface** or **Static**, syslog error messages show when you restart the computer, or during VRRP failover. This is caused by duplicate IP addresses for the VRRP Master and VRRP Backup. This is expected behavior because the VRRP Master and VRRP Backups temporarily use the same Virtual IP address until they get to the VRRP Master and VRRP Backup statuses.<br>Click **OK**.<br>The new VMAC mode shows in the in the **Backup Address** table. |
| 6 | To remove a Backup Address, select an address and click **Delete**.<br>The address is removed from the **Backup Address** table. |

| Step | Instructions |
|---|---|
| 7 | Click **Save**. |

# Configuring Monitored Circuit/Simplified VRRP in Gaia Clish

## Syntax

### Adding the Monitored Circuit/Simplified VRRP

1. Configure the priority:

```
add mcvr vrid VALUE priority VALUE priority-delta VALUE
[authtype {none | simple VALUE} hello-interval VALUE
```

2. Configure the backup address:

```
add mcvr vrid VALUE backup-address VALUE vmac-mode VALUE
```

### Configuring the Monitored Circuit/Simplified VRRP

```
set mcvr vrid VALUE
      authtype {none | simple VALUE}
      auto-deactivation {on | off}
      backup-address VALUE vmac-mode VALUE [static-mac VALUE]
      hello-interval VALUE
      preempt-mode {on | off}
      priority VALUE
      priority-delta VALUE
```

### Viewing the Monitored Circuit/Simplified VRRP configuration

```
show mcvr
      vrid VALUE
            all
            authtype
            backup-address VALUE
            backup-addresses
            hello-interval
            priority
            priority-delta
      vrids
```

### Deleting the Monitored Circuit/Simplified VRRP

```
delete mcvr vrid VALUE [backup-address VALUE]
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Parameters

#### CLI Parameters

| Parameter | Description |
|---|---|
| `vrid` *VALUE* | Configures the Virtual Router ID.<br>■ **Range:** 1 - 255<br>■ **Default:** No default value |
| `authtype {none \| simple` *VALUE*`}` | Configures authentication for the given Virtual Router.<br>You must use the same authentication method for all Security Gateways in a Virtual Router.<br>■ **Range:**<br>• `none` - Disables authentication<br>• `simple <`*plain-text password*`>` - Authenticates VRRP packets using a plain-text password<br>■ **Default:** No default value |
| `auto-deactivation {on \| off}` | When an interface is reported as DOWN, a cluster member's Priority value is reduced by the configured Priority Delta amount. If another cluster member exists with a higher Priority, it will then take over as VRRP Master to heal the network.<br>By default, some cluster member will be elected as VRRP Master, even if all cluster members have issues and are reporting a Priority of zero.<br>The auto-deactivation option can be enabled to change this behavior and ensure that no cluster member is elected as VRRP Master, if all cluster members have a Priority of zero.<br>When this option is enabled (on), Priority Delta should be set equal to the Priority value, so that Priority will become zero, if an interface goes down.<br>■ **Range:** `on`, or `off`<br>■ **Default:** `off` |
| `backup-address` *VALUE* | Configures the IPv4 address of the VRRP Backup Security Gateway.<br>You can define more than one address for a Virtual Router.<br>The backup address (Virtual IP Address) is the IP address that VRRP backs up, in order to improve network reliability. The Virtual IP Address is typically used as the default gateway for hosts on that network. VRRP ensures this IP address remains reachable, as long as at least one physical machine in the VRRP cluster is functioning and can be elected as the VRRP Master. |

| Parameter | Description |
|---|---|
| `vmac-mode {default-vmac \| extended-vmac \| interface-vmac \| static-vmac` *VALUE*`}` | Configures how the Virtual MAC (VMAC) address is calculated for the given Virtual IP Address.<br>Each Virtual IP Address for a Virtual Router implies the existence of a virtual network interface.<br>■ **Range:**<br>• `default-vmac` - Generates the VMAC using the standard method described in Section 7.3 of RFC 3768.<br>• `extended-vmac` - Generates the VMAC using an extended range of uniqueness by dynamically calculating 3 bytes of the VMAC instead of only 1.<br>• `interface-vmac` - Configures the VMAC to use the interface hardware MAC address.<br>• `static-vmac <`*VALUE*`>` - Configures the Virtual Router to use a specified static VMAC address.<br>■ **Default:** `default-vmac`<br>**Note** - If you set the VMAC mode to "`interface-vmac`" or "`static-vmac`", syslog error messages show when you restart the computer, or during VRRP failover. This is caused by duplicate IP addresses for the VRRP Master and VRRP Backup. This is expected behavior because the VRRP Master and VRRP Backups temporarily use the same Virtual IP address until they get to the VRRP Master and VRRP Backup statuses. |
| `hello-interval` *VALUE* | The interval in seconds, at which the VRRP Master sends VRRP advertisements. For a given Virtual Router, all VRRP cluster members should have the same value for Hello Interval.<br>■ **Range:** `default`, or `1 - 255`<br>■ **Default:** `1` |

| Parameter | Description |
|---|---|
| `preempt-mode {on \| off}` | Configures Preempt Mode for the given Virtual Router.<br>When the Preempt Mode is *enabled*, if the Virtual Router has a higher Priority than the current VRRP Master, it preempts the VRRP Master.<br>If the Preempt Mode is *disabled*, all Virtual Routers that have monitored interfaces, are participating to avoid potential split-brain network topology.<br>For more information on the implications of disabling Preempt Mode, see the help text for the "`set mcvr vrid <VALUE> monitor-vrrp`" command.<br>■ **Range:** `on`, or `off`<br>■ **Default:** `off` |
| `priority VALUE` | Configures the Priority to use in the VRRP Master election.<br>This is the maximum priority that can be achieved when all monitored interfaces are up.<br>The VRRP cluster member with the highest Priority value will be elected as the VRRP Master. Each cluster member should be given a different Priority value, such that a specific member is the preferred VRRP Master. This will ensure consistency in the outcome of the election process.<br>■ **Range:** `default`, or `1 - 254`<br>■ **Default:** `100` |
| `priority-delta VALUE` | Updates the Priority Delta of the given Virtual Router.<br>For a given Virtual Router, the VRRP cluster member with the highest Priority is elected as the VRRP Master. For each monitored interface with a status of DOWN, the Priority Delta value is subtracted from the Virtual Router's overall Priority. Thus, the VRRP Master will be the Virtual Router having the best list of working interfaces.<br>The Priority Delta value should be selected such that the Priority value will not become a negative number when the Priority Delta is subtracted from it for each non-operational interface.<br>■ **Range:** `default`, or `1 - 254`<br>■ **Default:** No default value |

# Configuring the VRRP Cluster for Simplified VRRP in SmartConsole

Follow the *R82 Installation and Upgrade Guide* > Chapter *Installing a ClusterXL, VSX Cluster, VRRP Cluster* > Section *Installing a VRRP Cluster*.

# Configuring Advanced VRRP

*In This Section:*



**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-2521).

Advanced VRRP lets you configure Virtual Routers at the interface level.

This section contains only those procedures that are directly related to Advanced VRRP configuration.

The general procedures for configuring VRRP clusters are described in *"Configuring Monitored Circuit/Simplified VRRP" on page 582*.

With Advanced VRRP, you must configure every Virtual Router to monitor every configured VRRP interface.

## Changing from Advanced VRRP to Monitored Circuit/Simplified VRRP

**Procedure**

| Step | Instructions |
|---|---|
| 1 | Delete all existing Virtual Routers. |
| 2 | Create new Virtual Routers in accordance with the procedures. |

You cannot move a Backup Address from one interface to another while a Security Gateway is a VRRP Master.

Perform these steps to delete and add new interfaces with the necessary IP addresses:

| Step | Instructions |
|---|---|
| 1 | Cause a failover from the VRRP Master to the VRRP Backup. |
| 2 | Reduce the priority, or disconnect an interface. |

| Step | Instructions |
|---|---|
| 3 | Delete the Virtual Router on the interface. |
| 4 | Create new Virtual Router using the new IP address. |
| 5 | Configure the Virtual Router as before. |

# Configuring Advanced VRRP in Gaia Portal

**Procedure**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **High Availability >Advanced VRRP**. |
| 2 | Configure the VRRP Global Settings (see *"Preparing a VRRP Cluster" on page 579*). |
| 3 | In the **Virtual Routers** section, click **Add**. |
| 4 | In the **Add New Virtual Router** window, configure these parameters: |
| | ■ **Interface** - Select the interface for the Virtual Router. |
| | ■ **Virtual Router ID** - Enter or select the ID number of the Virtual Router. |
| | ■ **Priority** - Enter or select the priority value.<br>The priority value determines, which router takes over in the event of a failure. The router with the higher priority becomes the new VRRP Master. The range of values for priority is 1 to 254. The default value is 100. |
| | ■ **Hello Interval** - Enter or select the number of seconds, at which the VRRP Master sends VRRP advertisements.<br>The range is 1 to 255 seconds. The default value is 1.<br>All nodes of a given Virtual Router must have the same hello Interval. If not, VRRP discards the packet and both platforms go to VRRP Master state.<br>The VRRP Hello interval also determines the failover interval - how long it takes a VRRP Backup router to take over from a failed VRRP Master. If the VRRP Master misses three VRRP Hello advertisements, it is considered to be down, because the minimum VRRP Hello interval is 1 second. Therefore, the minimum failover time is 3 seconds (3 * Hello Interval). |

| Step | Instructions |
|---|---|
| | ■ **Preempt Mode** - If you keep it selected (the default), when the original VRRP Master fails, a VRRP Backup system becomes the acting VRRP Master. When the original VRRP Master returns to service, it becomes VRRP Master again.<br>If you clear it, when the original VRRP Master fails, a VRRP Backup system becomes the acting VRRP Master, and the original does not become VRRP Master again when it returns to service. |
| | ■ **Auto-deactivation** - If you clear it (the default), a Virtual Router with the lowest priority available (1) can become VRRP Master, if no other Security Gateways exist on the network.<br>If you selected it, the effective priority can become 0. With this priority, the Virtual Router does not become the VRRP Master, even if there are no other Security Gateways on the network.<br>If you selected it, you should also configure the **Priority** and **Priority Delta** values to be equal, so that the effective priority becomes 0, if there is a VRRP failure. |

| Step | Instructions |
|---|---|
| | ■ **VMAC Mode** - For each Virtual Router, a Virtual MAC (VMAC) address is assigned to the Virtual IP address. The VMAC address is included in all VRRP packets as the source MAC address. The physical MAC address is not used.<br>Select the mode:<br>• **VRRP** - Sets the VMAC to use the standard VRRP protocol. It is automatically set to the same value on all Security Gateways in the Virtual Router. This is the default setting.<br>• **Interface** - Sets the VMAC to the local interface MAC address. If you define this mode for the VRRP Master and the VRRP Backup, the VMAC is different for each. VRRP IP addresses are related to different VMACs. This is because they are dependent on the physical interface MAC address of the currently defined VRRP Master.<br>**Note** - If you configure different VMACs on the VRRP Master and VRRP Backup, you must make sure that you select the correct proxy ARP setting for NAT.<br>• **Static** - Manually set the VMAC address. Enter the VMAC address in the applicable field.<br>• **Extended** - Gaia dynamically calculates and adds three bytes to the interface MAC address to generate VMAC address that is more random. If you select this mode, Gaia constructs the same MAC address for VRRP Master and VRRP Backups in the Virtual Router.<br>**Note** - If you set the VMAC mode to **Interface** or **Static**, syslog error messages show when you restart the computer, or during VRRP failover. This is caused by duplicate IP addresses for the VRRP Master and VRRP Backup. This is expected behavior because the VRRP Master and VRRP Backups temporarily use the same Virtual IP address until they get to the VRRP Master and VRRP Backup statuses. |
| | ■ **Authentication**:<br>• **None** - To disable authentication of VRRP packets.<br>• **Simple** - To authenticate VRRP packets using a plain-text password.<br>You must use the same authentication method for all Security Gateways in a Virtual Router. |

| Step | Instructions |
|---|---|
| 5 | In the **Backup Addresses** section:<br>a. Click **Add**.<br>b. In the **IPv4 address** field, enter the IPv4 address.<br>c. Click **OK**.<br>To change a Backup Address, select a Backup IP address and click **Edit**.<br>To remove a Backup Address, select a Backup IP address and click **Delete**. |
| 6 | In the **Monitored Interfaces** section:<br>a. Click **Add**.<br>Gaia shows a warning that adding a Monitored Interface will lock the Interface for this Virtual Router.<br>b. Click **OK** to confirm.<br>c. In the **Interface** field, select the interface.<br>d. In **Priority Delta** field, enter or select the number to subtract from the priority.<br>This creates an effective priority when an interface related to the VRRP Backup fails.<br>The range is 1-254.<br>e. Click **OK**.<br>To change a Monitored Interface, select a Monitored Interface and click **Edit**.<br>To remove a Monitored Interface, select a Monitored Interface and click **Delete**. |
| 7 | Click **Save**. |

# Configuring Advanced VRRP in Gaia Clish

## Syntax

### Configuring Advanced VRRP

```
set vrrp
      accept-connections {on | off}
      coldstart-delay VALUE
      disable-all-virtual-routers {on | off}
      monitor-firewall {on | off}
      interface-delay VALUE
```

### Configuring an Advanced VRRP interface

```
set vrrp interface VALUE
      authtype
            none
            simple VALUE
      monitored-circuit vrid VALUE
            auto-deactivation {on | off}
            backup-address VALUE {on | off}
            hello-interval VALUE
            monitored-interface VALUE
                  on
                  off
                  priority-delta <default | 1 - 254>}
            off
            on
            preempt-mode {on | off}
            priority VALUE
            vmac-mode
                  default-vmac
                  extended-vmac
                  interface-vmac
                  static-vmac VALUE
      off
      virtual-router legacy off
```

### Viewing the Advanced VRRP configuration

```
show vrrp
      [interface VALUE]
      [interfaces]
      [stats]
      [summary]
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Parameters

#### CLI Parameters

| Parameter | Description |
|---|---|
| `accept-connections {on \| off}` | Controls the **Accept Connections** option.<br>This option causes packets destined to VRRP Virtual IP Address(es) to be accepted, and any required responses be generated.<br>Enabling this option enhances VRRP's interaction with network management tools, which in turn allows for faster failure detection.<br>This option is required for High Availability applications (for example, routing protocols), whose service is tied to a Virtual IP Address.<br>■ **Range:** `on`, or `off`<br>■ **Default:** `off` |
| `coldstart-delay <VALUE>` | Specifies the number of seconds to wait after a system cold start before VRRP becomes active, and this cluster member can be elected as VRRP Master.<br>■ **Range:** 0 - 3600<br>■ **Default:** 0 |
| `disable-all-virtual-routers {on \| off}` | Enables or disables all IPv4 VRRP Virtual Routers.<br>If disabled, the VRRP configuration is preserved and can be enabled again.<br>■ **Range:** `on`, or `off`<br>■ **Default:** `off` |
| `monitor-firewall {on \| off}` | Enables or disables VRRP monitoring of the Security Gateway state.<br>If this option is enabled, and the Firewall is not ready, the cluster member will refuse to be the VRRP Master.<br>■ **Range:** `on`, or `off`<br>■ **Default:** `on` |

| Parameter | Description |
|---|---|
| `interface-delay <VALUE>` | The Interface Delay controls how long to wait (in seconds) after receiving an interface UP notification before VRRP assesses whether or not the related VRRP cluster member should increase its priority, and possibly become the new VRRP Master. The delay ensures that VRRP does not attempt to respond to interfaces, which are only momentarily active.<br>Note - Same value should be configured for both VRRPv2 and VRRPv3 if both protocols are configured.<br>■ **Range:** 0 - 3600<br>■ **Default:** 0 |
| `interface VALUE` | The name of the interface, on which to enable the VRRP. |
| `authtype {none \| simple VALUE}` | Configures authentication for the given Virtual Router.<br>You must use the same authentication method for all Security Gateways in a Virtual Router.<br>■ **Range:**<br>• `none` - Disables authentication<br>• `simple <plain-text password>` - Authenticates VRRP packets using a plain-text password<br>■ **Default:** No default value |
| `monitored-circuit vrid <VALUE>` | Configures the Virtual Router ID.<br>■ **Range:** 1 - 255<br>■ **Default:** No default value |

| Parameter | Description |
|---|---|
| `monitored-circuit vrid` *VALUE* `auto-deactivation {on \| off}` | When an interface is reported as DOWN, a cluster member's Priority value is reduced by the configured Priority Delta amount. If another cluster member exists with a higher Priority, it will then take over as VRRP Master to heal the network.<br>By default, some cluster member will be elected as VRRP Master, even if all cluster members have issues and are reporting a Priority of zero.<br>The auto-deactivation option can be enabled to change this behavior and ensure that no cluster member is elected as VRRP Master, if all cluster members have a Priority of zero. When this option is enabled (on), Priority Delta should be set equal to the Priority value, so that Priority will become zero, if an interface goes down.<br>■ **Range:** `on`, or `off`<br>■ **Default:** `off` |
| `monitored-circuit vrid` *VALUE* `backup-address` *VALUE* `{on \| off}` | Configures the IPv4 address of the VRRP Backup Security Gateway.<br>You can define more than one address for a Virtual Router.<br>The backup address (Virtual IP Address) is the IP address that VRRP backs up, in order to improve network reliability. The Virtual IP Address is typically used as the default gateway for hosts on that network. VRRP ensures this IP address remains reachable, as long as at least one physical machine in the VRRP cluster is functioning and can be elected as the VRRP Master. |
| `monitored-circuit vrid` *VALUE* `hello-interval` *VALUE* | The interval in seconds, at which the VRRP Master sends VRRP advertisements. For a given Virtual Router, all VRRP cluster members should have the same value for Hello Interval.<br>■ **Range:** `default`, or `1 - 255`<br>■ **Default:** `1` |

| Parameter | Description |
|---|---|
| `monitored-interface` *VALUE* `{on \| off \| priority-delta <default \| 1 - 254>}` | Configures the list of monitored interfaces names for the given Virtual Router.<br>■ `on` - Creates a VRRP Virtual Router<br>■ `off` - Removes a VRRP Virtual Router<br>■ `priority-delta` - Configures the Priority Delta value<br>When an interface fails, VRRP causes the backup cluster member to take over for that interface. The VRRP interface should also fail over when a different interface fails (if traffic is routed between the interfaces).<br>Otherwise, network destinations will become unreachable, etc. This coordinated failover is achieved by adding all dependent interfaces to the list of monitored interfaces.<br>The relative importance of each monitored interface is expressed by its Priority Delta value. More important interfaces should have higher Priority Deltas. Priority Delta causes the correct failover decision, if both cluster members are experiencing failures on different interfaces.<br>Refer to the following commands for additional details:<br>■ `set vrrp interface <`*VALUE*`> monitored-circuit vrid <`*VALUE*`> priority`<br>■ `set vrrp interface <`*VALUE*`> monitored-circuit vrid <`*VALUE*`> monitored-interface <`*VALUE*`> priority-delta` |
| `monitored-circuit vrid` *VALUE* `{on \| off}` | Creates (`on`) or removes (`off`) a VRRP Virtual Router. |
| `monitored-circuit vrid` *VALUE* `preempt-mode {on \| off}` | Configures Preempt Mode for the given Virtual Router.<br>When Preempt Mode is enabled, if the Virtual Router has a higher Priority than the current VRRP Master, it preempts the VRRP Master.<br>If Preempt Mode is disabled, all Virtual Routers that have monitored interfaces, are participating to avoid potential split-brain network topology.<br>For more information on the implications of disabling Preempt Mode, see the help text for the `set mcvr vrid <VALUE> monitor-vrrp` command.<br>■ **Range:** `on`, or `off`<br>■ **Default:** `off` |

| Parameter | Description |
|---|---|
| `monitored-circuit vrid VALUE priority VALUE` | Configures the Priority to use in the VRRP Master election. This is the maximum priority that can be achieved when all monitored interfaces are up.<br>The VRRP cluster member with the highest Priority value will be elected as the VRRP Master. Each cluster member should be given a different Priority value, such that a specific member is the preferred VRRP Master. This will ensure consistency in the outcome of the election process.<br>■ **Range:** `default`, or `1 - 254`<br>■ **Default:** `100` |
| `monitored-circuit vrid VALUE vmac-mode {default-vmac \| extended-vmac \| interface-vmac \| static-vmac VALUE}` | Configures how the Virtual MAC (VMAC) address is calculated for the given Virtual IP Address.<br>Each Virtual IP Address for a Virtual Router implies the existence of a virtual network interface.<br>■ **Range:**<br>• `default-vmac` - Generates the VMAC using the standard method described in Section 7.3 of RFC 3768.<br>• `extended-vmac` - Generates the VMAC using an extended range of uniqueness by dynamically calculating 3 bytes of the VMAC instead of only 1.<br>• `interface-vmac` - Configures the VMAC to use the interface hardware MAC address.<br>• `static-vmac <VALUE>` - Configures the Virtual Router to use a specified static VMAC address.<br>■ **Default:** `default-vmac` |
| `set vrrp interface VALUE off` | Deletes all Virtual Routers from the interface. |
| `set virtual-router legacy off` | Disables legacy VRRPv2 configuration.<br>Legacy Virtual Router configuration may exist due to an upgrade from an older IPSO OS configuration. For reference purposes, these settings may be preserved after upgrade, but are not supported.<br>Hence, you must replace all legacy "`virtual-router`" configuration commands using the equivalent "`monitored-circuit`" configuration commands. |

# Configuring the VRRP Cluster for Advanced VRRP in SmartConsole

Follow the *R82 Installation and Upgrade Guide* > Chapter *Installing a ClusterXL, VSX Cluster, VRRP Cluster* > Section *Installing a VRRP Cluster*.

# Troubleshooting VRRP

*In This Section:*



**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-2521).

This section shows known issues with VRRP configurations and fixes.

Read this section before contacting *Check Point Support*.

## Traces (Debug) for VRRP

You can log information about errors and events for troubleshooting VRRP.

**Enabling traces for VRRP**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Routing** > **Routing Options**. |
| 2 | In the **Trace Options** section, in the **Filter Visible Tables Below** drop down list, select **VRRP**. |
| 3 | In the **VRRP** table, select the applicable options.<br>We recommend you select **All**.<br>To select several specific options:<br>a. Press and hold the **CTRL** key on the keyboard.<br>b. Left-click on the applicable options. The selected options become highlighted.<br>To select several consecutive options:<br>a. Left-click on the first consecutive applicable option.<br>b. Press and hold the **SHIFT** key on the keyboard.<br>c. Left-click on the last consecutive applicable option. The selected options become highlighted. |

| Step | Instructions |
|---|---|
| 4 | Click **Add**.<br>The selected options show **Enabled**. |
| 5 | Scroll to the top of this page. |
| 6 | In the **Routing Options** section, click **Apply**.<br>The Gaia restarts the routing subsystem and signals it to reread its configuration.<br>The debug information is saved in **/var/log/routed.log*** files and **/var/log/routed_messages*** files.<br>**Note** - As an *example*, see sk84520 - How to debug OSPF and RouteD daemon on Gaia. |

**Disabling traces for VRRP**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Routing** > **Routing Options**. |
| 2 | In the **Trace Options** section, in the **Filter Visible Tables Below** drop down list, select **VRRP**.<br>In the **VRRP** table, select **All**. |
| 3 | Click **Remove**.<br>The options do not show **Enabled** anymore. |
| 4 | Scroll to the top of this page. |
| 5 | In the **Routing Options** section, click **Apply**.<br>The Gaia restarts the routing subsystem and signals it to reread its configuration. |

# General Configuration Considerations

If VRRP failover does not occur as expected, make sure that the configuration of these items.

- All Security Gateways in a Virtual Router must have the same system times. The simplest method to synchronize times is to enable NTP on all Security Gateways of the Virtual Router. You can also manually change the time and time zone on each Security Gateway to match the other Security Gateways. It must be no more than seconds apart.
- All routers of a Virtual Router must have the same VRRP Hello Interval.
- The Priority Delta must be sufficiently large for the Effective Priority to be lower than the VRRP Master router. Otherwise, when you pull an interface for a Monitored-Circuit VRRP test, other interfaces do not release IP addresses.
- Each unique Virtual Router ID must be configured with the same Backup Address on each Security Gateway.
- The VRRP monitor in the Gaia Portal might show one of the interfaces in *initialize* state. This might suggest that the IP address used as the Backup Address on that interface is invalid or reserved.
- An SNMP "Get" request on interfaces may list the incorrect IP addresses. This results in incorrect policy. An SNMP "Get" request fetches the lowest IP address for each interface. If interfaces are created when the Security Gateway is the VRRP Master, the incorrect IP address might be included. Repair this problem. Edit the interfaces by hand, if necessary.

# Firewall Policies

Configure the Access Control Policy to accept VRRP packets to and from the Gaia platform. The multicast destination assigned by the IANA for VRRP is 224.0.0.18. If the Access Control Policy does not accept packets sent to 224.0.0.18, Security Gateways in one Virtual Router take on VRRP Master state.

# Monitored-Circuit VRRP in Switched Environments

With Monitored-Circuit VRRP, some Ethernet switches might not recognize the VRRP MAC address after a change from VRRP Master to VRRP Backup. This is because many switches cache the MAC address related to the Ethernet device attached to a port. When failover to a VRRP Backup router occurs, the Virtual Router MAC address becomes associated with a different switch port. Switches that cache the MAC address might not change the associated cached MAC address to the new port during a VRRP change.

To repair this problem, you can take one of these actions

1. Replace the switch with a hub.
2. Disable MAC address caching on the switch, or switch ports, to which the VRRP cluster members are connected.

It might be not possible to disable the MAC address caching. If so, set the address aging value sufficiently low that the MAC addresses age out after a one second or two seconds. This causes more overhead on the switch. Therefore, find out if this is a viable option for your switch model.

The Spanning Tree Protocol (STP) prevents Layer 2 loops across multiple bridges. Spanning-Tree can be enabled on the ports connected to the two sides of a VRRP cluster. It can also "see" multicast VRRP Hello packets coming for the same MAC address on two different ports. When the two occur, it can suggest a loop, and the switch blocks traffic on one port. If a port is blocked, the VRRP cluster members cannot get VRRP Hello packets from each other. As a result, both VRRP cluster members enter the VRRP Master state.

If possible, turn off Spanning-Tree on the switch to resolve this issue. However, this can have harmful effects, if the switch is involved in a bridging loop. If you cannot disable Spanning-Tree, enable PortFast on the ports connected to the VRRP cluster members. PortFast causes a port to enter the Spanning-Tree forwarding state immediately, by passing the listening and learning states.

# Maintenance

This chapter includes procedures and reference information for:

- Working with License
- Snapshot Management
- Download of SmartConsole
- Hardware Health Monitoring
- Monitoring RAID Synchronization
- Shut Down and Reboot
- System Backup

# License Status

*In This Section:*



You can view, add, or delete licenses in one of these ways:

- In Gaia Portal > **Maintenance** section > **License Status** page.

  **Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

- With the "`cplic db_add`" and "`cplic del`" commands (see the *R82 CLI Reference Guide*).

  **Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

  **Note** - While all the "`cplic`" commands are available in Gaia, they are not grouped into a Gaia feature.

## On Check Point Appliances

If a Management Server and its managed Security Gateways are *able* to connect to Check Point User Center, licenses and contracts activated and updated automatically.

If a Management Server and its managed Security Gateways are **not** able to connect to Check Point User Center, then manage licenses and contracts in either SmartConsole or the command line.

## On Check Point Maestro

See the *R82 Scalable Platforms Administration Guide* > Chapter *Configuring Security Groups* > Section *License Installation*.

## On Open Servers and Virtual Machines

If a Management Server and its managed Security Gateways are *able* to connect to Check Point User Center, then activate the license during the Gaia First Time Configuration Wizard, or later in Gaia Portal, SmartConsole, or the command line. After the activation is completed, licenses and contracts are updated automatically.

If a Management Server and its managed Security Gateways are **not** able to connect to Check Point User Center, then manage licenses and contracts in either SmartConsole or the command line.

# Activating a License in Gaia Portal

### Activating a license manually online

| Step | Instructions |
|---|---|
| 1 | If this Security Management Server, Domain Management Server, or Security Gateway (or Cluster Members) connects to the Internet through a proxy server, then configure the applicable proxy in SmartConsole:<br>**Note** - The prerequisite for Security Gateways and Cluster Members is to establish a Secure Internal Communication (SIC Trust) with a Management Server.<br>■ To configure the same default proxy for all objects:<br>a. Click **Menu** > **Global properties** > **Proxy**.<br>b. Select **Use proxy server**.<br>c. Enter the proxy server address (Hostname or IP address).<br>d. Enter the proxy server port.<br>e. Click **OK**.<br>f. Publish the SmartConsole session.<br>g. Click **Menu** > **Install database** > select all objects > click **Install**.<br>h. Install the Access Control Policy on all managed Security Gateways and Clusters.<br>■ To configure specific proxy in an object:<br>a. From the left navigation panel, click **Gateways & Servers**.<br>b. Double-click the applicable object.<br>c. From the left tree, click **Network Management** > **Proxy**.<br>d. Select **Use custom proxy settings for this network object**.<br>e. Select **Use proxy server**.<br>f. Enter the proxy server address (Hostname or IP address).<br>g. Enter the proxy server port.<br>h. Click **OK**.<br>i. Publish the SmartConsole session.<br>j. Complete the configuration:<br>• If this object is a Management Server:<br>Click **Menu** > **Install database** > select the Management Server object > click **Install**.<br>• If this object is a Security Gateway or Cluster:<br>Install the Access Control Policy. |
| 2 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`). |
| 3 | In the navigation tree, click **Maintenance** > **License Status**. |

| Step | Instructions |
|---|---|
| 4 | Click **Activate Now**.<br>Gaia fetches the license, and the status changes to **Activated**.<br>The Software Blades enabled by the license appear in the table. |

**Activating a license manually offline**

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`). |
| 2 | In the navigation tree, click **Maintenance** > **License Status**. |
| 3 | Click **Offline Activation**. |
| 4 | Click **New**. |
| 5 | Enter the license data manually, or click **Paste License** to enter the data automatically.<br>The **Paste License** button only appears in Internet Explorer.<br>For other web browsers, paste the license strings into the empty text field. |
| 6 | Click **OK**. |

### Deleting an installed license

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`). |
| 2 | In the navigation tree, click **Maintenance** > **License Status**. |
| 3 | Click **Offline Activation**. |
| 4 | Select the license. |
| 5 | Click **Delete**. |
| 6 | Click **OK**. |

**Note** - To delete a license in the command line, use the "`cplic del`" command (see the *R82 CLI Reference Guide*).

# Snapshot Management

A snapshot is a backup of the system settings and products. It includes:

- File system, with customized files
- System configuration (interfaces, routing, hostname, and similar)
- Software Blades configuration
- Management database (on a Security Management Server or a Multi-Domain Server)

A snapshot is very large. A snapshot includes the entire root partition, part of the `/var/log` partition, and other important files.

For this reason, snapshots cannot be scheduled the same way that Backups can.

Backup and Restore is the preferred method of recovery.

**Notes:**

- When Gaia creates a snapshot, all system processes and services continue to run.
  Policy enforcement is not interrupted.
- You can import a snapshot created on a different software release or on this software release.
  You must import a snapshot on the appliance or open server of the same hardware model, from which it was exported.
- After importing the snapshot, you must activate the device license from the Gaia Portal or the User Center.
- We do not recommend to use snapshots as a way of regularly backing up your system.
  System Backup is the preferred method.
  Schedule system backups on a regular basis, daily or weekly, to preserve the Gaia OS configuration and Firewall database.

**Best Practice for creating snapshots:**

- Immediately after Gaia installation and first time configuration.
- Before making a major system change, such as installing a hotfix or route changes.
- In addition, see *"lightshot" on page 733*.

**Important:**

- After you take the Gaia snapshot, export it to an external storage.
  You must **not** rename the exported image. If you rename a snapshot image, it is not possible to revert to it.
- See sk98068: Gaia Limitations after Snapshot Recovery.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Snapshot operations (in the Global Gaia Portal or Global Gaia Clish).
  To collect or import a Gaia Snapshot in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

# Snapshot Options

| Option | Description |
|---|---|
| **Revert** | Reverts to a user created image.<br>Reverts to a factory default image, which is automatically created on Check Point appliances by the installation or upgrade procedure. |
| **Delete** | Deletes an image from the local file system. |
| **Export** | Exports an existing image.<br>This creates a compressed version of the image.<br>You can download the exported image to a different computer and delete the exported image from the local file system.<br>This saves disk space. |
| **Import** | Imports an exported image. |
| **View** | Shows a list of images that are stored locally. |

**Notes:**

- You must not rename the exported image. If you rename a snapshot image, it is not possible to revert to it.
- You can import a snapshot only on the machine of the same hardware type, from which it was exported.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Snapshot operations (in the Global Gaia Portal or Global Gaia Clish).
  To collect or import a Gaia Snapshot in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

# Snapshot Prerequisites

**Important:**
Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Snapshot operations (in the Global Gaia Portal or Global Gaia Clish).
To collect or import a Gaia Snapshot in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

- We recommended to configure the GRUB password. See *"System Passwords" on page 300*.
- Before you **revert** to a snapshot on a new appliance, or after a reset to factory defaults, you must run the Gaia First Time Configuration Wizard and configure the same settings as before you created the snapshot.
- Before you **create** a new snapshot image, make sure the appliance or storage destination meets these prerequisites:
  - The required free disk space is the size of the system root partition multiplied by 1.15.

    **Note** - A snapshot image is created in unallocated space on the disk. Not all of the unallocated space on a disk can be used for snapshots.
    To find out if you have enough free space for snapshots:

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on the Gaia computer. |
| 2 | Log in to Gaia Clish. |
| 3 | On Scalable Platforms, go to Gaia gClish:<br>Type `gclish` and press Enter. |
| 4 | Run:<br>`show snapshots`<br>The output shows the amount of space on the disk available for snapshots.<br>The value in the output does not represent all of the unallocated space on the disk. |

- The free disk space required in the export file location is the size of the snapshot image multiplied by 2.

  The minimum size of a snapshot image is 2.5GB.

  Therefore, the minimum necessary free disk space in the export file location is 5GB.

# Snapshot Management in Gaia Portal

**Important:**

- On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Snapshot operations (in the Global Gaia Portal or Global Gaia Clish).
  To collect or import a Gaia Snapshot in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

Before you create a snapshot image, make sure the appliance or storage destination meets the prerequisites.

**Creating a new snapshot image**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance > Snapshot Management**. |
| 2 | In the **Snapshot Management** section, click **New**.<br>The **New Image** window opens. |
| 3 | In the **Name** field, enter a name for the image.<br>**Optional:** In the **Description** field, enter a description for the image. |
| 4 | Click **OK**. |

### Exporting an existing snapshot image

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance > Snapshot Management**. |
| 2 | In the **Snapshot Management** section, select a snapshot. |
| 3 | Check the snapshot size. |
| 4 | Make sure that there is enough free disk space in the `/var/log/` partition:<br>a. Connect to the command line on Gaia.<br>b. Log in to the Expert mode.<br>c. Run:<br>`df -kh \| egrep "Mounted\|/var/log"`<br>Check the value in the `Avail` column. |
| 5 | In Gaia Portal, select a snapshot. |
| 6 | Click **Export**.<br>The **Export Image** window opens. |
| 7 | Click **Start Export**. |

**Important** - You must **not** rename the exported image. If you rename a snapshot image, it is not possible to revert to it.

### Importing a snapshot

To use the snapshot on another appliance, it has to be the same type of appliance you used to export the image.

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance > Snapshot Management**. |
| 2 | In the **Snapshot Management** section, click **Import**.<br>The **Import Image** window opens. |
| 3 | Click **Browse** to select the snapshot file for upload. |
| 4 | Click **Upload**. |
| 5 | Click **OK**. |

### Reverting to an existing snapshot image

**Important:**

- Reverting to the selected snapshot overwrites the existing running configuration and settings. Make sure you know credentials of the snapshot, to which you revert.
- Before you **revert** to a snapshot on a new appliance, or after a reset to factory defaults, you must run the Gaia First Time Configuration Wizard and configure the same settings as before you created the snapshot.

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance > Image Management**. |
| 2 | In the **Snapshot Management** section, select a snapshot. |
| 3 | Click **Revert**.<br>The **Revert** window opens.<br>**Important** - Pay close attention to the warnings about overwriting settings, the credentials, and the reboot and the image details. |
| 4 | Click **OK**. |
| 5 | If you reverted a snapshot on a Security Gateway / Cluster Member, install the Security Policy. |

### Deleting a snapshot

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance > Snapshot Management**. |
| 2 | In the **Snapshot Management** section, select a snapshot. |
| 3 | Click **Delete**.<br>The **Delete Image** window opens. |
| 4 | Click **OK**. |

### Scheduled Snapshots

To configure scheduled snapshots in Gaia Clish, see *"Snapshot Management in Gaia Clish - Scheduled Snapshots" on page 632*.

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance > Snapshot Management**.<br>Refer to the **Scheduled Snapshots** section. |
| 2 | Click the **Scheduled Snapshot Settings** button. |
| 3 | Select the **Enable** option to configure a schedule.<br>(Clear the **Enable** option to disable the configured schedule.) |
| 4 | In the **Snapshot name** field, enter the name of the job.<br>The final name of the snapshot consists of two parts - the prefix (you enter in this field) and the time stamp (format is hard-coded):<br>`<Prefix>_<YYYY_MM_DD__HH_mm>`<br>■ The prefix maximum length is 15 characters.<br>■ The prefix can consist only of letters, numbers, or underscore "_".<br>■ Default prefix: `snap`. |
| 5 | **Optional:** In the **Description** field, enter the description of the snapshot image.<br>Default description : `default_snapshot` |
| 6 | In the **Destination** section, configure the location of the backup file:<br>■ **Local LVM**<br>To keep the collected snapshot locally in the `/var/log/CPbackup/backups/` directory.<br>■ **SCP server**<br>To send the collected snapshot to an SCP server.<br>Enter the IP address, User name, Password, and Upload path.<br>**Important:**<br>• First, you must follow sk164234 to configure the SCP server as a trusted host on Gaia.<br>• The username must have permissions to delete files on the SCP server.<br>■ **FTP server**<br>To send the collected snapshot to an FTP server.<br>Enter the IP address, User name, Password, and Upload path.<br>**Important** -The username must have permissions to delete files on the FTP server. |

| Step | Instructions |
|---|---|
| 7 | In the **Recurrence** section, configure the frequency (**Daily**, **Weekly**, **Monthly**, **Minute Interval**, **Hourly**) for this snapshot.<br><br>**Note** - This is available only for the **Local LVM** location. |
| 8 | **Optional:** In the **Retention Policy** section, configure the snapshot retention policy:<br><br>■ In the **Maximum snapshots** field, configure the maximum number of snapshot images to save.<br>If the new snapshot image exceeds this number, then Gaia deletes the oldest snapshot.<br>■ In the **Keep disk-space above (in GB)** field, configure the amount of free disk space to maintain at all times.<br>If the new snapshot image exceeds this number, then Gaia does not create the new snapshot image.<br>■ In the **Minimum snapshots** field, configure the minimum number of snapshot images to save.<br>When Gaia deletes the old snapshots, it always keeps the specified number of snapshot images.<br><br>**Important:**<br><br>■ The retention policy supports only the local LVM volume.<br>■ The retention policy applies only to the new snapshots (and does not apply to existing snapshots).<br>■ If the retention policy fails to calculate the configured criteria, Gaia does not create the new snapshot image.<br>In this case, Gaia does not show a notification.<br>An administrator must manually check why Gaia did not create the new snapshot image. |

| Step | Instructions |
|---|---|
| | The disk space limit you need to configure is:<br>`Limit = (Available free disk space for all snapshot images) - (Free disk space to maintain)`<br>Where:<br>`Available free disk space for all snapshot images = = (Output of: vgdisplay \| grep Free) - 1.1*(Output of: lvs \| egrep "LSize\|lv_current")`<br>**Example**<br>For more information, see sk80260.<br>A. Log in to the Expert mode.<br>B. Get the free disk space in volume groups:<br>`[Expert@MyGaia:0]# vgdisplay \| grep Free`<br>`  Free  PE / Size  4090 / 127.81 GiB`<br>`[Expert@MyGaia:0]#`<br>C. Get the free disk space in the "lv_current" partition:<br>`[Expert@MyGaia:0]# lvs \| egrep "LSize\|lv_current"`<br>`  LV  VG  Attr  LSize  Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert`<br>`  lv_current vg_splat -wi-ao---- 40g`<br>`[Expert@MyGaia:0]#`<br>D. Calculate the free disk space available for snapshot images:<br>`Available free disk space for all snapshot images = = (Output of "vgdisplay" command) - 1.1*(Output of "lvs" command) = = (127.81) - 1.1*(40) = 83.81 GB`<br>E. Calculate the limit for the scheduled snapshot task:<br>For example, you need to maintain 30 GB of free disk space at all times.<br>`Limit = (Available free disk space for all snapshot images) - (Free disk space to maintain) = = (83.81 GB) - (30 GB) = 53.81 GB` |
| 9 | Click **Apply**.<br>The scheduled snapshot configuration appears in the **Scheduled Snapshot** section. |

### Troubleshooting

- If a snapshot was not created, examine these files:

```
/var/log/messages*
```

- If a snapshot was created, but there were some issues, examine this file:

```
/var/log/CPsnapshot/<Snapshot Name>_<Timestamp>
```

# Snapshot Management in Gaia Clish - Regular Snapshots

**Important:**

- On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Snapshot operations (in the Global Gaia Portal or Global Gaia Clish).
  To collect or import a Gaia Snapshot in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

Before you create a snapshot image, make sure the appliance or storage destination meets the prerequisites - see *"Snapshot Prerequisites" on page 617*.

### Description

Manage system images (snapshots).

### Syntax

#### Creating a new snapshot image

These commands only create a new snapshot image.

##### Creating a new snapshot image as a local LVM volume

```
add snapshot-onetime name <Name of Snapshot> [description
"<Description of Snapshot>"]
```

**Note** - Gaia Snapshots are not files, but Logical Volume Management (LVM) volumes. Gaia stores these snapshots as a disk partition. To show the list of virtual drives, run the "`lvs`" command in the Expert mode.

##### Creating a new snapshot image and exporting it to a local file

```
add snapshot-onetime name <Name of Snapshot> [description
"<Description of Snapshot>"] target local path <Local Path>
```

### Creating a new snapshot image as a file and uploading it to an FTP server

```
add snapshot-onetime name <Name of Snapshot> [description
"<Description of Snapshot>"] target ftp ip <IPv4 Address of
FTP Server> path <Path on FTP Server> username <User Name on
FTP Server> password <Password in Plain Text>
```

### Creating a new snapshot image as a file and uploading it to an SCP server

```
add snapshot-onetime name <Name of Snapshot> [description
"<Description of Snapshot>"] target scp ip <IPv4 Address of
SCP Server> path <Path on SCP Server> username <User Name on
SCP Server> password <Password in Plain Text>
```

### Exporting an existing snapshot image

These commands only export an existing snapshot image from a local LVM volume.

#### Exporting an existing snapshot image and saving it as a local file

```
set snapshot-onetime export <Name of Exported Snapshot> target
local path <Local Path>
```

#### Exporting an existing snapshot image as a file and uploading it to an FTP server

```
set snapshot-onetime export <Name of Exported Snapshot> target
ftp path <Path on FTP Server> ip <IPv4 Address of FTP Server>
username <User Name on FTP Server> password <Password in Plain
Text>
```

#### Exporting an existing snapshot image as a file and uploading it to an SCP server

```
set snapshot-onetime export <Name of Exported Snapshot> target
scp path <Path on SCP Server> ip <IPv4 Address of SCP Server>
username <User Name on SCP Server> password <Password in Plain
Text>
```

### Importing an existing snapshot image

These commands only import an existing snapshot image file and store it on Gaia as a local LVM volume.

#### Importing an existing snapshot image from a local file

```
set snapshot-onetime import <Name of Imported Snapshot> target
local path <Local Path>
```

#### Importing an existing snapshot image from an FTP server

```
set snapshot-onetime import <Name of Imported Snapshot> target
ftp ip <IPv4 Address of FTP Server> path <Path on FTP Server>
username <User Name on FTP Server> password <Password in Plain
Text>
```

#### Importing an existing snapshot image from an SCP server

```
set snapshot-onetime import <Name of Imported Snapshot> target
scp ip <IPv4 Address of SCP Server> path <Path on SCP Server>
username <User Name on SCP Server> password <Password in Plain
Text>
```

### Importing and reverting to an existing snapshot image

These commands import an existing snapshot image, store it on Gaia as a local LVM volume, and then revert to that imported snapshot image.

**Important**:

- When Gaia reverts to a snapshot, it overwrites the existing running configuration and settings. Make sure you know credentials of the snapshot, to which you revert.
- Before you **revert** to a snapshot on a new appliance, or after a reset to factory defaults, you must run the Gaia First Time Configuration Wizard and configure the same settings as before you created the snapshot.
- If you reverted a snapshot on a Security Gateway / Cluster Member, install the Security Policy.

#### Importing and reverting an existing snapshot image from a local LVM volume

```
set snapshot-onetime revert target lvm name <External Name of Snapshot>
```

**Note** - Gaia Snapshots are not files, but disk volumes. Gaia stores these snapshots as a disk partition. To show the list of virtual drives, run the "`lvs`" command in the Expert mode.

#### Importing and reverting an existing snapshot image from a local file

```
set snapshot-onetime revert target local name <Imported Name of Snapshot> path <Local Path>
```

#### Importing and reverting an existing snapshot image from an FTP server

```
set snapshot-onetime revert target ftp name <Imported Name of Snapshot> path <Path on FTP Server> ip <IPv4 Address of FTP Server> username <User Name on FTP Server> password <Password in Plain Text>
```

#### Import and reverting an existing snapshot image from an SCP server

```
set snapshot-onetime revert target scp name <Imported Name of Snapshot> path <Path on SCP Server> ip <IPv4 Address of SCP Server> username <User Name on SCP Server> password <Password in Plain Text>
```

### Viewing existing snapshot images

```
show snapshots
```

```
show snapshot <Name of Snapshot>
      all
      date
      description
      size
```

### Deleting a local snapshot image

```
delete snapshot <Name of Snapshot>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

**Parameters**

| Parameter | Description |
|---|---|
| `name <Name of Snapshot>` | Configures the name of the new snapshot image.<br>You must enter a string that does not contain spaces. |
| `name <Name of Exported Snapshot>` | Configures the name, under which the exported snapshot image file is stored.<br>You must enter a string that does not contain spaces.<br>You must **not** add an extension. |
| `name <Name of Imported Snapshot>` | Configures the name, under which the imported snapshot image is stored on this Gaia.<br>You must enter a string that does not contain spaces. |
| `description "<Description of Snapshot>"` | Optional.<br>Configures the description of the snapshot image.<br>You must enclose the text in double quotes, or enter the string that does not contain spaces. |
| `export <Name of Snapshot>` | Exports the snapshot image by the specified name.<br>You must enter a string that does not contain spaces. |
| `import <Name of Snapshot>` | Imports the snapshot image by the specified name.<br>You must enter a string that does not contain spaces. |
| `target` | When you create or export a snapshot, specifies the destination for the snapshot image.<br>When you import a snapshot, specifies the source of the snapshot image.<br>■ `target lvm` - Local LVM volume on this Gaia<br>■ `target local` - Local file on this Gaia<br>■ `target ftp` - Remote FTP server<br>■ `target scp` - Remote SCP server |
| `ip` | Specifies the IPv4 address of the remote server:<br>■ `ip <IPv4 Address of FTP Server>`<br>Specifies the IPv4 address of the remote FTP server.<br>■ `ip <IPv4 Address of SCP Server>`<br>Specifies the IPv4 address of the remote SCP server. |

| Parameter | Description |
|---|---|
| `path` | Specifies the path to the snapshot image file.<br>When you export, this is the path to the directory (`/path_to/directory/`).<br>When you import, this is the path to the directory and the snapshot image (`/path_to/directory/snapshot`).<br>■ `path <Local Path>`<br>Specifies the local absolute path on this Gaia.<br>■ `path <Path on FTP Server>`<br>Specifies the path on the remote FTP server.<br>■ `path <Path on SCP Server>`<br>Specifies the path on the remote SCP server. |
| `username` | Specifies the login username on the remote server:<br>■ `username <User Name on FTP Server>`<br>Specifies the user name required to log in to the remote FTP server.<br>■ `username <User Name on SCP Server>`<br>Specifies the user name required to log in to the remote SCP server. |
| `password <Password in Plain Text>` | Specifies the password (in plain text) required to log in to the remote server. |

**Examples**

- Creating a new snapshot image locally as a file:

```
gaia> add snapshot-onetime name 1st_image_after_install
description "First image after installation" target local
path /var/log/
```

- Creating a new snapshot image as a file and uploading it to an SCP server:

```
gaia> add snapshot-onetime name 1st_image_after_install
description "First image after installation" target scp ip
192.168.20.30 path /var/log/ username scp_admin password
123456
```

- Importing an existing snapshot image from an SCP server:

```
gaia> set snapshot-onetime import 1st_image_after_install
target scp ip 192.168.20.30 path /var/log/ username scp_
admin password 123456
```

### Troubleshooting

- If a snapshot was not created, examine these files:

  ```
  /var/log/messages*
  ```

- If a snapshot was created, but there were some issues, examine this file:

  ```
  /var/log/CPsnapshot/<Snapshot Name>_<Timestamp>
  ```

# Snapshot Management in Gaia Clish - Scheduled Snapshots

**Important:**

- On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Snapshot operations (in the Global Gaia Portal or Global Gaia Clish).
  To collect or import a Gaia Snapshot in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

Before you create a snapshot image, make sure the appliance or storage destination meets the prerequisites.

### Description

Manage system images (snapshots).

From R81, you can also configure scheduled system images (snapshots).

**Notes:**

- R82 supports only *one* scheduled snapshot task.
- It is not possible to change any of the settings in the scheduled snapshot task.
  You must configure the task from scratch.
- To configure scheduled snapshots in Gaia Portal, see *"Snapshot Management in Gaia Portal" on page 619*.

### Syntax

```
set snapshot-scheduled activation {enabled | disabled}
```

```
set snapshot-scheduled recurrence
      daily time <HH:MM>
      hourly hours {<Hours> | all} at <0-59>
      interval minutes <1-59>
      monthly month {<Months> | all} days <Days> time <HH:MM>
      weekly days {<Days> | all} time <HH:MM>
```

```
set snapshot-scheduled retention-policy
      keep-disk-space-above-in-GB <Limit>
      max-snapshots-to-keep <1-9999>
      min-snapshots-to-keep <1-9999>
```

```
set snapshot-scheduled settings snapshot-name-prefix <Prefix of
Snapshot Name> description <Description of Snapshot>
      target ftp ip <IPv4 Address of FTP Server> path <Path on FTP
Server> username <User Name on FTP Server> {password <Password in
Plain Text> | password-hash <Password Hash>}
      target lvm
      target scp ip <IPv4 Address of SCP Server> path <Path on SCP
Server> username <User Name on SCP Server> {password <Password in
Plain Text> | password-hash <Password Hash>}
```

```
show snapshot-scheduled <Prefix of Snapshot Name>
```

### Procedure

1. **Configure the scheduled snapshot task**

   R82 supports only *one* of these scheduled snapshot tasks.

   You can only configure one task for a local LVM volume, one task for an FTP server, or one task for an SCP server.

   **Creating a new snapshot image as a local LVM volume**

   ```
   set snapshot-scheduled settings snapshot-name-prefix
   <Prefix of Snapshot Name> [description "<Description of
   Snapshot>"] target lvm
   ```

   **Note** - Gaia Snapshots are not files, but Logical Volume Management (LVM) volumes. Gaia stores these snapshots as a disk partition. To show the list of virtual drives, run the "`lvs`" command in the Expert mode.

**Creating a new snapshot image as a file and uploading it to an SCP server**

```
set snapshot-scheduled settings snapshot-name-prefix
<Prefix of Snapshot Name> [description "<Description of
Snapshot>"] target scp ip <IPv4 Address of SCP Server>
path <Path on SCP Server> username <User Name on SCP
Server> {password <Password in Plain Text> | password-hash
<Password Hash>}
```

**Important:**

- First, you must follow sk164234 to configure the SCP server as a trusted host on Gaia.
- The username must have permissions to delete files on the SCP server.

**Creating a new snapshot image as a file and uploading it to an FTP server**

```
set snapshot-scheduled settings snapshot-name-prefix
<Prefix of Snapshot Name> [description "<Description of
Snapshot>"] target ftp ip <IPv4 Address of FTP Server>
path <Path on FTP Server> username <User Name on FTP
Server> {password <Password in Plain Text> | password-hash
<Password Hash>}
```

**Important** -The username must have permissions to delete files on the FTP server.

2. **Configure the recurrence for the snapshot schedule**

**Running one time on each day at specified time**

```
set snapshot-scheduled recurrence daily time <HH:MM>
```

**Running several times each day at specified times**

```
set snapshot-scheduled recurrence hourly hours {<Hours> |
all} at <0-59>
```

**Running several times each day at specified intervals**

```
set snapshot-scheduled recurrence interval minutes <1-59>
```

**Running in specified months on specified days and at specified time**

```
set snapshot-scheduled recurrence monthly month {<Months>
| all} days <Days> time <HH:MM>
```

**Running each week on specified days of week and at specified time**

```
set snapshot-scheduled recurrence weekly days {<Days> |
all} time <HH:MM>
```

3. **Configure the snapshot retention policy**

   **Important:**
   - This step applies only if you save the new snapshot image as a local LVM volume.
   - The retention policy applies only to the new snapshots (and does not apply to existing snapshots).
   - When Gaia creates new snapshots, it deletes the oldest snapshot that exceeds the configured policy parameters.

   **Configuring the maximum number of snapshot images to save**

   ```
   set snapshot-scheduled retention-policy max-snapshots-to-
   keep <1-9999>
   ```

   **Configuring the minimum number of snapshot images to save**

   ```
   set snapshot-scheduled retention-policy min-snapshots-to-
   keep <1-9999>
   ```

### Configuring the amount of free disk space to maintain

This command lets you configure how much of the disk space must remain free at all times:

```
set snapshot-scheduled retention-policy keep-disk-space-
above-in-GB <Limit>
```

The limit you need to configure with this command is:

```
Limit = (Available free disk space for all snapshot
images) - (Free disk space to maintain)
```

Where:

```
Available free disk space for all snapshot images =
= (Output of: vgdisplay | grep Free) - 1.1*(Output of: lvs
| egrep "LSize|lv_current")
```

### Example

For more information, see sk80260.

a. Log in to the Expert mode.

b. Get the free disk space in volume groups:

```
[Expert@MyGaia:0]# vgdisplay | grep Free
  Free  PE / Size       4090 / 127.81 GiB
[Expert@MyGaia:0]#
```

c. Get the free disk space in the "lv_current" partition:

```
[Expert@MyGaia:0]# lvs | egrep "LSize|lv_current"
  LV         VG       Attr       LSize  Pool Origin
Data%  Meta%  Move Log Cpy%Sync Convert
  lv_current vg_splat -wi-ao---- 40g
[Expert@MyGaia:0]#
```

d. Calculate the free disk space available for snapshot images:

```
Available free disk space for all snapshot images =
= (Output of "vgdisplay" command) - 1.1*(Output of
"lvs" command) =
= (127.81) - 1.1*(40) = 83.81 GB
```

e. Calculate the limit for the scheduled snapshot task:

For example, you need to maintain 30 GB of free disk space at all times.

```
Limit = (Available free disk space for all snapshot
images) - (Free disk space to maintain) =
= (83.81 GB) - (30 GB) = 53.81 GB
```

f. Log in to Gaia Clish.

g. Configure the limit (round up or round down the limit you calculated in the previous step):

```
set snapshot-scheduled retention-policy keep-disk-
space-above-in-GB 54
save config
```

4. **Enable the scheduled snapshot feature**

- To control this feature in Gaia Clish:
  - To enable the snapshot schedule:

    ```
    set snapshot-scheduled activation enabled
    ```

    **Important:**
    - You must run this command after you configure a scheduled snapshot for the first time.
    - You must run this command after any change in the existing configuration of a scheduled snapshot.

  - To disable the snapshot schedule:

    ```
    set snapshot-scheduled activation disabled
    ```

- To control this feature in Gaia Portal:

  a. In the navigation tree, click **Maintenance** > **Snapshot Management**.

  b. In the section **Scheduled Snapshots**:
     - To enable the snapshot schedule, select **Activate / Deactivate**.
     - To disable the snapshot schedule, clear **Activate / Deactivate**.

  c. Click **Apply**.

5. **Examine the scheduled snapshot configuration**

```
show snapshot-scheduled
```

### Deleting a scheduled snapshot

You can only disable the snapshot schedule to stop the scheduled task:

```
set snapshot-scheduled activation disabled
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

**Parameters**

| Parameter | Description |
|---|---|
| `snapshot-name-prefix <Prefix of Snapshot Name>` | The final name of the snapshot consists of two parts - the prefix (configured by the user) and the time stamp (format is hard-coded): `<Prefix>_<YYYY_MM_DD__HH_mm>`<br>■ The prefix maximum length is 15 characters.<br>■ The prefix can consist only of letters, numbers, or underscore "_".<br>■ Default prefix: `snap`. |
| `description "<Description of Snapshot>"` | Optional.<br>Configures the description of the snapshot image. You must enclose the text in double quotes, or enter the string that does not contain spaces.<br>Default description : `default_snapshot` |
| `target` | Specifies the destination for the snapshot image:<br>■ `target lvm` - Local LVM volume on this Gaia (this is the default)<br>■ `target ftp` - Remote FTP server<br>■ `target scp` - Remote SCP server |
| `ip` | Specifies the IPv4 address of the remote server:<br>■ `ip <IPv4 Address of FTP Server>` Specifies the IPv4 address of the remote FTP server.<br>■ `ip <IPv4 Address of SCP Server>` Specifies the IPv4 address of the remote SCP server.<br>**Important** - First, you must follow sk164234 to configure the SCP server as a trusted host on Gaia. |

| Parameter | Description |
|---|---|
| `path` | Specifies the path to the snapshot image file:<br>■ `path <Local Path>`<br>Specifies the local absolute path on this Gaia to save the snapshot image file (`/path_to/directory/`).<br>■ `path <Path on FTP Server>`<br>Specifies the path on the remote FTP server where to upload the snapshot image file (`/path_to/directory/`).<br>■ `path <Path on SCP Server>`<br>Specifies the path on the remote SCP server where to upload the snapshot image file (`/path_to/directory/`). |
| `username` | Specifies the login username on the remote server:<br>■ `username <User Name on FTP Server>`<br>Specifies the user name required to log in to the remote FTP server.<br>■ `username <User Name on SCP Server>`<br>Specifies the user name required to log in to the remote SCP server.<br>**Important** - The username must have permissions to delete files on the remote server. |
| `password <Password in Plain Text>` | Specifies the password (in plain text) required to log in to the remote server. |
| `password-hash <Password Hash>` | Specifies the hash of the password required to log in to the remote server. |

| Parameter | Description |
|---|---|
| `recurrence daily time <HH:MM>` | Specifies that the job should run once a day - every day, at specified time.<br>Enter the time of day in the 24-hour clock format - <Hours>:<Minutes>.<br>Example:<br>`HostName> set snapshot-scheduled recurrence daily time 14:35`<br>`HostName> show snapshot-scheduled`<br>`Scheduled snapshot configuration:`<br>`...`<br>`Every day at 14:35` |
| `recurrence hourly hours {<Hours> \| all} at <Minutes 0-59>` | Specifies that the job must run many times during the day - at the specified time.<br>■ You can specify a single hour of a day by a number from 0 to 23.<br>■ You can specify several hours of a day. Enter the hours separated by commas. Example - for hours 14, 15, and 16, enter: 14,15,16<br>■ To specify each hour of a day, enter: `all`<br>■ You must specify the minutes of each configured hour by a number from 0 to 59.<br>Example:<br>`HostName> set snapshot-scheduled recurrence hourly hours 14,15,16 at 35`<br>`HostName> show snapshot-scheduled`<br>`Scheduled snapshot configuration:`<br>`...`<br>`Every day at 14:35,15:35,16:35` |

| Parameter | Description |
|---|---|
| `recurrence interval minutes <1-59>` | Specifies that the job must run many times during the day - at intervals of the specified number of minutes.<br>Example:<br>`HostName> set snapshot-scheduled recurrence interval minutes 30`<br>`HostName> show snapshot-scheduled`<br>`Scheduled snapshot configuration:`<br>`...`<br>`Every 30 minutes.` |
| `recurrence monthly month {<Months> \| all} days <Days> time <HH:MM>` | Specifies that the job must run once a month - on the specified months, on the specified dates, and at the specified time.<br>■ Specify the months by numbers from 1 to 12: January = 1, February = 2, ..., December = 12.<br>■ To specify several months, enter their numbers separated by commas.<br>Example - for January, February, and March, enter: 1,2,3<br>■ To specify each month of the year, enter: `all`<br>■ Specify the dates of a month by numbers from 1 to 31.<br>■ To specify several dates, enter their numbers separated by commas.<br>Example - for 1st, 2nd and 3rd day of month, enter: 1,2,3<br>Example:<br>`HostName> set snapshot-scheduled recurrence monthly month 1,2,3 days 1,2,3 time 14:35`<br>`HostName> show snapshot-scheduled`<br>`Scheduled snapshot configuration:`<br>`...`<br>`Each January, February, March on days 1, 2, 3 at 14:35` |

| Parameter | Description |
|---|---|
| `recurrence weekly days {<Days> \| all} time <HH:MM>` | Specifies that the job must run once a week - on specified days of week, and at specified time.<br>■ Specify the days of a week by numbers from 0 to 6:<br>Sunday = 0, Monday = 1, Tuesday = 2, Wednesday = 3, Thursday = 4, Friday = 5, Saturday = 6.<br>■ To specify several days of a week, enter their numbers separated by commas.<br>Example- for Sunday, Monday, and Tuesday, enter: 0,1,2<br>■ To specify each day of the week, enter: `all`<br>Example:<br>`HostName> set snapshot-scheduled recurrence weekly days 1,3 time 14:35`<br>`HostName> show snapshot-scheduled`<br>`Scheduled snapshot configuration:`<br>`...`<br>`Every week on Monday, Wednesday at 14:35` |
| `retention-policy` | Configures the retention policy when you save the new snapshot image as a local LVM volume:<br>(when Gaia creates new snapshots, it deletes the oldest snapshot that exceeds the configured policy parameters)<br>■ `max-snapshots-to-keep <1-9999>`<br>Specifies the maximum number of snapshot images to save. The default threshold is: 9999.<br>■ `min-snapshots-to-keep <1-9999>`<br>Specifies the minimum number of snapshot images to save. The default threshold is: 1.<br>■ `keep-disk-space-above-in-GB <1-Maximum>`<br>Specifies the amount of free disk space to maintain between 1 GB and the maximum available space. |

| Parameter | Description |
|---|---|
| `activation {enabled \| disabled}` | Enables or disables the snapshot schedule. |

### Examples

- Creating a daily snapshot image as a local LVM volume:

```
gaia> set snapshot-scheduled settings snapshot-name-prefix
Daily description "Daily snapshot image" target lvm
gaia>
gaia> set snapshot-scheduled recurrence daily time 22:00
gaia>
gaia> set snapshot-scheduled retention-policy max-snapshots-
to-keep 10
gaia>
gaia> set snapshot-scheduled retention-policy min-snapshots-
to-keep 3.
gaia>
gaia> set snapshot-scheduled retention-policy keep-disk-
space-above-in-GB 50
gaia>
gaia> show snapshot-scheduled
Scheduled snapshot configuration:
name: Daily
description: Daily
activation: disabled
target: lvm
max-snapshots-to-keep: 10
min-snapshots-to-keep: 3
keep-disk-space-above-in-GB: 50
Every day at 22:00
gaia>
gaia> set snapshot-scheduled activation enabled
gaia>
gaia> save config
```

- Creating a monthly snapshot image as a file and uploading it to an SCP server:

```
gaia> set snapshot-scheduled settings snapshot-name-prefix
Monthly description "Monthly snapshot image" target scp ip
192.168.20.30 path /var/log/my_snapshots/ username backup_
user password 123456
gaia>
gaia> set snapshot-scheduled recurrence monthly month all
days 1 time 22:00
gaia>
gaia> show snapshot-scheduled
Scheduled snapshot configuration:
name: Monthly
description: Monthly
activation: disabled
target: scp
username: backup_user
ip: 192.168.20.30
uploadPath: /var/log/my_snapshots/
Every month on day 1 at 22:00
gaia>
gaia> set snapshot-scheduled activation enabled
gaia>
gaia> save config
```

### Troubleshooting

If a scheduled snapshot task fails, there is no notification about it. You must manually check if a snapshot was created.

- If a snapshot was not created, examine these files:

  ```
  /var/log/messages*
  ```

- If a snapshot was created, but there were some issues, examine this file:

  ```
  /var/log/CPsnapshot/<Snapshot Name>_<Timestamp>
  ```

# Working with Snapshot Management in the Expert mode (g_snapshot)

**Important:**

- This section applies **only** to Scalable Platforms (ElasticXL, Maestro, and Chassis).
- On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in the Expert mode on the applicable Security Group.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Snapshot operations (in the Global Gaia Portal or Global Gaia Clish).
  To collect or import a Gaia Snapshot in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

## Description

Use the "`g_snapshot`" command in the Expert mode to show and revert snapshots for specific Security Group Members.

This command is different from the Gaia Clish "`snapshot`" command, which works for all Security Group Members together.

## Syntax

```
g_snapshot [-b <SGM IDs>] show
g_snapshot [-b <SGM IDs>] revert <Name of Snapshot>
```

## Parameters

| Parameter | Description |
|---|---|
| `show` | Shows saved snapshots for the specified Security Group Members. |
| `revert` | Restores the specified Security Group Members to the specified snapshot. |
| *<Name of Snapshot>* | Specifies the snapshot file name to restore. |

| Parameter | Description |
|---|---|
| `-b <SGM IDs>` | Applies to Security Group Members as specified by the `<SGM IDs>`.<br>`<SGM IDs>` can be:<br>■ No `<SGM IDs>` specified, or `all`<br>Applies to all Security Group Members and all Sites<br>■ One Security Group Member (for example, `1_1`)<br>■ A comma-separated list of Security Group Members (for example, `1_1,1_4`)<br>■ A range of Security Group Members (for example, `1_1-1_4`)<br>■ One Site (`chassis1`, or `chassis2`)<br>■ The Active Site (`chassis_active`) |

## Examples

### Example 1 - Restore Security Group Members 1_1 and 1_4 to the snapshot called "My_Snapshot"

```
[Expert@HostName-ch0x-0x:0]# g_snapshot -b 1_1,1_4 revert My_Snapshot
```

### Example 2 - Restore the Chassis2 to the snapshot called "My_Snapshot"

```
[Expert@HostName-ch0x-0x:0]# g_snapshot -b chassis2 revert My_Snapshot
```

### Example 3 - Show the saved snapshots for all Security Group Members on the Chassis1

```
[Expert@HostName-ch0x-0x:0]# g_snapshot -b chassis1 show
```

# SMO Image Cloning

**Important** - This section applies **only** to Scalable Platforms (ElasticXL, Maestro, and Chassis).

### Background

You can use SMO Image Cloning as a tool for cloning images from the Single Management Object (SMO) in a Security Group.

In addition to cloning the SMO version, this mechanism clones all installed Hotfixes, if there are any.

**Best Practice**:

- On Maestro, we recommend to use this tool when you add a new Maestro Security Appliance (an additional one, or a replacement for a failed one) to a Security Group
- On Scalable Chassis, we recommend to use this tool when you add a new SGM (an additional one, or a replacement for a failed one) to a Scalable Chassis.

When you activate the auto-clone feature, each Security Group Member updates these:

- MD5 of its local image during reboot
- Admin UP state
- Installed Hotfixes

If the MD5 of the local image is different from the MD5 of the SMO image, the Security Group Member clones the SMO image.

### Working with image auto-clone in Gaia gClish:

| Command | Instructions |
|---|---|
| `show cluster configuration image auto-clone state` | Shows the current auto-clone state. |
| `set cluster configuration image auto-clone state {on \| off}` | Controls the auto-cloning state:<br>■ `on` - enabled<br>■ `off` - disabled |

**Note** - SMO Image Cloning does **not** support Gaia snapshot (the included *fcd*).

**Working with image's MD5 in Gaia gClish:**

| Command | Instructions |
|---|---|
| `show cluster configuration image md5sum` | Shows the MD5 of the local image. |
| `set cluster configuration image md5sum` | Updates the MD5 of the local image.<br>This is done automatically during reboot, admin UP, and hotfix installation. |

# Restoring a Factory Default Image on Check Point Appliance

Factory default images on Check Point appliances are created automatically when you install or upgrade an appliance to another release.

You can restore your Check Point appliance to the factory default image for a specified release.

**Important** - This procedure overwrites all existing configuration settings.

**Best Practices:**

- Create a snapshot image before you restore a factory default image.
- Export all existing snapshots from the appliance before you restore a factory default image.

### Restoring a Factory Default image in Gaia Portal

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance > Factory Defaults**. |
| 2 | Select the factory image. |
| 3 | Click **Apply**. |

### Restoring a Factory Default image in Gaia Clish

| Step | Instructions |
|---|---|
| 1 | Connect to the command line on your appliance. |
| 2 | Log in to Gaia Clish. |
| 3 | Run:<br>`set fcd revert<SPACE><TAB>`<br>`set fcd revert <Name of Default Image>` |
| 4 | Follow the instructions on the screen. |
| 5 | Reboot:<br>`reboot` |

# Download SmartConsole

You can download the SmartConsole application package from the Gaia Portal of your Security Management Server / Multi-Domain Server / Standalone Server.

| Step | Instructions |
|---|---|
| 1 | With a web browser, connect to Gaia Portal at:<br>`https://<IP address of Gaia Management Interface>`<br>If you changed the default port of Gaia Portal from 443, then you must also enter it (`https://<IP address>:<Port>`). |
| 2 | There are two options to get the SmartConsole package.<br>Option 1:<br>a. In the navigation tree, click **Overview**.<br>b. At the top of the page, click the **Download Now!** button.<br>c. On the download page, click the **Download** button.<br>d. Save the package.<br>Option 2:<br>a. In the navigation tree, click **Maintenance** > **Download SmartConsole**.<br>b. Click the **Download** button.<br>c. On the download page, click the **Download** button.<br>d. Save the package. |
| 3 | Double-click the SmartConsole package and follow the installation wizard instructions. |

For next steps in SmartConsole, refer to the *R82 Security Management Administration Guide*.

# Hardware Health Monitoring

*In This Section:*



You can monitor these hardware elements:

- Fan sensors - Shows the fan number, status, and speed.
- System Temperature sensors
- Voltage sensors
- Power Supplies (on servers that support it)

In addition, see sk119232 - Hardware sensors thresholds on Check Point appliances.

**Important** - For Scalable Platforms, see the *R82 Scalable Platforms Administration Guide*.

## Showing Hardware Health Information in Gaia Portal

In the navigation tree, click **Maintenance** > **Hardware Health**.

**Note** - The **Hardware Health** page appears only on supported hardware.

You can see the status of the machine fans, system temperature, the voltages, and (for supported hardware only) the power supply.

For each component sensor, the table shows the value of its operation, and the status: **OK**, **Low**, or **High**.

- To see the health history of a component, select the component sensor. A graph shows the values over time.
- To change the time intervals that the graph shows, click the **Minute** arrows.
- To view different times, click the **Forward/Backward** arrows.
- To refresh, click **Refresh**.

# Showing Hardware Health Information in Gaia Clish

### Description

These commands display the status for various system hardware components.

Components, for which the status can be shown, include BIOS, cooling fans, power supplies, temperature, and voltages.

**Note** - The command returns information only for installed hardware components and only on supported hardware.

### Syntax

```
show sysenv
      all
      bios
      fans
      ps
      temp
      volt
```

### Parameters

| Parameter | Description |
|---|---|
| `all` | Shows all system and hardware information. |
| `bios` | Shows BIOS information. |
| `fans` | Shows speed of cooling fans. |
| `ps` | Shows voltages and states of power supplies. |
| `temp` | Shows information from temperature sensors. |
| `volt` | Shows voltages information. |

### Example

```
gaia> show sysenv all

Hardware Information

Name   Value    unit      type     status  Maximum  Minimum
+12V   29.44    Volt      Voltage    0      12.6      11.4
+5V     6.02    Volt      Voltage    0      5.3       4.75
VBat    3.23    Volt      Voltage    0      3.47      2.7

gaia>
```

# Showing Hardware Information

You can see information about the hardware, on which Gaia is installed using these commands:

| Command | Description |
|---|---|
| `show asset<SPACE><TAB>` | You can run it in Gaia Clish only. |
| `cpstat os -f sensors` | You can run it in Gaia Clish, or Expert mode. |

**The "`show asset`" command**

### Description

Shows information about the hardware, on which Gaia is installed.

You can run this command in Gaia Clish only.

The information shown depends on the type of hardware.

Common types of information shown are:

- Serial number
- Amount of physical RAM
- CPU frequency
- Number of disks in the system
- Disk capacity

### Syntax

```
show asset<SPACE><TAB>
show asset all
show asset <Category Name>
```

### Parameters

| Parameter | Description |
|---|---|
| `<SPACE><TAB>` | Press these keys to show a list of asset categories, such as `system` and `disk`.<br>The available categories depend on the type of hardware. |

| Parameter | Description |
|---|---|
| `all` | Shows all available hardware information.<br>The information shown depends on the type of hardware. |
| *<Category Name>* | Shows available information for a specified category. |

### Example output

```
gaia> show asset system
Platform: Check Point 5800
Serial Number: XXX
CPU Model: Intel(R) Xeon(R) E3-1285Lv4
CPU Frequency: 3400
Disk Size: 500GB
Number of Cores: 8
CPU Hyperthreading: Enabled
gaia>
```

## The "`cpstat os -f sensors`" command

### Description

Shows information from supported hardware sensors.

You can run this command in Gaia Clish, or the Expert mode.

### Syntax

```
cpstat os -f sensors
```

### Example output

```
Temperature Sensors
------------------------------------------------
|Name        |Value|Unit     |Type       |Status|
------------------------------------------------
|CPU1 Temp   |49.50|degrees C|Temperature|     0|
|CPU0 Temp   |52.75|degrees C|Temperature|     0|
|Outlet Temp|27.50|degrees C|Temperature|     0|
|Intake Temp|28.75|degrees C|Temperature|     0|
------------------------------------------------

Fan Speed Sensors
-------------------------------------
|Name         |Value|Unit|Type|Status|
-------------------------------------
|System Fan 4|3349 |RPM |Fan |     0|
|System Fan 3|3375 |RPM |Fan |     0|
|System Fan 2|3383 |RPM |Fan |     0|
|System Fan 1|3333 |RPM |Fan |     0|
-------------------------------------

Voltage Sensors
----------------------------------------
|Name         |Value|Unit |Type   |Status|
----------------------------------------
|VBAT        |3.25 |Volts|Voltage|     0|
|5VSB        |5.04 |Volts|Voltage|     0|
|3VSB        |3.31 |Volts|Voltage|     0|
|VCC 5V      |5.03 |Volts|Voltage|     0|
|VCC 3V      |3.30 |Volts|Voltage|     0|
|VCC 12V     |12.07|Volts|Voltage|     0|
|CPU1 DDR4-2|1.19 |Volts|Voltage|     0|
|CPU1 DDR4-1|1.19 |Volts|Voltage|     0|
|CPU0 DDR4-2|1.19 |Volts|Voltage|     0|
|CPU0 DDR4-1|1.19 |Volts|Voltage|     0|
|CPU1 Vcore |1.81 |Volts|Voltage|     0|
|CPU0 Vcore |1.81 |Volts|Voltage|     0|
----------------------------------------
```

# Hardware Diagnostics

## Introduction

On Check Point appliances, you can run the built-in Hardware Diagnostics Tool that supports these tests:

- Spec Test
- Memory Test
- Network Test
- Disk Test
- Long Disk Test

**Related Information:**

- *"Hardware Health Monitoring" on page 654*
- *"Monitoring RAID Synchronization" on page 662*
- sk171436 - HealthCheck Point (HCP) Release Updates

## Requirement

To save the tool logs on a USB device, you must format it as FAT, FAT32, EXT2, or EXT3 file system. (NTFS or extFAT are not supported.)

## Running the tool through the LCD (recommended)

1. In the LCD on your appliance, select the **HW Diagnostics** option.
2. Follow the instructions on the LCD.

## Running the tool over the Console connection (recommended)

1. Connect a computer to the console port on your appliance.

   Configure the serial connection in your Terminal application.

   See the Getting Started Guide for your appliance model.
2. Reboot your appliance.
3. In the Terminal application, press any key to get the Boot Menu.
4. In the **Boot Menu**, select the option **HW Diagnostics**.
5. Follow the instructions on the screen.
6. When you exit the **HW Diagnostics** tool, the appliance reboots.

## Running the tool in the Expert mode (optional)

1. Connect to the command line over SSH (or console port).
2. Log in to the Expert mode.
3. Run:

   ```
   diagMain
   ```
4. Follow the instructions on the screen.
5. When you exit the **HW Diagnostics** tool, the appliance reboots

   **Note** - If you do not want the appliance to reboot:
   a. Connect over SSH for the second time.
   b. In the second shell, run:

   ```
   killall diagMain
   ```

## Limitations

On 3100 and 3200 appliances: The Network Test using an external loopback device in interfaces eth1, eth2, eth3, and eth4 is not supported.

# Monitoring RAID Synchronization

You can monitor the RAID status of the disks to see when the hard disks are synchronized.

If you reboot the appliance before the hard disks are synchronized, the synchronization starts again at the next boot.

## Showing RAID Information in Gaia Portal

In the navigation tree, click **Maintenance** > **RAID Monitoring**.

You can see the information about **RAID Volumes** and **RAID Volume Disks**.

## Showing RAID Information in Command Line

Run one of these commands in Gaia Clish or Expert mode:

- **The "`raid_diagnostic`" command**

  **Description**

  This command shows data about the RAID and hard disks, with the percent synchronization done.

  **Syntax**

  ```
  raid_diagnostic
  ```

  **Example output from a Smart-1 225 appliance**

  ```
  Raid Status:
  VolumeID:0 RaidLevel: RAID-1 NumberOfDisks:2 RaidSize:465GB State:DEGRADED Flags:
  ENABLED RESYNC _IN_PROGRESS
  DiskID:0 DiskNumber:0 Vendor:ATA     ProductID:<HDD Model> Size:465GB State:ONLINE
  Flags:NONE
  DiskID:1 DiskNumber:1 Vendor:ATA     ProductID:<HDD Model> Size:465GB
  State:INITIALIZING Flags:OUT_OF-SYNC SyncState: 12%
  ```

  - `DiskID 0` is the left hard disk.
  - `DiskID 1` is the right hard disk.

- **The "`cpstat os -f raidInfo`" command**

### Description

This command shows almost the same information as the "`raid_diagnostic`" command, in tabular format.

### Syntax

```
cpstat os -f raidInfo
```

### Example output

```
Volume list
-------------------------------------------------------------------------------------------
-----
|Volume id|Volume type|Number of disks|Max LBA  |Volume state|Volume flags|Volume size
(GB)|
-------------------------------------------------------------------------------------------
-----
|        0|          2|              2|975175680|           0|           1|
465|
-------------------------------------------------------------------------------------------
-----

Volume list
-------------------------------------------------------------------------------------------
-----------------------------------------------------
|Volume id|Disk id|Disk number|Disk vendor|Disk product id|Disk revision|Disk max
LBA|Disk state|Disk flags|Disk sync state|Disk size (GB)|
-------------------------------------------------------------------------------------------
-----------------------------------------------------
|        0|      0|          0|NONE       |NONE            |NONE         |            0|
       1|         0|              0|             0|
|        0|      1|          1|NONE       |NONE            |NONE         |            0|
       1|         0|              0|             0|
-------------------------------------------------------------------------------------------
-----------------------------------------------------
```

# Shut Down

There are two ways to shut down:

- **Reboot:** Shuts down the system and then immediately restarts it.
- **Halt:** Shuts down the system. You start the system manually with the power switch.

## Rebooting and Shutting Down in Gaia Portal

**Important:**

- If you connected to the Gaia Portal of the applicable Security Group, these actions apply to the entire Security Group.
- If you connected to the Gaia Portal of the applicable Security Group Member, these actions apply only to that Security Group Member.

**Shutting down the system and then immediately restarting it**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance** > **Shut Down**. |
| 2 | Click **Reboot**. |

**Shutting down the system completely**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance** > **Shut Down**. |
| 2 | Click **Halt**. |

# Rebooting and Shutting Down in Gaia Clish

**Important:**

- If you connected to the Gaia gClish of the applicable Security Group, these commands apply to the entire Security Group.
- If you connected to the Gaia Clish of the applicable Security Group Member, these commands apply only to that Security Group Member.

**Shutting down the system and then immediately restarting it**

```
reboot
```

**Shutting down the system completely**

```
halt
```

# System Backup

- Back up the configuration of the Gaia operating system and of the Security Management Server database.

  You can restore a previously saved configuration.

  You can run the backup manually, or on a schedule.

  The configuration backup is saved in a `*.tgz` file in the `/var/log/CPbackup/backups/` directory (on Check Point Appliances and Open Servers).

  You can store backups locally, or remotely to a TFTP, SCP or FTP server.

- Save your Gaia system configuration settings as a ready-to-run CLI shell script.

  This lets you quickly restore your system configuration after a system failure or migration.

**Note** - You can only do a migration using the same Gaia version on the source and target computers.

**Important:**

- When you create a backup on a Security Management Server, make sure to close all SmartConsole clients. Otherwise, backup does not start.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Backup operations (in the Global Gaia Portal or Global Gaia Clish).
  To collect or import a Gaia Backup in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

# Backing Up and Restoring the System

*In This Section:*



**Important:**

- You can restore a backup file on Gaia OS with the same software version, Jumbo Hotfix Accumulator, and hotfixes as installed on the source Gaia OS, on which you collected this backup file.
- If you restored a backup on a Security Gateway / Cluster Member, install the Security Policy.
- To back up the Quantum Maestro Orchestrator configuration, follow the instructions in sk174202.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Backup operations (in the Global Gaia Portal or Global Gaia Clish).
  To collect or import a Gaia Backup in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

**Note** - Gaia Operating System uses this template for the name of a manual backup output file regardless of the Gaia Display Format for Time and Date:

```
backup_--_<HostName>.<Domain>_<YYYY>_<MM>_<DD>_<HH>_<MM>_
<SS>.tgz
```

Example for 20 May 2024, 18:04:43:

```
backup_--_MyGW.MyDomain.com_2024_May_20_18_04_43.tgz
```

**Note** - In addition to the regular backup file, the Gaia Operating System also creates a file with the required metadata. If you later need to upload this regular backup file to Check Point cloud (for example, Zero Touch), then you also have to upload this metadata file. The Gaia Operating System uses this template for the name of a regular backup metadata file regardless of the Gaia Display Format for Time and Date (the same file name as the regular backup file, with a different file extension):

```
backup_--_<HostName>.<Domain>_<YYYY>_<MM>_<DD>_<HH>_<MM>_
<SS>.info
```

Example for 20 May 2024, 18:04:43:

```
backup_--_MyGW.MyDomain.com_2024_May_20_18_04_43.info
```

## Excluding Files from the Gaia Backup

### Background

The Gaia Operating System contains backup configuration files (schema files) that control which files to collect during the backup for different software modules.

| File | Software Blade / Feature | Security Gateway | Management Server, Log Server |
|---|---|---|---|
| `/var/CPbackup/schemes/cvpn.cpbak` | Mobile Access | ✓ | – |
| `/var/CPbackup/schemes/dlp_gw.cpbak` | Data Loss Prevention | ✓ | – |
| `/var/CPbackup/schemes/dtps.cpbak` | Desktop Policy Server for SecureClients | ✓ | – |
| `/var/CPbackup/schemes/fg1.cpbak` | QoS | ✓ | – |
| `/var/CPbackup/schemes/fw1.cpbak` | Firewall | ✓ | – |
| `/var/CPbackup/schemes/fw1logs.cpbak` | Firewall Logs | ✓ | ✓ |
| `/var/CPbackup/schemes/ioc.cpbak` | External IoC Feeds | ✓ | ✓ |
| `/var/CPbackup/schemes/mgmts.cpbak` | Network Management | – | ✓ |
| `/var/CPbackup/schemes/ppak.cpbak` | SecureXL | ✓ | – |
| `/CPbackup/schemes/rt.cpbak` | SmartReporter | – | ✓ |
| `/var/CPbackup/schemes/rtm.cpbak` | Monitoring | ✓ | ✓ |
| `/var/CPbackup/schemes/scalable_platform.cpbak` | Scalable Platforms (Maestro and Chassis) | ✓ | – |

| File | Software Blade / Feature | Security Gateway | Management Server, Log Server |
|---|---|---|---|
| /var/CPbackup/schemes/snapshot.cpbak | Snapshot Utility | ✓ | ✓ |
| /var/CPbackup/schemes/svn.cpbak | Common Infrastructure ($CPDIR) | ✓ | ✓ |
| /var/CPbackup/schemes/system_configuration.cpbak | Gaia OS | ✓ | ✓ |
| /var/CPbackup/schemes/te.cpbak | Threat Emulation | ✓ | – |
| /var/CPbackup/schemes/uepm.cpbak | Endpoint Policy Management | – | ✓ |
| /var/CPbackup/schemes/vsx.cpbak | VSX | ✓ | – |
| /var/CPbackup/schemes/vsx_mgmt.cpbak | VSX Policy | – | ✓ |

**Procedure**

| Step | Instructions |
|---|---|
| 1 | Connect to the Command Line on the Gaia Server. |
| 2 | Log in to the Expert mode. |
| 3 | Back up the current configuration file:<br>`cp -v /var/CPbackup/schemes/<Name-of-File>.cpbak{,_BKP}` |
| 4 | Edit the current configuration file:<br>`vi /var/CPbackup/schemes/<Name-of-File>.cpbak` |

| Step | Instructions |
|---|---|
| 5 | Make the required changes in the applicable section:<br>■ The section <INCLUDE_FILES> controls which files to include during the backup.<br>■ The section <EXCLUDE_FILES> controls which files not to include during the backup. |
| 6 | Save the changes in the file and exit the editor. |

# Backing Up and Restoring the System in Gaia Portal

### Creating a regular backup

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance** > **System Backup**.<br>Refer to the **Regular Backup** section. |
| 2 | Click **Backup**. |
| 3 | Select the location of the backup file:<br>■ **This appliance**<br>To keep the collected backup locally in the `/var/log/CPbackup/backups/` directory.<br>■ **Management**<br>To send the collected backup to the Management Server that manages this Security Gateway.<br>Enter the Username and Password for the applicable SCP user.<br>The Security Gateway (or Cluster Member) uploads the file to the `/home/<username>/` directory on the Management Server.<br>**Important** - Follow sk164234 to configure the Security Gateway (or Cluster Member) as a trusted host on the Management Server.<br>■ **Private server:**<br>In the **Protocol** field, select the server type.<br>• **FTP**<br>To send the collected backup to an FTP server.<br>Enter the IPv4 address, Username, Password, and Upload Path.<br>• **TFTP**<br>To send the collected backup to a TFTP server.<br>Enter the IPv4 address.<br>• **SCP**<br>To send the collected backup to an SCP server.<br>Enter the IPv4 address, Username, Password, and Upload Path.<br>**Important** - First, you must follow sk164234 to configure the SCP server as a trusted host on Gaia.<br>■ **Cloud storage**<br>In the **Cloud type** field, select the cloud vendor.<br>• **Amazon S3**<br>To send the collected backup to an Amazon S3 bucket.<br>Enter the S3 Region, S3 Bucket Name, Upload Path, S3 Access Key, and S3 Secret Access Key.<br>• **Azure Storage**<br>To send the collected backup to a Microsoft Azure storage container.<br>Enter the Storage Account, Storage Container, SAS Token, and Upload Path. |

**Important:**

- Gaia Portal does not support the change of backup file names. You can change a backup file name in the Expert mode. Make sure **not** to use special characters.
- Gaia OS backup on Quantum Maestro Orchestrators does not contain the Maestro configuration files (for example, *sgdb.json*).
  To back up the Quantum Maestro Orchestrator configuration, use this Gaia Clish command on the Quantum Maestro Orchestrator:

  ```
  set maestro export <options>
  ```

  For a use case, see sk174202.

**Restoring from a locally saved backup**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance** > **System Backup**. Refer to the **Regular Backup** section. |
| 2 | Select the backup file. |
| 3 | Click **Restore**. |

**Restoring from a remotely saved backup**

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance** > **System Backup**.<br>Refer to the **Regular Backup** section. |
| 2 | Click **Restore Remote Backup**. |
| 3 | Enter the full name of the backup file on a remote server. |
| 4 | Select the location of the backup file:<br>■ **This appliance**<br>To restore the collected backup from this appliance.<br>■ **Management**<br>To restore the collected backup from the Management Server that manages this Security Gateway.<br>■ **Private server:**<br>In the **Protocol** field, select the server type.<br>• **FTP**<br>To restore the collected backup from an FTP server.<br>Enter the IPv4 address, Username, Password, and Upload Path.<br>• **TFTP**<br>To restore the collected backup from a TFTP server<br>Enter the IPv4 address.<br>• **SCP**<br>To restore the collected backup from an SCP server.<br>Enter the IPv4 address, Username, Password, and Upload Path.<br>■ **Cloud storage**<br>In the **Cloud type** field, select the cloud vendor.<br>• **Amazon S3**<br>To restore the collected backup from an Amazon S3 bucket.<br>Enter the S3 Region, S3 Bucket Name, Upload Path, S3 Access Key, and S3 Secret Access Key.<br>• **Azure Storage**<br>To restore the collected backup from a Microsoft Azure storage container.<br>Enter the Storage Account, Storage Container, SAS Token, and Upload Path. |
| 5 | Click **Restore**. |

### Exporting an existing locally saved backup

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance** > **System Backup**.<br>Refer to the **Regular Backup** section. |
| 2 | Select the backup file. |
| 3 | Click **Export**. |
| 4 | Click **OK** to confirm.<br>Make sure you have enough free disk space on your computer. |

### Importing a local backup

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance** > **System Backup**.<br>Refer to the **Regular Backup** section. |
| 2 | Select the backup file. |
| 3 | Click **Import**. |
| 4 | Click **Browse** and select the backup file on your computer. |
| 5 | Click **Import**. |

### Deleting a locally saved backup

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance** > **System Backup**.<br>Refer to the **Regular Backup** section. |
| 2 | Select the backup file. |
| 3 | Click **Delete**. |
| 4 | Click **OK** to confirm. |

# Backing Up the System in Gaia Clish

## Syntax

### Collecting a backup and storing it locally

```
add backup local [interactive]
```

### Collecting a backup and uploading it to an SCP server

```
add backup scp ip <IPv4 Address of SCP Server> path <Path on SCP Server> username <Username on SCP Server> [password <Password in Plain Text>] [interactive]
```

### Collecting a backup and uploading it to an FTP server

```
add backup ftp ip <IPv4 Address of FTP Server> path <Path on FTP Server> username <Username on FTP Server> [password <Password in Plain Text>] [interactive]
```

### Collecting a backup and uploading it to a TFTP server

```
add backup tftp ip <IPv4 Address of TFTP Server> [interactive]
```

### Collecting a backup and uploading it to an Amazon S3 bucket

```
add backup aws region <AWS S3 Region> bucket <AWS S3 Bucket>
path <Path in AWS S3 Bucket> access-key <AWS S3 Access Key>
secret-access-key <AWS S3 Secret Access Key> [interactive]
```

```
add backup aws region <AWS S3 Region> bucket <AWS S3 Bucket>
path <Path in AWS S3 Bucket> access-key <AWS S3 Access Key>
secret-access-key <AWS S3 Secret Access Key> security-token <AWS S3 Security Token> [interactive]
```

### Collecting a backup and uploading it to a Microsoft Azure storage container

```
add backup azure storage <Azure Storage> container <Azure Container> path <Path in Azure Container> sas-token <Azure SAS Token> [interactive]
```

### Viewing the status of the latest backup

```
show backup {last-successful | logs | status}
```

### Viewing the list of local backups and their location

```
show backups
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

**Important:**

- Gaia Clish does not support the change of backup file names. You can change a backup file name in the Expert mode. Make sure **not** to use special characters.

**Example**

```
MyGW> add backup local
Creating backup package. Use the command 'show backups' to
monitor creation progress.
MyGW>
MyGW> show backup status
Performing local backup
MyGW>
MyGW> show backups
backup_--_MyGW.MyDomain.com_2024_May_20_18_04_43.tgz Mon, May
20, 2024 109.73 MB
MyGW>
```

# Restoring the System in Gaia Clish

## Syntax

### Restoring a backup from a local hard disk

```
set backup restore local<SPACE><TAB>
```

### Restoring a backup from an SCP Server

```
set backup restore scp ip <IPv4 Address of SCP Server> path
<Path on SCP Server> file <Name of Backup File> username
<Username on SCP Server> [password <Password in Plain Text>]
[interactive]
```

### Restoring a backup from an FTP Server

```
set backup restore ftp ip <IPv4 Address of FTP Server> path
<Path on FTP Server> file <Name of Backup File> username
<Username on FTP Server> [password <Password in Plain Text>]
[interactive]
```

### Restoring a backup from a TFTP Server

```
set backup restore tftp ip <IPv4 Address of TFTP Server> file
<Name of Backup File> [interactive]
```

### Restoring a backup from an Amazon S3 bucket

```
set backup restore aws region <AWS S3 Region> bucket <AWS S3
Bucket> path <Path in AWS S3 Bucket> file <Name of Backup File>
access-key <AWS S3 Access Key> secret-access-key <AWS S3 Secret
Access Key> [interactive]
```

```
set backup restore aws region <AWS S3 Region> bucket <AWS S3
Bucket> path <Path in AWS S3 Bucket> file <Name of Backup File>
access-key <AWS S3 Access Key> secret-access-key <AWS S3 Secret
Access Key> security-token <AWS S3 Security Token> [interactive]
```

### Restoring a backup from a Microsoft Azure container

```
set backup restore azure storage <Azure Storage> container
<Azure Container> path <Path in Azure Container> file <Name of
Backup File> sas-token <Azure SAS Token> [interactive]
```

**Note** - To restore the Gaia OS configuration quickly after a system failure or migration, use the Gaia Clish "`configuration`" feature (see *"Working with System Configuration in Gaia Clish" on page 699*).

# Configuring Scheduled Backups

*In This Section:*



**Important:**

- When you create a backup on a Management Server, make sure to close all SmartConsole clients. Otherwise, scheduled backup does not start.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Backup operations (in the Global Gaia Portal or Global Gaia Clish).
  To collect or import a Gaia Backup in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.
- You can configure only one schedule for one location. For example, you can configure only one schedule for an SCP server, and only one schedule for an FTP server.
- For regular backups, see *"Backing Up and Restoring the System" on page 667*.

**Note** - Gaia Operating System uses this template for the name of a scheduled backup output file regardless of the Gaia Display Format for Time and Date:

```
backup_-<Name_of_Scheduled_Backup>-_<HostName>.<Domain>_
<YYYY>_<MM>_<DD>_<HH>_<MM>_<SS>.tgz
```

Example for 20 May 2024, 18:04:43:

```
backup_-MyDailyBkp-_MyGW.MyDomain.com_2024_May_20_18_04_
43.tgz
```

**Note** - In addition to the scheduled backup file, the Gaia Operating System also creates a file with the required metadata. If you later need to upload this scheduled backup file to Check Point cloud (for example, Zero Touch), then you also have to upload this metadata file. The Gaia Operating System uses this template for the name of a scheduled backup metadata file regardless of the Gaia Display Format for Time and Date (the same file name as the scheduled backup file, with a different file extension):

```
backup_-<Name_of_Scheduled_Backup>-_<HostName>.<Domain>_
<YYYY>_<MM>_<DD>_<HH>_<MM>_<SS>.info
```

Example for 20 May 2024, 18:04:43:

```
backup_-MyDailyBkp-_MyGW.MyDomain.com_2024_May_20_18_04_
43.info
```

# Configuring Scheduled Backups in Gaia Portal

**Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

### Adding a scheduled backup

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance** > **System Backup**.<br>Refer to the **Scheduled Backup** section. |
| 2 | Click **Add Scheduled Backup**. |
| 3 | In the **Backup Name** field, enter the name of the job.<br>■ The maximum length is 15 characters.<br>■ The name can consist only of letters, numbers, or underscore "_". |

| Step | Instructions |
|---|---|
| 4 | In the **Backup Type** section, configure the location of the backup file:<br>■ **This appliance**<br>To keep the collected backup locally in the `/var/log/CPbackup/backups/` directory.<br>■ **Management**<br>To send the collected backup to the Management Server that manages this Security Gateway.<br>Enter the Username and Password for the applicable SCP user.<br>The Security Gateway (or Cluster Member) uploads the file to the `/home/<username>/` directory on the Management Server.<br>**Important** - Follow sk164234 to configure the Security Gateway (or Cluster Member) as a trusted host on the Management Server.<br>■ **Private server:**<br>In the **Protocol** field, select the server type.<br>• **FTP**<br>To send the collected backup to an FTP server.<br>Enter the IPv4 address, Username, Password, and Upload path.<br>**Important** -The username must have permissions to delete files on the FTP server.<br>• **TFTP**<br>To send the collected backup to a TFTP server.<br>Enter the IPv4 address.<br>• **SCP**<br>To send the collected backup to an SCP server.<br>Enter the IPv4 address, Username, Password, and Upload path.<br>**Important:**<br>◦ First, you must follow sk164234 to configure the SCP server as a trusted host on Gaia.<br>◦ The username must have permissions to delete files on the SCP server.<br>■ **Cloud storage**<br>In the **Cloud type** field, select the cloud vendor.<br>• **Amazon S3**<br>To send the collected backup to your Amazon S3 bucket.<br>Enter the S3 Region, S3 Bucket Name, Upload Path, S3 Access Key, and S3 Secret Access Key.<br>• **Azure Storage**<br>To send the collected backup to your Microsoft Azure storage container.<br>Enter the Storage Account, Storage Container, Shared Access Signature (SAS) Token, and Upload Path. |

| Step | Instructions |
|---|---|
| 5 | In the **Backup Schedule** section, configure the frequency for this backup (**Daily**, **Weekly**, **Monthly**, **Minute Interval**, **Hourly**). |
| 6 | **Optional:** In the **Retention Policy** section, configure the backup retention policy:<br>■ In the **Maximum backups to keep** field, configure the maximum number of backup files to save.<br>If the new backup files exceeds this number, then Gaia deletes the oldest backup file.<br>■ In the **Maximum disk space to be used (in MB)** field, configure the amount of free disk space to maintain at all times.<br>If the new backup files exceeds this number, then Gaia does not create the new backup file.<br>**Important:**<br>■ These settings apply only to the new backup files (and do not apply to existing backup files).<br>■ If the job creates a new backup file, it deletes the oldest existing backup file.<br>■ The scheduled backup job stops, if Gaia cannot meet the configured retention policy.<br>For example, the disk space limit is not enough to create a new backup file, and the minimum number of backup files does not allow to delete the existing backup files.<br>In this case, Gaia does not show a notification.<br>An administrator must manually check why Gaia did not create the new backup file.<br>■ These settings do not support a job that uploads a backup file to a TFTP server because TFTP servers cannot delete files.<br>■ These settings apply only to scheduled backup files configured and created in R82 version. |
| 7 | Click **Add**.<br>The scheduled backup appears in the **Scheduled Backups** table. |

### Deleting a scheduled backup

| Step | Instructions |
|---|---|
| 1 | In the navigation tree, click **Maintenance** > **System Backup**. Refer to the **Scheduled Backup** section. |
| 2 | Select the backup to delete. |
| 3 | Click **Delete**. |

## Configuring Scheduled Backups in Gaia Clish

**Important** - On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

### Syntax

```
add backup-scheduled name <Name of Schedule>
      aws region <AWS S3 Region> bucket <AWS S3 Bucket> path
<Path in AWS S3 Bucket> access-key <AWS S3 Access Key> secret-
access-key <AWS S3 Secret Access Key>
      azure storage <Azure Storage> container <Azure Container>
path <Path in Azure Container> sas-token <Azure SAS Token>
      ftp path <Path on FTP Server> ip <IPv4 Address of FTP
Server> username <Username on FTP Server> {password <Password in
Plain Text> | internal <Password>}
      local
      management username <SCP Username on Management Server>
password <Password in Plain Text>
      scp path <Path on SCP Server> ip <IPv4 Address of SCP
Server> username <Username on SCP Server> {password <Password in
Plain Text> | internal <Password>}
      tftp ip <IPv4 Address of TFTP Server>
```

```
set backup-scheduled name <Name of Schedule> recurrence
      daily time <HH:MM>
      hourly hours {<Hours> | all} at <0-59>
      interval minutes <1-59>
      monthly month {<Months> | all} days <Days> time <HH:MM>
      weekly days {<Days> | all} time <HH:MM>
```

```
set backup-scheduled name <Name of Schedule> retention-policy
      keep-occupied-disk-space-in-MB {<Disk Space> | 0}
      max-backups-to-keep {<Number> | 0}
      min-backups-to-keep {<Number> | 0}
```

```
show backup-scheduled <Name of Schedule>
```

```
delete backup-scheduled <Name of Schedule>
```

## Procedure

1. **Add a backup schedule**

   **Adding a backup schedule that keeps the backup file locally**

   ```
   add backup-scheduled name <Name of Schedule> local
   ```

   **Adding a backup schedule that uploads the backup file to the Management Server**

   ```
   add backup-scheduled name <Name of Schedule> management
   username <SCP Username on Management Server> password
   <Password in Plain Text>
   ```

   **Important** - Follow sk164234 to configure the Security Gateway (or Cluster Member) as a trusted host on the Management Server.

   **Adding a backup schedule that uploads the backup file to an FTP server**

   ```
   add backup-scheduled name <Name of Schedule> ftp ip <IPv4
   Address of FTP Server> path <Path on FTP Server> username
   <Username on FTP Server> password <Password on FTP Server
   in Plain Text>
   ```

   **Adding a backup schedule that uploads the backup file to an SCP server**

   ```
   add backup-scheduled name <Name of Schedule> scp ip <IPv4
   Address of SCP Server> path <Path on SCP Server> username
   <Username on SCP Server> password <Password on SCP Server
   in Plain Text>
   ```

   **Important:**
   - First, you must follow sk164234 to configure the SCP server as a trusted host on Gaia.
   - The username must have permissions to delete files on the SCP server.

   **Adding a backup schedule that uploads the backup file to a TFTP server**

   ```
   add backup-scheduled name <Name of Schedule> tftp ip <IPv4
   Address of TFTP Server>
   ```

**Adding a backup schedule that uploads the backup file to an Amazon S3 bucket**

```
add backup-scheduled name <Name of Schedule> aws region
<AWS S3 Region> bucket <AWS S3 Bucket> path <Path in AWS
S3 Bucket> access-key <AWS S3 Access Key> secret-access-
key <AWS S3 Secret Access Key>
```

**Adding a backup schedule that uploads the backup file to a Microsoft Azure storage container**

```
add backup-scheduled name <Name of Schedule> azure storage
<Azure Storage> container <Azure Container> path <Path in
Azure Container> sas-token <Azure SAS Token>
```

2. **Configure the backup schedule recurrence**

**Running one time on each day at specified time**

```
set backup-scheduled name <Name of Schedule> recurrence
daily time <HH:MM>
```

**Running several times each day at specified times**

```
set backup-scheduled name <Name of Schedule> recurrence
hourly hours {<Hours> | all} at <0-59>
```

**Running several times each day at specified intervals**

```
set backup-scheduled name <Name of Schedule> recurrence
interval minutes <1-59>
```

**Running in specified months on specified days and at specified time**

```
set backup-scheduled name <Name of Schedule> recurrence
monthly month {<Months> | all} days <Days> time <HH:MM>
```

**Running each week on specified days of week and at specified time**

```
set backup-scheduled name <Name of Schedule> recurrence
weekly days {<Days> | all} time <HH:MM>
```

3. **Configure the backup retention policy**

a. Configure the amount of free disk space to maintain:

```
set backup-scheduled name <Name of Schedule> retention-
policy keep-occupied-disk-space-in-MB {<Disk Space> | 0}
```

b. Configure the maximum number of backup files to save:

```
set backup-scheduled name <Name of Schedule> retention-
policy max-backups-to-keep {<Number> | 0}
```

c. Configure the maximum number of backup files to save:

```
set backup-scheduled name <Name of Schedule> retention-
policy min-backups-to-keep {<Number> | 0}
```

4. **Examine the scheduled backup configuration**

```
show backup-scheduled<SPACE><TAB>
show backup-scheduled <Name of Schedule>
```

### Deleting a scheduled backup

```
delete backup-scheduled<SPACE><TAB>
delete backup-scheduled <Name of Schedule>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Parameters

| Parameter | Description |
|---|---|
| `name <Name of Schedule>` | Defines the name of the scheduled backup:<br>■ The maximum length is 15 characters.<br>■ The name can consist only of letters, numbers, or underscore "_". |
| `local` | Keeps the backup file locally on this Security Gateway (or Cluster Member). Gaia keeps the file in the `/var/log/CPbackup/backups/` directory. |

| Parameter | Description |
|---|---|
| `management username <SCP Username on Management Server> password <Password in Plain Text>` | Uploads the backup file over SCP to the Management Server that manages this Security Gateway.<br>The Security Gateway (or Cluster Member) uploads the file to the `/home/<username>/` directory on the Management Server.<br>**Important** - Follow sk164234 to configure the Security Gateway (or Cluster Member) as a trusted host on the Management Server. |
| `ftp ip <IPv4 Address of FTP Server>` | Specifies the IPv4 address of the remote FTP server. |
| `scp ip <IPv4 Address of SCP Server>` | Specifies the IPv4 address of the remote SCP server.<br>**Important** - First, you must follow sk164234 to configure the SCP server as a trusted host on Gaia. |
| `tftp ip <IPv4 Address of TFTP Server>` | Specifies the IPv4 address of the remote TFTP server. |
| `path <Path on FTP Server>` | Specifies the path on the remote FTP server where to upload the backup file. |
| `path <Path on SCP Server>` | Specifies the path on the remote SCP server where to upload the backup file. |
| `path <Path in AWS S3 Bucket>` | Specifies the path AWS S3 Bucket where to upload the backup file. |
| `path <Path in Azure Container>` | Specifies the path Azure Container where to upload the backup file. |
| `username <Username on FTP Server>` | Specifies the username required to log in to the remote FTP server.<br>**Important** - The username must have permissions to delete files on the FTP server. |

| Parameter | Description |
|---|---|
| `username <Username on SCP Server>` | Specifies the username required to log in to the remote SCP server.<br>**Important** - The username must have permissions to delete files on the SCP server. |
| `password <Password in Plain Text>` | Specifies the password (in plain text) required to log in to the remote server. |
| `region <AWS S3 Region>` | Specifies the Amazon S3 Region. |
| `bucket <AWS S3 Bucket>` | Specifies the Amazon S3 Bucket. |
| `access-key <AWS S3 Access Key>` | Specifies the Amazon S3 Access Key. |
| `secret-access-key <AWS S3 Secret Access Key>` | Specifies the Amazon S3 Secret Access Key. |
| `storage <Azure Storage>` | Specifies the Microsoft Azure Storage Account. |
| `container <Azure Container>` | Specifies the Microsoft Azure Container. |
| `sas-token <Azure SAS Token>` | Specifies the Microsoft Azure Shared Access Signature (SAS) Token. |
| `recurrence daily time <HH:MM>` | Specifies that the job must run once a day - each day, at specified time.<br>Enter the time of day in the 24-hour clock format - <Hours>:<Minutes>.<br>Example:<br>`HostName> set backup-scheduled name MyBackup recurrence daily time 14:35`<br>`HostName> show backup-scheduled MyBackup`<br>`The scheduled backup is performed locally.`<br>`Every day at 14:35` |

| Parameter | Description |
|---|---|
| `recurrence hourly hours {<Hours> \| all} at <Minutes 0-59>` | Specifies that the job must run many times during the day - at the specified time.<br>■ You can specify a single hour of a day by a number from 0 to 23.<br>■ You can specify several hours of a day.<br>Enter the hours separated by commas.<br>Example - for hours 14, 15, and 16, enter: 14,15,16<br>■ To specify each hour of a day, enter: `all`<br>■ You must specify the minutes of each configured hour by a number from 0 to 59.<br>Example:<br>`HostName> set backup-scheduled name MyBackup recurrence hourly hours 14,15,16 at 35`<br>`HostName> show backup-scheduled MyBackup`<br>`The scheduled backup is performed locally.`<br>`Every day at 14:35,15:35,16:35` |

| Parameter | Description |
|---|---|
| `recurrence interval minutes <1-59>` | Specifies that the job must run many times during the day - at intervals of the specified number of minutes.<br>Example:<br>`HostName> set backup-scheduled name MyBackup recurrence interval minutes 30`<br>`HostName> show backup-scheduled MyBackup`<br>`The scheduled backup is performed locally.`<br>`Every 30 minutes.` |

| Parameter | Description |
|---|---|
| `recurrence monthly month {<Months> \| all} days <Days> time <HH:MM>` | Specifies that the job must run once a month - on the specified months, on the specified dates, and at the specified time.<br>■ Specify the months by numbers from 1 to 12:<br>January = 1, February = 2, ..., December = 12.<br>■ To specify several months, enter their numbers separated by commas.<br>Example - for January, February, and March, enter: 1,2,3<br>■ To specify each month of the year, enter: `all`<br>■ Specify the dates of a month by numbers from 1 to 31.<br>■ To specify several dates, enter their numbers separated by commas.<br>Example - for 1st, 2nd and 3rd day of month, enter: 1,2,3<br>Example:<br>`HostName> set backup-scheduled name MyBackup recurrence monthly month 1,2,3 days 1,2,3 time 14:35`<br>`HostName> show backup-scheduled MyBackup`<br>`The scheduled backup is performed locally.`<br>`Each January, February, March on days 1, 2, 3 at 14:35` |

| Parameter | Description |
|---|---|
| `recurrence weekly days {<Days> \| all} time <HH:MM>` | Specifies that the job must run once a week - on specified days of week, and at specified time.<br>■ Specify the days of a week by numbers from 0 to 6: Sunday = 0, Monday = 1, Tuesday = 2, Wednesday = 3, Thursday = 4, Friday = 5, Saturday = 6.<br>■ To specify several days of a week, enter their numbers separated by commas. Example- for Sunday, Monday, and Tuesday, enter: 0,1,2<br>■ To specify each day of the week, enter: `all`<br>Example:<br>`HostName> set backup-scheduled name MyBackup recurrence weekly days 1,3 time 14:35`<br>`HostName> show backup-scheduled MyBackup`<br>`The scheduled backup is performed locally.`<br>`Every week on Monday, Wednesday at 14:35` |

| Parameter | Description |
|---|---|
| `retention-policy <Options>` | Specifies how much disk space the backup files can take and how many backup files to keep on Gaia:<br>■ `retention-policy keep-occupied-disk-space-in-MB {<Disk Space> \| 0}`<br>Specifies how many much disk space (in megabytes) the existing backup files can take on Gaia.<br>■ `retention-policy max-backups-to-keep {<Number> \| 0}`<br>Specifies how many backup files to keep on Gaia at maximum.<br>If the job creates a new backup file, it deletes the oldest existing backup file.<br>The value for maximum number of backup files to keep must be greater than the value for minimum number of backup files.<br>■ `retention-policy min-backups-to-keep {<Number> \| 0}`<br>Specifies how many backup files to keep on Gaia at minimum. |

| Parameter | Description |
|---|---|
| | **Notes:**<br>■ Each of these retention policy settings is optional.<br>■ These settings apply only to the new backup files (and do not apply to existing backup files).<br>■ To change the current configuration, run the command again with a new value.<br>■ To disable this configuration, run the command again with the value 0 (zero).<br>■ If the job creates a new backup file, it deletes the oldest existing backup file.<br>■ If the job uploads a backup file to a remote server, the username must have permissions to delete files on the remote server.<br>■ The scheduled backup job stops, if Gaia cannot meet the configured retention policy.<br>For example, the disk space limit is not enough to create a new backup file, and the minimum number of backup files does not allow to delete the existing backup files.<br>In this case, Gaia does not show a notification.<br>An administrator must manually check why Gaia did not create the new backup file.<br>■ These settings do not support a job that uploads a backup file to a TFTP server because TFTP servers cannot delete files.<br>■ These settings apply only to scheduled backup files configured and created in R82 version. |

### Examples

- Creating a daily backup file as a local LVM volume:

```
gaia> add backup-scheduled name Daily local
gaia>
gaia> set backup-scheduled name Daily recurrence daily time
22:00
gaia>
gaia> set backup-scheduled name Daily retention-policy keep-
occupied-disk-space-in-MB 50000
gaia>
gaia> set backup-scheduled name Daily retention-policy max-
backups-to-keep 10
gaia>
gaia> set backup-scheduled name Daily retention-policy min-
backups-to-keep 3
gaia>
gaia> show backup-scheduled Daily
The scheduled backup is performed locally.
Retention-policy:
       max-backups-to-keep 10
       min-backups-to-keep 3
       keep-occupied-disk-space-in-MB 50000
Every day at 22:00
gaia>
gaia> save config
```

- Creating a monthly snapshot image as a file and uploading it to an SCP server:

```
gaia> add backup-scheduled name Monthly ftp ip 192.168.20.30
path /var/log/my_backups/ username backup_user password
123456
gaia>
gaia> set backup-scheduled name Monthly recurrence monthly
month all days 1 time 22:00
gaia>
gaia> show backup-scheduled Monthly
The scheduled backup is performed to an ftp server.
 IP: 192.168.20.30
 Username: backup_user
Every month on day 1 at 22:00
gaia>
gaia> save config
```

## Troubleshooting

Examine the location of the backup file.

Examine the `/var/log/messages` files.

# Working with System Configuration in Gaia Clish

You can save your Gaia configuration settings as a ready-to-run CLI shell script.

This feature lets you quickly restore your system configuration after a system failure or migration.

**Note** - You can only do a migration using the same Gaia version on the source and target computers.

**Important:**

- In a Management Data Plane Separation (MDPS) environment (see sk138672), you must run these commands in each plane.
- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Backup operations (in the Global Gaia Portal or Global Gaia Clish).
  To collect or import a Gaia Backup in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

## Syntax

### Saving the system configuration to a CLI script

```
save configuration <Name of Script>
```

### Restoring the configuration settings

```
load configuration <Name of Script>
```

### Viewing the latest configuration settings

```
show configuration
```

### Example

This example shows part of the configuration settings as last saved to a CLI shell script:

```
mygaia> show configuration
#
# Configuration of mygaia
# Language version: 10.0v1
#
# Exported by admin on Mon Mar 19 15:06:22 2012
#
set hostname mygaia
set timezone Asia / Jerusalem
set password-controls min-password-length 6
set password-controls complexity 2
set password-controls palindrome-check true
set password-controls history-checking true
set password-controls history-length 10
set password-controls password-expiration never
set ntp active off
set router-id 6.6.6.103
set ipv6-state off
set snmp agent off
set snmp agent-version any
set snmp community public read-only
set snmp traps trap authorizationError disable
set snmp traps trap coldStart disable
set snmp traps trap configurationChange disable
... ... ...[truncated for brevity]... ... ...
mygaia>
```

# LVM Overview

## Description

The Gaia Clish command "`show system lvm overview`" shows information about system logical volumes.

## Syntax

```
show system lvm overview
```

## Example

```
gaia> show system lvm overview
LVM overview
============
                         Size(GB)   Used(GB)   Configurable    Description
    lv_current           38         8          yes             Check Point OS and products
    lv_log               56         2          yes             Logs volume
    upgrade reserved     42         N/A        no              Reserved space for version
upgrade
    swap                 16         N/A        no              Swap memory volume
    unallocated space    148        N/A        no              Unused space
    -------              ----
    total                300        N/A        no              Total size

gaia>
```

## Related information

See *"Configuring Log Volume" on page 417*.

# Advanced Gaia Configuration

This chapter contains procedures for advanced Gaia configuration, such as SSH settings, Global Parameters on a Security Gateway, Gaia Portal Web Server.

## Resetting the Expert Mode Password on a Security Gateway

**Important:**

- On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.
- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

Follow sk106490 if you forget your Expert mode password for a Security Gateway, Cluster Member, or Scalable Platform Security Group.

# Configuring Supported SSH Ciphers, MACs, and KexAlgorithms

### Background

You can configure different settings for the SSH daemon on the Gaia Operating System.

You can configure these SSH settings in Gaia Clish:

### Available SSH Settings

| Setting | Description |
|---|---|
| SSH Ciphers | SSH uses ciphers for privacy of data it sends over an SSH connection. |
| SSH Message Authentication Codes | SSH uses Message Authentication Codes to maintain the integrity of each message it sends over and SSH connection. This provides integrity between SSH peers. |
| SSH Key Exchange Algorithms | SSH uses Key Exchange Algorithms to exchange a shared session key securely with an SSH peer. |
| SSH Client Alive Interval | In SSHv2, this is a timeout interval (in seconds), after which if no data is received from an SSH client, the *sshd* daemon sends a message through the encrypted channel to request a response from the client.<br>This controls the "`ClientAliveInterval`" parameter for the *sshd* daemon.<br>By default, this feature is disabled (the default value is 0).<br>See https://man7.org/linux/man-pages/man5/sshd_config.5.html. |
| SSH Password Authentication | Specifies whether password authentication is allowed.<br>This controls the "`PasswordAuthentication`" parameter for the *sshd* daemon.<br>By default, this feature is enabled (the default value is "`yes`").<br>See https://man7.org/linux/man-pages/man5/sshd_config.5.html. |
| SSH Permit Root Login | Specifies whether the root user can log in over SSH.<br>This controls the "`PermitRootLogin`" parameter for the *sshd* daemon.<br>By default, this feature is enabled (the default value is "`yes`").<br>See https://man7.org/linux/man-pages/man5/sshd_config.5.html. |

| Setting | Description |
|---|---|
| SSH DNS Usage | Specifies whether the *sshd* daemon needs to look up the remote hostname and make sure the resolved hostname for the remote IP address maps back to the same IP address.<br>This controls the "`UseDNS`" parameter for the *sshd* daemon.<br>By default, this feature is disabled (the default value is "`no`").<br>See https://man7.org/linux/man-pages/man5/sshd_config.5.html. |

### Complete Syntax

```
set ssh server
      cipher <Cipher>{on | off}
      client-alive-interval 0-65535
      kex <Key Exchange Algorithm> {on | off}
      mac <Message Authentication Code> {on | off}
      password-authentication {yes | no}
      permit-root-login {yes | no | without-password | prohibit-
password | forced-commands-only}
      use-dns {yes | no}
```

```
show ssh server
      cipher enabled
      cipher supported
      client-alive-interval
      kex enabled
      kex supported
      mac enabled
      mac supported
      password-authentication
      permit-root-login
      use-dns
```

### Syntax for SSH Ciphers

- To view the supported SSH Ciphers:

  ```
  show ssh server cipher supported
  ```

  These are the supported SSH Ciphers:

  - `3des-cbc`
  - `aes128-cbc`
  - `aes128-ctr`

- aes128-gcm@openssh.com
- aes192-cbc
- aes192-ctr
- aes256-cbc
- aes256-ctr
- aes256-gcm@openssh.com
- chacha20-poly1305@openssh.com
- rijndael-cbc@lysator.liu.se

- To view the enabled SSH Ciphers:

```
show ssh server cipher enabled
```

These are the SSH Ciphers that are enabled by default:

- aes128-ctr
- aes128-gcm@openssh.com
- aes192-ctr
- aes256-ctr
- aes256-gcm@openssh.com
- chacha20-poly1305@openssh.com

- To enable or disable the supported SSH Ciphers:

```
set ssh server cipher <Cipher> {on | off}
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Syntax for SSH Key Exchange Algorithms

- To view the supported SSH Key Exchange Algorithms:

```
show ssh server kex supported
```

These are the supported SSH Key Exchange Algorithms:

- curve25519-sha256
- curve25519-sha256@libssh.org
- diffie-hellman-group1-sha1

- diffie-hellman-group14-sha1
- diffie-hellman-group14-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group-exchange-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

- To view the enabled SSH Key Exchange Algorithms:

```
show ssh server kex enabled
```

These are the SSH Key Exchange Algorithms that are enabled by default:

- curve25519-sha256
- curve25519-sha256@libssh.org
- diffie-hellman-group14-sha1
- diffie-hellman-group14-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512
- diffie-hellman-group-exchange-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

- To enable or disable the supported SSH Key Exchange Algorithms:

```
set ssh server kex <Key Exchange Algorithm> {on | off}
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Syntax for SSH Message Authentication Codes (MACs)

- To view the supported SSH Message Authentication Codes:

  ```
  show ssh server mac supported
  ```

  These are the supported SSH Message Authentication Codes:

  - hmac-md5-96-etm@openssh.com
  - hmac-md5-etm@openssh.com
  - hmac-sha1
  - hmac-sha1-96-etm@openssh.com
  - hmac-sha1-etm@openssh.com
  - hmac-sha2-256
  - hmac-sha2-256-etm@openssh.com
  - hmac-sha2-512
  - hmac-sha2-512-etm@openssh.com
  - umac-64-etm@openssh.com
  - umac-64@openssh.com
  - umac-128-etm@openssh.com
  - umac-128@openssh.com

- To view the enabled SSH Message Authentication Codes:

  ```
  show ssh server mac enabled
  ```

  These are the SSH Message Authentication Codes that are enabled by default:

  - hmac-sha1
  - hmac-sha1-etm@openssh.com
  - hmac-sha2-256
  - hmac-sha2-256-etm@openssh.com
  - hmac-sha2-512
  - hmac-sha2-512-etm@openssh.com
  - umac-64-etm@openssh.com

- umac-64@openssh.com
- umac-128-etm@openssh.com
- umac-128@openssh.com

- To enable or disable the supported SSH Message Authentication Codes:

```
set ssh server mac <Message Authentication Code> {on | off}
```

**Important** - After you add, configure, or delete features, run the "save config" command to save the settings permanently.

### Syntax for SSH Client Alive Interval

- To view the current interval:

```
show ssh server client-alive-interval
```

- To configure the required interval (in seconds):

```
set ssh server client-alive-interval 0-65535
```

**Important** - After you add, configure, or delete features, run the "save config" command to save the settings permanently.

### Syntax for SSH Password Authentication

- To view the current permission:

```
show ssh server password-authentication
```

- To configure the required permission:

```
set ssh server password-authentication {yes | no}
```

**Important** - After you add, configure, or delete features, run the "save config" command to save the settings permanently.

### Syntax for SSH Permit Root Login

- To view the current permission:

```
show ssh server permit-root-login
```

- To configure the required permission:

```
set ssh server permit-root-login {yes | no | without-
password | prohibit-password | forced-commands-only}
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

### Syntax for SSH DNS Usage

- To view the current permission:

```
show ssh server use-dns
```

- To configure the required permission:

```
set ssh server use-dns {yes | no}
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

# Configuring an IPv6 Address on a Multi-Domain Server

Starting in R82, it is possible to use IPv6 addresses for the internal Check Point communication:

- Between a Multi-Domain Security Management Server, its Domain Management Servers, and their managed Security Gateways.

  This internal Check Point communication includes Secure Internal Communication (SIC), policy installation, and logging.

- Between a Multi-Domain Log Server, its Domain Log Servers, and the managed Security Gateways.

  This internal Check Point communication includes Secure Internal Communication (SIC) and logging.

- Between a Multi-Domain Security Management Server and a Multi-Domain Log Server.

  This internal Check Point communication includes Secure Internal Communication (SIC) and logging.

**Procedure to configure a new IPv6 Address on a Multi-Domain Server**

**Part 1 - Configuring the Multi-Domain Server**

1. Enable IPv6 support in the Gaia OS on the Multi-Domain Server.

   See *"System Configuration" on page 398*.

2. Reboot the Multi-Domain Server.

   See *"Shut Down" on page 664*.

3. On the **Leading Interface** of the Multi-Domain Server, configure the required IPv6 address.

   See *"Physical Interfaces" on page 103*.

4. Configure the applicable IPv6 static routes on the Multi-Domain Server.

   See *"IPv6 Static Routes" on page 279*.

5. Add the same IPv6 address you configured on the **Leading Interface** to the Multi-Domain Server database with the API command "`set-mds`":

a. In the Management API Reference:

   a. Open the chapter "**Multi-Domain**".

   b. Open the section "**Multi-Domain Server (MDS)**".

   See one of these Management API references:

   - The online *Check Point Management API Reference*.
   - The local *Management API Reference* (first, you must follow sk174606 to allow access to this local Management API reference):

     ```
     https://<IP Address or Gaia Management Interface>/api_docs/#introduction
     ```

b. Run the API command "`set-mds`":

   (The syntax below is for the CLI command "`mgmt_cli`".)

   ```
   mgmt_cli --domain 'System Data' set-mds name <Name of Multi-Domain Server Object> ipv6-address "IPv6 Address Configured on Leading Interface>"
   ```

   **Notes:**
   - In the "`name`" parameter, you must enter the name of the Multi-Domain Server object as it appears in SmartConsole.
   - If you run command in the CLI on the Primary Multi-Domain Server, then in the "`name`" parameter you can specify the name of the Secondary Multi-Domain Server object.

6. Restart the Check Point services on the Multi-Domain Server with these commands in the CLI (Gaia Clish or the Expert mode):

   a. Stop the Check Point services:

      ```
      mdsstop
      ```

   b. Start the Check Point services:

      ```
      mdsstart
      ```

7. Make sure all the required processes are running on the Multi-Domain Server with this command in the CLI (Gaia Clish or the Expert mode):

   ```
   mdsstat
   ```

8. Configure the required IPv6 address in the Domain Management Server / Domain Log Server with the applicable API command.

You can update and existing object or create a new object.

(The syntax below is for the CLI command "`mgmt_cli`".)

- To update an existing Domain Management Server / Domain Log Server object and restart it:

```
mgmt_cli set domain name "<Name of Domain Object>"
servers.update.multi-domain-server "Name of Multi-
Domain Server Object" servers.update.name "Name of
Domain Management Server or Domain Log Server Object"
servers.update.ipv6-address "<IPv6 Address of Domain
Management Server or Domain Log Server Object>"
servers.update.restart-domain-server true
```

- To create a new Domain Management Server / Domain Log Server object with both an IPv4 and an IPv6 addresses:
  - To create a new Domain Management Server and start it:

```
mgmt_cli add domain name "Name of Domain Object"
servers.1.multi-domain-server "<Name of Multi-
Domain Security Management Server Object>"
servers.1.name "<Name of Domain Management Server
Object>" servers.1.type "management server"
servers.1.ipv4-address "<IPv4 Address of Domain
Management Server Object>" servers.1.ipv6-address
"<IPv6 Address of Domain Management Server Object>"
```

    **Note** - Digit "1" in the syntax "servers.1." means the first Domain Management Server on this Multi-Domain Security Management Server. If there are already configured Domain Management Servers, then enter the next subsequent number.

  - To create a new Domain Log Server and start it:

```
mgmt_cli add domain name "Name of Domain Object"
servers.1.multi-domain-server "<Name of Multi-
Domain Log Server Object>" servers.1.name "<Name of
Domain Log Server Object>" servers.1.type "log
server" servers.1.ipv4-address "<IPv4 Address of
Domain Log Server Object>" servers.1.ipv6-address
"<IPv6 Address of Domain Log Server Object>"
```

    **Note** - Digit "1" in the syntax "servers.1." means the first Domain Log Server on this Multi-Domain Log Server. If there are already configured Domain Log Servers, then enter the next subsequent number.

9. Make sure all the required processes are running on the Multi-Domain Server with this command in the CLI (Gaia Clish or the Expert mode):

```
mdsstat
```

### Part 2 - Configuring the Security Gateways and Cluster Members

1. Enable IPv6 support in the Gaia OS on the applicable Security Gateways and each applicable Cluster Member.

   See *"System Configuration" on page 398*.

2. Reboot the Security Gateways and each Cluster Member.

   See *"Shut Down" on page 664*.

3. Configure IPv6 addresses on the applicable interfaces.

   See *"Network Interfaces" on page 102*.

4. Configure the applicable IPv6 static routes.

   See *"IPv6 Static Routes" on page 279*.

### Part 3 - Configuring the Security Gateways and Cluster objects in SmartConsole

Follow the *R82 Security Management Administration Guide*.

**Procedure to change an existing IPv6 address on a Multi-Domain Server**

1. Connect to the command line on the Multi-Domain Security Management Server.
2. Log in to the Expert mode.
3. Disable the current IPv6 configuration:

   ```
   mdsconfig -n disable_ipv6 <Name of Leading Interface>
   ```

4. Restart the Check Point services on the Multi-Domain Server:
   a. Stop the Check Point services:

      ```
      mdsstop
      ```

   b. Start the Check Point services:

      ```
      mdsstart
      ```

5. Make sure all the required processes are running on the Multi-Domain Server:

   ```
   mdsstat
   ```

6. Configure the new IPv6 address on the Leading Interface.

   Follow steps 3-7 in *"Part 1 - Configuring the Multi-Domain Server" on page 710*.

7. Change the IPv6 addresses assigned Domain Management Servers / Domain Log Servers with the API command "`set domain`":

   (The syntax below is for the CLI command "`mgmt_cli`".)

   ```
   mgmt_cli set domain name "<Name of Domain Object>"
   servers.update.multi-domain-server "<Name of Multi-Domain
   Server Object>" servers.update.name "<Name of Domain
   Management Server or Domain Log Server Object>"
   servers.update.ipv6-address "<IPv6 Address of Domain
   Management Server or Domain Log Server Object>"
   servers.update.restart-domain-server true
   ```

8. Make sure all the required processes are running on the Multi-Domain Server:

   ```
   mdsstat
   ```

# Working with Global Parameters on a Security Gateway

## Background

On a Security Gateway, Cluster Members, and Scalable Platform Security Group, you can control the default behavior of specific features by changing the values of the corresponding Check Point global parameters.

In the versions R81.20 and lower, you must configure the required values of the Check Point global parameters in various configuration files.

For example:

- You configure the Firewall kernel parameters in the `$FWDIR/boot/modules/fwkern.conf` file.
- You configure the SecureXL kernel parameters in the `$PPKDIR/conf/simkern.conf` file.

Starting in R82, you can view and configure the required values of the Check Point global parameters in these ways:

| Configuration Method | Description and Instructions |
|---|---|
| Centralized Database | **Important:**<br>The R82 release contains the new infrastructure.<br>Full support for the kernel parameters will be added gradually in the R82 Jumbo Hotfix Accumulator.<br>If cannot configure a kernel parameter using the new infrastructure, then use the legacy configuration files.<br>The information below describes the complete feature as if it already supports the configuration of kernel parameters.<br>**Important** - The centralized database has a higher priority than the legacy configuration files.<br>This method changes the value of the Check Point global parameters (in the current session, or permanently) in a centralized database instead of editing the legacy configuration files.<br>This feature is called "**Config Point**".<br>Use one of these commands:<br>■ CLI commands in Gaia Clish / Gaia gClish (**recommended**):<br>• `show global-param`<br>See *"Syntax to View Global Parameters in Gaia Clish / Gaia gClish" on page 719*.<br>• `set global-param`<br>See *"Syntax to Configure Global Parameters in Gaia Clish / Gaia gClish" on page 721*.<br>■ CLI command in the Expert mode:<br>• `confp_cli`<br>See *"Syntax to View and Configure Global Parameters in the Expert mode" on page 724*.<br>■ Gaia REST API calls:<br>• `show-global-params`<br>• `set-global-params`<br>See one of these Gaia API References:<br>• Online *Check Point Gaia API Reference* v1.8 (and higher) > Section "*Global Parameters*".<br>• Local *Check Point Gaia API Reference* on your Gaia server:<br>◦ `https://<IPv4 Address of Gaia>/gaia_docs/#web/show-global-params~v1.8%20`<br>◦ `https://<IPv4 Address of Gaia>/gaia_docs/#web/set-global-params~v1.8%20`<br>See *"Working with Gaia RESTful API" on page 749*. |

| Configuration Method | Description and Instructions |
|---|---|
| | **Notes:**<br>■ During an upgrade to R82 and during each boot of R82, Gaia OS automatically:<br>1. Transfers the configured kernel parameters (that are not commented out) from the legacy configuration files `$FWDIR/boot/modules/fwkern.conf` and `$FWDIR/boot/modules/fwkern.conf` to the centralized database.<br>Support for more legacy configuration files is planned for later versions.<br>2. Comments out the configured kernel parameters in the legacy configuration files (adds the # character in the beginning of the line and adds the corresponding command at the end of the line).<br>■ If a kernel parameter value is already configured in the centralized database, and you configure a value for the same kernel parameter in the legacy configuration file, then during the next boot, the value from the legacy configuration file overrides the previous value in the centralized database. |
| Legacy Configuration Files | This method changes the value of the Check Point global parameter in one of the legacy configuration files as done in R81.20 and lower.<br>For example, you configure kernel parameters in these files:<br>■ `$FWDIR/boot/modules/fwkern.conf`<br>■ `$PPKDIR/conf/simkern.conf`<br>Use these CLI commands (in Gaia Clish or the Expert mode) to configure kernel parameters:<br>■ `fw ctl get int ...`<br>■ `fw ctl get str ...`<br>■ `fw ctl set [-f] int ...`<br>■ `fw ctl set [-f] str ...`<br>For the complete procedure to configure kernel parameters, see the *R82 Quantum Security Gateway Guide* > Chapter "*Working with Kernel Parameters*". |

# Syntax to View Global Parameters in Gaia Clish / Gaia gClish

**Syntax**

**Notes:**

- On a VSNext Gateway / Legacy VSX Gateway, you must go to the context of the of the applicable Virtual Gateway / Virtual System:

  ```
  set virtual-system <ID>
  ```

- The command "`show global-param`" does **not** show the kernel parameters configured in the legacy configuration files.

```
show global-param all
      [filter-by]
            modified [format {json | table}]
            not-default [format {json | table}]
            with-comments [format {json | table}]
      [format {json | table}]
```

```
show global-param path {all | <Full Path in DB> | <Path with
Wildcards in DB>}
      [filter-by]
            modified [format {json | table}]
            not-default [format {json | table}]
            with-comments [format {json | table}]
      [format {json | table}]
```

**Parameters**

| Parameter | Description |
|---|---|
| `show global-param all` | Shows all global parameters with values, descriptions, and comments. |
| `filter-by` | Specifies a filter for the output:<br>■ `modified`<br>Shows global parameters, whose values were configured explicitly.<br>■ `not-default`<br>Shows global parameters, whose values are not default.<br>■ `with-comments`<br>Shows global parameters with comments. |
| `format {json \| table}` | Specifies the output format:<br>■ `json` - JSON.<br>■ `table` - table (this is the default). |
| `show global-param path <Path in DB>` | Specifies the path of a global parameter in the database:<br>■ `all`<br>Shows all global parameters.<br>■ *`<Full Path in DB>`*<br>Shows the global parameters based on the specified full path in the database.<br>■ *`<Path with Wildcards in DB>`*<br>Shows the global parameters based on the specified path with wildcards "`*`" in the database:<br>a. Enter the relevant path characters (at least 2 characters).<br>b. Enter the `*` character in the relevant place.<br>c. If needed, enter the relevant path characters.<br>d. Press the Space key.<br>e. Enter the sub-command "`use-regex true`".<br>f. Press the Tab key to see the next available sub-command. |

# Syntax to Configure Global Parameters in Gaia Clish / Gaia gClish

**Syntax**

**Note** - On a VSNext Gateway / Legacy VSX Gateway, you must go to the context of the of the applicable Virtual Gateway / Virtual System:

```
set virtual-system <ID>
```

```
set global-param path <Parameter Path in DB>
      comment "Comment Text"
      param-value <Parameter Value>
            comment "Comment Text"
            use-regex {true | false} dry-run {true | false}
            volatile true use-regex {true | false} dry-run {true
| false}
      use-default {true | false}
            comment "Comment Text"
            use-regex {true | false} dry-run {true | false}
            volatile true use-regex {true | false} dry-run {true
| false}
      volatile {true | false} use-regex {true | false} dry-run
{true | false}
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

**Parameters**

| Parameter | Description |
|---|---|
| `set global-param path <Parameter Path in DB>` | Configures the global parameter settings in the database. You must specify one of these paths for the global parameter:<br>■ The full path in the database.<br>■ The path with wildcards "`*`" in the database:<br>a. Enter the relevant path characters (at least 2 characters).<br>b. Enter the `*` character in the relevant place.<br>c. If needed, enter the relevant path characters.<br>d. Press the Space key.<br>e. Enter the sub-command "`use-regex true`".<br>f. Press the Tab key to see the next available sub-command. |
| `comment "Comment Text"` | Configures the comment text (up to 256 characters) for the specified global parameter(s). |
| `param-value <Parameter Value>` | Configures a new value for the specified global parameter (s).<br>Different global parameters accept different value types:<br>■ integer.<br>■ boolean.<br>■ string.<br>The required values are provided in *Check Point Support Center* and by Check Point Support Engineers. |
| `use-default {true \| false}` | Specifies whether to configure (`true`) or not (`false`, this is the default) the default value for the specified global parameter. |

| Parameter | Description |
|---|---|
| `volatile {true \| false}` | Specifies whether to configure the new value only temporarily for the specified global parameter:<br>**Important** - By default, the new value is configured permanently.<br>■ `volatile true`<br>Configures the new value for the specified global parameter only temporary - until the next reboot, or until you run "`volatile false`".<br>During the next boot, the previous value of the specified global parameter is restored.<br>■ `volatile false`<br>Restores the previous value for the specified global parameter after you ran "`volatile true`". |
| `use-regex {true \| false}` | Specifies whether the specified global parameter's path includes wildcards "`*`" (`true`) or not (`false`, this is the default). |
| `dry-run {true \| false}` | Specifies whether to save the new value for the specified global parameter permanently in the database:<br>■ `dry-run true`<br>Does not save the new value for the specified global parameter - the change does not survive the reboot.<br>■ `dry-run false`<br>Saves the new value for the specified global parameter - the change survives the reboot. |

# Syntax to View and Configure Global Parameters in the Expert mode

**Syntax**

**Notes:**

- On a VSNext Gateway / Legacy VSX Gateway, you must do one of these:
  - Run the command with the parameter "`-vsid <ID>`".
  - Go to the context of the of the applicable Virtual Gateway / Virtual System:

    ```
    vsenv <ID>
    ```
- The "`confp_cli show`" command does **not** show the kernel parameters configured in the legacy configuration files.

```
confp_cli show
      [-p <Parameter Path in DB>]
      [{-fo | --format} {json | table}]
      [{-fi | --filter} {modified | not-default | with-
comments}]
      [-vsid <ID>]
      [--member-id <Member ID>]
      ['<JSON input>']
```

```
confp_cli set
      [-p <Parameter Path in DB>]
      [-v <Parameter Value>]
      [-c "<Comment Text>"]
      [-d {true | false}]
      [-vsid {<ID> | all}]
      [{-vo | --volatile} {true | false}]
      [--regex {true | false}]
      [--dry-run {true | false}]
      [--distribute {true | false}]
      ['<JSON input>']
```

```
confp_cli fetch
```

```
confp_cli get
      [-p <Parameter Path in DB>]
      [-vsid <ID>]
```

```
confp_cli get_value
      [-p <Parameter Path in DB>]
      [-vsid <ID>]
      [{-fo | --format} {json | string | fwset}]
```

**Parameters**

| Parameter | Description |
|---|---|
| `confp_cli show` | Shows all global parameters with values, descriptions, and comments.<br>■ `-p <Parameter Path in DB>`<br>Specifies the path of a global parameter in the database:<br>• `all`<br>Shows all global parameters.<br>• *`<Full Path in DB>`*<br>Shows the global parameters based on the specified full path in the database.<br>• *`<Partial Path in DB>`*<br>Shows the global parameters based on the path that starts with the specified characters in the database.<br>• *`<Path with Wildcards in DB>`*<br>Shows the global parameters based on the specified path with wildcards "`*`" in the database:<br>a. Enter the relevant path characters (at least 2 characters).<br>b. Enter the `*` character in the relevant place.<br>c. If needed, enter the relevant path characters.<br>You must also enter "`--regex true`".<br>■ `{-fo \| --format} {json \| table}`<br>Specifies the output format:<br>• `json` - JSON.<br>• `table` - table (this is the default). |

| Parameter | Description |
|---|---|
| | ■ `{-fi \| --filter} {modified \| not-default \| with-comments}`<br>Specifies a filter for the output:<br>• `modified`<br>Shows global parameters, whose values were configured explicitly.<br>• `not-default`<br>Shows global parameters, whose values are not default.<br>• `with-comments`<br>Shows global parameters with comments.<br>■ `-vsid <ID>`<br>On a VSNextGateway, specifies the ID of the Virtual Gateway.<br>On a Legacy VSX Gateway, specifies the ID of the Virtual System.<br>■ `--member-id <Member ID>`<br>On a Scalable PlatformSecurity Group, specifies the ID of the Security Group Member.<br>■ `'<JSON input>'`<br>Specifies the input in the JSON format. Must be enclosed in single quote characters (`' '`). |
| `confp_cli set` | Configures the parameter value and comment<br>■ `-p <Parameter Path in DB>`<br>Specifies the path of a global parameter in the database.<br>You must specify one of these paths for the global parameter:<br>• The full path in the database.<br>• The partial path that starts with the specified characters in the database.<br>• The path with wildcards "`*`" in the database:<br>a. Enter the relevant path characters (at least 2 characters).<br>b. Enter the `*` character in the relevant place.<br>c. If needed, enter the relevant path characters.<br>You must also enter "`--regex true`".<br>■ `-v <Parameter Value>`<br>Specifies the new value for the global parameter.<br>Different global parameters accept different value types:<br>• integer.<br>• boolean.<br>• string.<br>The required values are provided in *Check Point Support Center* and by Check Point Support Engineers. |

| Parameter | Description |
|---|---|
| | ■ `-c "<Comment Text>"`<br>Configures the comment text (up to 256 characters) for the specified global parameter(s).<br>■ `-d {true \| false}`<br>Specifies whether to configure (`true`) or not (`false`, this is the default) the default value for the specified global parameter.<br>■ `-vsid {<ID> \| all}`<br>On a VSNextGateway, specifies the ID of the Virtual Gateway.<br>On a Legacy VSX Gateway, specifies the ID of the Virtual System.<br>Enter "`all`" to apply the command to all IDs.<br>■ `{-vo \| --volatile} {true \| false}`<br>Specifies whether to configure the new value only temporarily for the specified global parameter:<br>**Important** - By default, the new value is configured permanently.<br>• `{-vo \| --volatile} true`<br>Configures the new value for the specified global parameter only temporary - until the next reboot, or until you run "`{-vo \| --volatile} false`".<br>During the next boot, the previous value of the specified global parameter is restored.<br>• `{-vo \| --volatile} false`<br>Restores the previous value for the specified global parameter after you ran "`{-vo \| --volatile} true`" |

| Parameter | Description |
|---|---|
| | ■ `--regex {true \| false}`<br>Specifies whether the specified global parameter's path includes wildcards "`*`" (`true`) or not (`false`, this is the default).<br>■ `--dry-run {true \| false}`<br>Specifies whether to save the new value for the specified global parameter permanently in the database:<br>• `--dry-run true`<br>Does not save the new value for the specified global parameter - the change does not survive the reboot.<br>• `--dry-run false`<br>Saves the new value for the specified global parameter - the change survives the reboot.<br>■ `--distribute {true \| false}`<br>On a Scalable PlatformSecurity Group, specifies whether to configure (`true`, this is the default) or not (`false`) the specified global parameters on all other Security Group Members.<br>■ `'<JSON input>'`<br>Specifies the input in the JSON format. Must be enclosed in single quote characters (`' '`). |
| `confp_cli fetch` | Shows the names of all the existing global parameters. |
| `confp_cli get` | Shows the parameters, their values, and user tags:<br>■ `-p <Parameter Path in DB>`<br>You must specify one of these paths for the global parameter:<br>• The full path in the database.<br>• The partial path that starts with the specified characters in the database.<br>■ `-vsid <ID>`<br>On a VSNext Gateway, specifies the ID of the Virtual Gateway.<br>On a Legacy VSX Gateway, specifies the ID of the Virtual System. |

| Parameter | Description |
|---|---|
| `confp_cli get_value` | Shows the parameters and their current values only:<br>■ `-p <`*`Parameter Path in DB`*`>`<br>You must specify one of these paths for the global parameter:<br>• The full path in the database.<br>• The partial path that starts with the specified characters in the database.<br>■ `-vsid <`*`ID`*`>`<br>On a VSNext Gateway, specifies the ID of the Virtual Gateway.<br>On a Legacy VSX Gateway, specifies the ID of the Virtual System.<br>■ `{-fo \| --format} {json \| string \| fwset}`<br>Specifies the output format:<br>• `json` - JSON (this is the default).<br>• `string` - String.<br>• `fwset` - Check Point FWSET format. |

# Syntax to Control the 'Config Point' in the Expert mode

### Syntax

**Note** - This command is for advanced troubleshooting only.
In the VSNext / VSX mode, this command applies to the entire Security Gateway.

```
config_point
      confirm_fixed_warnings
      generate_docs [{-s|--schema} <Full Path to Schema File>]
      restart
      start
      stop
      validate_schema [{-s|--schema} <Full Path to Schema File>]
```

### Parameters

| Parameter | Description |
|---|---|
| `confirm_fixed_warnings` | Confirms that you resolved warnings / errors that appeared after an upgrade to R82.<br>For "Config Point" troubleshooting, see sk181917. |
| `generate_docs [{-s \| --schema} <Full Path to Schema File>]` | Generates documentation for schema files.<br>If you do not specify a schema file, then this command generates documentation for all schema files in the `/config_point/schemas/` directory. |
| `restart` | Restarts the 'Config Point' server. |
| `start` | Starts the 'Config Point' server after you stopped it. |
| `stop` | Stops the 'Config Point' server. |
| `validate_schema [{-s \| --schema} <Full Path to Schema File>]` | Validates the schema files.<br>If you do not specify a schema file, then this command validates all schema files in the `/config_point/schemas/` directory. |

# Configuring the Gaia Portal Web Server

**Important:**

- On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.
- On Scalable Platforms (ElasticXL, Maestro, and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

## Background

You can configure the web server responsible for the Gaia Portal.

## Syntax

- To show the Gaia Portal web server configuration:

```
show web
      daemon-enable
      session-timeout
      ssl-port
      ssl3-enabled
      table-refresh-rate
```

- To configure the Gaia Portal web server:

```
set web
      daemon-enable {on | off}
      session-timeout <Timeout>
      ssl-port <Port>
      ssl3-enabled {on | off}
      table-refresh-rate <Rate>
```

**Important** - After you add, configure, or delete features, run the "`save config`" command to save the settings permanently.

## Parameters

| Parameter | Description |
|---|---|
| `daemon-enable {on \| off}` | Enables or disables the Gaia Portal web daemon.<br>■ **Range:** `on`, or `off`<br>■ **Default:** `on` |

| Parameter | Description |
|---|---|
| `session-timeout <Timeout>` | Configures the time (in minutes), after which the HTTPS session to the Gaia Portal terminates.<br>■ **Range:** `1 - 720`<br>■ **Default:** `15` |
| `ssl-port <Port>` | Configures the TCP port number, on which the Gaia Portal can be accessed over HTTPS.<br>■ **Range:** `1 - 65535`<br>■ **Default:** `443`<br>Use this command for initial configuration only.<br>Changing the port number on the command line may cause inconsistency with the setting defined in SmartConsole. Use SmartConsole to set the SSL port for the Portal.<br>**Note** - This setting does **not** affect HTTP connections. Normally this port should be left at the default 443. If you change the port number, you must change the URL used to access the Gaia Portal<br>from `https://<Hostname or IP Address>/`<br>to `https://<Hostname or IP Address>:<PORTNUMBER>` |
| `ssl3-enabled {on \| off}` | Enables or disables the HTTPS SSLv3 connection to Gaia Portal.<br>■ **Range:** `on`, or `off`<br>■ **Default:** `off` |
| `table-refresh-rate <Rate>` | Configures the refresh rate (in seconds), at which some tables in the Gaia Portal are refreshed.<br>■ **Range:** `10 - 240`<br>■ **Default:** `10` |

# lightshot

**Notes:**

- You must run this command in the Expert mode.
- In Gaia gClish, use these commands:
  - `add lightshot`
  - `show lightshot`
  - `show lightshots`
  - `show lightshot-partition`
  - `set lightshot`
  - `set lightshot-partition`
  - `delete lightshot`

### Description

Utility to work with light Gaia OS snapshots.

The log file for this utility: `/var/log/lightshot.log`

The utility saves the snapshots in this partition: `/mnt/lightshot`

### Syntax

```
lightshot -h
```

```
lightshot [--ip <IP Address> [--username <Username>] [--pswd
<Password>]] [--format {txt | json | yaml}
      callback
            -h
            update-token
```

```
lightshot [--ip <IP Address> [--username <Username>] [--pswd
<Password>]] [--format {txt | json | yaml}
      clone
            -h
            --reboot
            --ssh-mode
```

```
lightshot [--ip <IP Address> [--username <Username>] [--pswd
<Password>]] [--format {txt | json | yaml}
      create
            -h
           [--descr <"Description>"]
           [--force]
           [<Name of Snapshot>]
```

```
lightshot [--ip <IP Address> [--username <Username>] [--pswd
<Password>]] [--format {txt | json | yaml}
      delete
            -h
           [--fcd]
           [--force]
           [--keep <Number>]
           [<Name of Snapshot>]
```

```
lightshot [--ip <IP Address> [--username <Username>] [--pswd
<Password>]] [--format {txt | json | yaml}
      expert
            -h
            mount
            show-token
            umount
            update-token
```

```
lightshot [--ip <IP Address> [--username <Username>] [--pswd
<Password>]] [--format {txt | json | yaml}
      import
            -h
           [<Name of Snapshot>]
```

```
lightshot [--ip <IP Address> [--username <Username>] [--pswd
<Password>]] [--format {txt | json | yaml}
      restore
            -h
           [--fcd]
           [--now]
           [--reboot]
           [<Name of Snapshot>]
```

```
lightshot [--ip <IP Address> [--username <Username>] [--pswd
<Password>]] [--format {txt | json | yaml}
      set
            -h
            configuration
                  -h
                  state {enabled | disabled}
                  verbosity {0 | 1 | 2 | 3}
```

```
lightshot [--ip <IP Address> [--username <Username>] [--pswd
<Password>]] [--format {txt | json | yaml}
      show
            -h
            configuration
                  -h
                  savelogs
            diff
                  -h
                  <Name of Snapshot 1> <Name of Snapshot 1>
            partition
                  -h
                  [--filter <Parameter>]
            snapshot
                  -h
                  [--name <Name of Snapshot>]
            snapshots
                  -h
                  [--verbose]
```

### Parameters

| Parameter | Description |
|---|---|
| `-h` | Shows the built-in help. |
| `--ip <IP Address` | Specifies the IP address of a remote Gaia server.<br>This IP address must be reachable over the SSH protocol.<br>■ `--username <Username>]`<br>Specifies the username for an SSH connection.<br>This username must have root permissions.<br>■ `--pswd <Password>`<br>Specifies the password for an SSH connection. |

| Parameter | Description |
|---|---|
| `--format {txt \| json \| yaml}` | Specifies the output format:<br>■ `txt` - Plain text (this is the default)<br>■ `json` - JSON<br>■ `yaml` - YAML |
| `lightshot callback` | Deletes the registered request to restore a lightshot snapshot (with the "`lightshot restore`" sub-command) during the next reboot.<br>This command works only if you did not reboot the Gaia server yet. |
| `lightshot clone <Parameters>` | Clones the lightshot snapshot from a remote Gaia server to this Gaia server.<br>■ `--ssh-mode`<br>Forces to use the SSH protocol.<br>■ `--reboot`<br>Forces to reboot after the cloning.<br>These parameters are mandatory for this sub-command: `--ip <IP Address> [--username <Username>] [--pswd <Password>]` |
| `lightshot create <Parameters>` | Creates a new lightshot snapshot.<br>■ `--descr <"Description>"`<br>Specifies the description for this snapshot.<br>■ `--force`<br>Forces the update of an existing snapshot file.<br>■ `<Name of Snapshot>`<br>Specifies the name of the snapshot. |
| `lightshot delete <Parameters>` | Deletes an existing lightshot snapshot.<br>■ `--fcd`<br>Forces the deletion of an entire partition.<br>■ `--force`<br>Forces the deletion of an existing snapshot file.<br>■ `--keep <Number>`<br>Configures the number of last snapshots to keep.<br>In the last parameter "`<Name of Snapshot>`", you can enter a string to filter for snapshots, whose name contains this string.<br>■ `<Name of Snapshot>`<br>Specifies the name of the snapshot. |

| Parameter | Description |
|---|---|
| `lightshot expert <Parameters>` | Expert sub-commands:<br>■ `mount`<br>■ `show-token`<br>■ `umount`<br>■ `update-token` |
| `lightshot import <Parameters>` | Imports the lightshot snapshot from a remote Gaia server to this Gaia server.<br>■ *<Name of Snapshot>*<br>Specifies the name of the snapshot. |
| `lightshot restore <Parameters>` | Restores an existing lightshot snapshot on this Gaia server. You must make sure that the size of the Lightshot partition equals, at a minimum, to the size of the snapshot you need to restore.<br>■ `--fcd`<br>Forces the restoration of an entire partition.<br>■ `--now`<br>Forces the immediate restoration.<br>■ `--reboot`<br>Forces the restoration after a reboot.<br>■ *<Name of Snapshot>*<br>Specifies the name of the snapshot. |
| `lightshot set <Parameters>` | Configures the lightshot snapshot settings.<br>■ `configuration savelogs state`<br>Enables or disables (this is the default) the saving of the logs state.<br>■ `configuration savelogs verbosity {0 \| 1 \| 2 \| 3}`<br>Configures the log verbosity level:<br>• `0` - General Log (this is the default)<br>• `1` - General Log, and Commands<br>• `2` - General Log, Commands, and HCP<br>• `3` - General Log, Commands, HCP, CPInfo, and CPviewDB |
| `lightshot show configuration <Parameters>` | Shows the lightshot configuration for logs.<br>■ `configuration savelogs`<br>Shows the log state and log verbosity level. |

| Parameter | Description |
|---|---|
| `lightshot show diff <Parameters>` | Compares two specified lightshot snapshots. |
| `lightshot show partition <Parameters>` | Shows the information about the Lightshot partition.<br>■ `partition --filter <Parameter>`<br>Shows only the specified parameter:<br>• `available`<br>• `mount-on`<br>• `required-space`<br>• `size`<br>• `used` |
| `lightshot show snapshot <Parameters>` | Shows the specified existing lightshot snapshots (Name, Description, Date and Time). |
| `lightshot show snapshots <Parameters>` | Shows all existing lightshot snapshots (Name, Description, Date and Time).<br>■ `snapshots --verbose`<br>Also shows the snapshot size (this output can take some time). |

# Monitoring Transceivers

## Background

To connect fiber optic cables to Check Point Appliances, you use Small Form-Factor Pluggable (SFP) and Quad Small Form-factor Pluggable (QSFP) transceivers.

The Gaia Clish commands described below provide real-time data about the transceivers installed in the Appliance

## Viewing Information About an Interface Transceiver

### Syntax

```
show interface <Name of Interface> xcvr
```

### Example Output

```
gaia> show interface eth1-01 xcvr

 Port  Check Point  Temp  Voltage  Laser Bias  Transmit  Rec
LOS   Transmitter
        Certified   (°C)     (V)     Current     Power   Power
       Fault
       Transceiver                    (mA)       (dBm)    (dBm)
 ----     ---       -----  -----    ------     -----    -----  -
--    -------
eth1-01   Yes       26.53  3.35     39.19      -1.30    -0.02
Off      Off

gaia>
```

# Viewing Detailed Information About an Interface Transceiver

### Syntax

```
show interface <Name of Interface> xcvr_detail
```

### Example Output

```
gaia> show interface eth1-01 xcvr_detail

eth1-01 SFP is present
Product Type: 10G Base-LR
Vendor name: FINISAR CORP.
Vendor PN: FTLX1471D3BCV-CK
Vendor rev: A
Vendor SN: AWN0L3T
Check Point part number: CPAC-TR-10LR
Check Point Material ID: 309856
Laser wavelength: 1310nm
Link Length for SMF,km: 10km
Link Length for SMF: 10000m
Link Length for 50um: 0m
Link Length for 62.5um: 0m
Link Length for Copper: 0m
Link Length for OM3: 0m
No tx fault, No rx loss

QSFP Diagnostic Information
-------------------------------------------------------------------
----------------
                                        Alarms
Warnings
                                   High         Low          High
     Low
-------------------------------------------------------------------
----------------
Temperature    26.80 C           78.00 C     -13.00 C    73.00 C
     -8.00 C
Voltage         3.35 V            3.70 V       2.90 V     3.60 V
      3.00 V
Current        39.21 mA          85.00 mA      7.00 mA   80.00
mA     12.00 mA
Tx Power       -1.29 dBm          2.00 dBm    -8.00 dBm   1.00
dBm    -7.00 dBm
Rx Power       -0.02 dBm          2.50 dBm   -20.00 dBm   2.00
dBm   -18.01 dBm

gaia>
```

# Viewing Information About Transceivers for All Interfaces

### Syntax

```
show interfaces xcvr
```

### Example Output

```
gaia> show interfaces xcv

 Port  Check Point  Temp  Voltage  Laser Bias  Transmit  Rec
LOS   Transmitter
        Certified   (°C)     (V)     Current     Power   Power
       Fault
       Transceiver                    (mA)       (dBm)    (dBm)
 ----     ---       -----  -----    ------     -----    -----  -
--    -------
eth1    transceiver information not available
eth1-01   Yes       26.94  3.35     39.30      -1.30    -0.06
Off      Off
eth1-02   Yes       30.36  3.35      8.79      -2.53    -2.86
Off      Off
eth1-03   Yes       27.96  3.35     35.08      -1.43    -0.53
Off      Off
eth1-04 transceiver information not available
eth2    transceiver information not available
eth2-01   Yes       27.46  3.35      7.51      -2.18    -2.78
Off      Off
eth2-02 transceiver information not available
eth2-03 transceiver information not available
eth2-04 transceiver information not available
eth3    transceiver information not available
eth4    transceiver information not available
eth5    transceiver information not available
eth6    transceiver information not available
eth7    transceiver information not available
eth8    transceiver information not available

gaia>
```

# Viewing Detailed Information About Transceivers for All Interfaces

### Syntax

```
show interfaces xcvr_detail
```

### Example Output

```
gaia> show interfaces xcvr_detail
eth1 no information available

eth1-01 SFP is present
Product Type: 10G Base-LR
Vendor name: PROLABS
Vendor PN: ER-SFP-10G-I-CPA
Vendor rev: A1__
Vendor SN: CPT111BF7903
Check Point part number: CPAC-TR-10ER-C
Check Point Material ID: 328822
Laser wavelength: 1550nm
Link Length for SMF,km: 40km
Link Length for SMF: 25500m
Link Length for 50um: 0m
Link Length for 62.5um: 0m
Link Length for Copper: 0m
Link Length for OM3: 0m
No tx fault, Yes rx loss

QSFP Diagnostic Information
-------------------------------------------------------------------
---------------
                                        Alarms
Warnings
                                   High        Low          High
     Low
-------------------------------------------------------------------
---------------
Temperature    33.32 C           88.00 C     -43.00 C    85.00 C
    -40.00 C
Voltage         3.33 V            3.60 V       3.00 V     3.50 V
      3.10 V
Current        67.08 mA         120.00 mA     10.00 mA  110.00
mA     20.00 mA
Tx Power        1.08 dBm          5.00 dBm    -3.00 dBm   4.00
dBm    -2.00 dBm
Rx Power        1.88 dBm          1.50 dBm   -20.00 dBm   0.50
dBm   -18.01 dBm
```

```
eth1-02 SFP is present
Product Type: 10G Base-SR
Vendor name: FINISAR CORP.
Vendor PN: FTLX8574D3BCV-CP
Vendor rev: A
Vendor SN: UWC2M1S
Check Point part number: CPAC-TR-10SR-B
Check Point Material ID: 317353
Laser wavelength: 850nm
Link Length for SMF,km: 0km
Link Length for SMF: 0m
Link Length for 50um: 80m
Link Length for 62.5um: 30m
Link Length for Copper: 0m
Link Length for OM3: 300m
No tx fault, No rx loss

QSFP Diagnostic Information
-------------------------------------------------------------------
----------------
                                        Alarms
Warnings
                                  High        Low         High
     Low
-------------------------------------------------------------------
----------------
Temperature    30.46 C           78.00 C     -13.00 C    73.00 C
     -8.00 C
Voltage         3.33 V            3.70 V       2.90 V     3.60 V
      3.00 V
Current         8.56 mA          13.20 mA      2.00 mA   12.60
mA      3.00 mA
Tx Power       -2.67 dBm          0.00 dBm    -8.00 dBm  -1.00
dBm    -7.00 dBm
Rx Power       -2.98 dBm          0.00 dBm   -20.00 dBm  -1.00
dBm   -18.01 dBm


eth1-03 SFP is present
Product Type: 10G Base-LR
Vendor name: FINISAR CORP.
```

```
or PN: FTLX8574D3BCV-CP
Vendor rev: A
Vendor SN: A0SC750
Check Point part number: CPAC-TR-10SR-B
Check Point Material ID: 317353
Laser wavelength: 850nm
Link Length for SMF,km: 0km
Link Length for SMF: 0m
Link Length for 50um: 80m
Link Length for 62.5um: 30m
Link Length for Copper: 0m
Link Length for OM3: 300m
No tx fault, No rx loss

QSFP Diagnostic Information
-----------------------------------------------------------------
----------------
                                          Alarms
Warnings
                                    High         Low          High
     Low
-----------------------------------------------------------------
----------------
Temperature    27.19 C           78.00 C     -13.00 C    73.00 C
     -8.00 C
Voltage         3.34 V            3.70 V       2.90 V     3.60 V
      3.00 V
Current         8.64 mA          13.20 mA      2.00 mA   12.60
mA      3.00 mA
Tx Power       -2.31 dBm          0.00 dBm    -8.00 dBm  -1.00
dBm    -7.00 dBm
Rx Power       -2.60 dBm          0.00 dBm   -20.00 dBm  -1.00
dBm   -18.01 dBm

eth2-02 no information available
eth2-03 no information available
eth2-04 no information available
eth3 no information available
eth4 no information available
eth5 no information available
eth6 no information available
eth7 no information available
eth8 no information available

gaia>
```

# CPUSE - Software Updates

**Important** - It is **not** supported to manually upgrade the CPUSE Agent on Scalable Platforms (Known Limitation MBS-2372).

With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself. The software update packages and full images are for major releases, minor releases and Hotfixes. All of the CPUSE processes are handled by the Deployment Agent daemon (DA).

Gaia automatically locates and shows the available software update packages and full images that are applicable to the Gaia operating system version installed on the computer, the computer's role (Security Gateway, Security Management Server, Standalone), and other specific properties. The images and packages can be downloaded from the *Check Point Support Center* and installed.

You can add a private package to the list of available packages. A private package is a Hotfix, which is located on the Check Point Support Center, and is only available to limited audiences.

When you update Check Point software, make sure to:

- Define the CPUSE policy for downloads and installation.

  Downloads can be:

  - Manual
  - Automatic
  - Scheduled (daily, weekly, monthly, or one time only).

  Installations are:

  - Hotfixes are downloaded and installed automatically by default
  - Full installation and upgrade packages must be installed manually
- Define mail notifications for completed package actions and for the new package updates.
- Run the software download and installation.

**Note** - You must have a CPUSE policy defined, before you download and run upgrades.

For details, see sk92449.

# API

This section describes how to use API to work with the Gaia Operating System.

# Working with Gaia RESTful API

**Note** - For additional API references, go to *Check Point API Reference*.

## API Overview

Gaia RESTful API provides a way to read information and to send commands to the Check Point Gaia Operating System.

Just like it is possible to use Gaia Portal or Gaia Clish commands to work with Gaia, it is possible to do the same using API commands.

**Note** - Gaia API does not yet support the configuration of all Gaia OS settings.

## Running the Gaia API Commands

- Use a 3rd-party API client to send API commands over an HTTPS connection.
- Use the Check Point "`mgmt_cli`" command in the Expert mode on the Gaiaoperating system.
- Use the Check Point "`mgmt_cli.exe`" command in the SmartConsole installation folder.

## Online Gaia API Reference

See the *Check Point Gaia API Reference*.

**Note** - The online API reference is updated from time to time with textual corrections.

# Local Gaia API Reference

In a web browser, connect to:

```
https://<IP Address or Gaia Management Interface>/gaia_
docs/#introduction
```

Example:

```
https://192.168.3.57/gaia_docs/#introduction
```

**Note** - The local API reference is **not** updated with textual corrections through hotfixes, unless they are critical.

# Local Management API Reference

This local Management API reference exists on a Security Management Server / Multi-Domain Security Management Server.

**Important** - First, you must follow sk174606 to allow access this local Management API reference.

In a web browser, connect to:

```
https://<IP Address or Gaia Management Interface>/api_
docs/#introduction
```

Example:

```
https://192.168.3.57/api_docs/#introduction
```

**Note** - The local API reference is **not** updated with textual corrections through hotfixes, unless they are critical.

# Gaia API Proxy

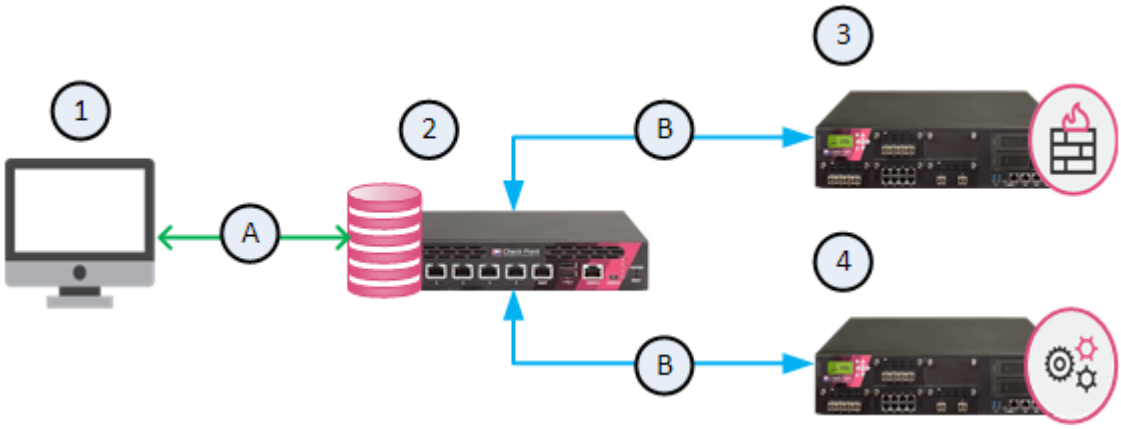
Check Point products support API commands. See the *Check Point API Reference*.

With the Gaia API Proxy feature on a Management Server, you run the Gaia API commands on managed Security Gateways and Cluster Members:

1. An administrator connects with an API Client to a Management Server.
2. From the Management Server, an administrator runs the Gaia API commands on managed Security Gateways and Cluster Members.

The Gaia API Proxy feature on the R82 Management Server works with all managed Security Gateways and Cluster Members that support the Gaia API.

### Example diagram




| Item | Description |
|---|---|
| 1 | An API Client |
| 2 | A Management Server with the Gaia API Proxy feature |
| 3 | A managed Security Gateway |
| 4 | A managed ClusterXL |
| A | Management API communication |
| B | Gaia API communication |

**Important** - Scalable Platforms (ElasticXL, Maestro, and Chassis) do **not** support this feature (Known Limitation MBS-10832).

**Workflow:**

1. **Run the Management API "`login`" command to log in to the Management Server**

   When you work with an API Client, run the Check Point API "`login`" command to log in to the Management Server (see the *Check Point Management API Reference*).

   **Important** - The administrator that logs in must have the **Run One Time Script** permission enabled in the assigned permission profile:
   a. Connect with SmartConsole to the Management Server.
   b. From the left navigation panel, click **Manage & Settings**.
   c. In the top section, click **Permissions & Administrators** > **Permission Profiles**.
   d. Open the applicable permission profile.
   e. From the left tree, click **Overview**.
      - If you selected **Read/Write All**, then click **Cancel**.
        The required permission is already enabled.
      - If you selected **Customized**, then:
        i. From the left tree, click **Gateways**.
        ii. In the **Scripts** section, select **Run One Time Script**.
        iii. Click **OK**.
        iv. Publish the SmartConsole session

2. **Run the Gaia API commands on managed Security Gateways and Cluster Members**

   The Management API "`login`" command returns the Session Unique Identifier (SID) token.

   In the same API Client, use this SID token in the "`X-chkp-sid`" field of the Gaia API commands you run on managed Security Gateways and Cluster Members.

   Gaia API Syntax:

   ```
   POST https://<IP Address of Management Server>/web_api/gaia-api/<Gaia API Version>/<Gaia API Command>
   ```

   See the *Check Point Gaia API Reference*.

   The body of the Gaia API command must identify the managed Security Gateway or Cluster Member by one of these parameters:

- Object name
- Object primary IP address
- Object UID

3. **The Gaia API Proxy logs in to the specified Security Gateway or Cluster Member**

   The Gaia API Proxy on the Management Server interprets the Gaia API command and logs in to the specified Security Gateway or Cluster Member.

   a. This login returns the SID for the Security Gateway or Cluster Member.

   b. The Gaia API Proxy uses this SID to run the Gaia API commands.

   c. The Gaia API Proxy saves this SID in its database:

      - The SID timeout is 580 seconds on the Management Server.
      - The SID timeout is 10 minutes on a Security Gateway or Cluster Member.

4. **The Gaia API Proxy forwards the response from the Security Gateway or Cluster Member to the API client**

   - To increase performance, the Gaia API Proxy saves the response in the Gaia API Proxy cache on the Management Server.
   - If the Gaia API Proxy gets the same Gaia API request during the cache timeout, it returns the Gaia API response from its cache and updates the cache.

- An administrator can configure these cache parameters in the `$FWDIR/api/conf/cache.conf` file on the Management Server:

  **Note** - After you change the `$FWDIR/api/conf/cache.conf` file, you must reload the API server configuration with the "`api reconf`" command in the Expert mode.

| Parameter | Accepted Values | Description |
|---|---|---|
| `timeout` | 0, or greater | Specifies the time, after which the next Gaia API command triggers a cache update for that Gaia API command:<br>• `0` - The Gaia API proxy does not use cache<br>• *<integer>* - The Gaia API proxy saves the Gaia API responses in its cache for the specified number of seconds (default: 60 seconds) |
| `total_gateways` | integer | Specifies the number of unique Security Gateways and Cluster Members, from which to save the Gaia API responses. |
| `maximum_entries` | integer | Specifies the number of unique Gaia API commands to save for each Security Gateway and Cluster Member. |

**Important** - The Gaia API Proxy sends Gaia API command over HTTPS. The Access Control policy for the Security Gateway or ClusterXL must explicitly allow HTTPS traffic from the Management Server to the Security Gateway or Cluster Members.

## Examples

### Gaia API command "show-hostname"

In this example, we identify the managed Security Gateway by the object primary IP address.

#### Request

```
POST https://<IP Address of Management Server>/gaia-api/show-
hostname
Content-Type: application/json
X-chkp-sid: <Session ID>
{
  "target" : "192.168.1.1"
}
```

#### Response

```
{
  "command-name" : "show-hostname",
  "response-message" : {
    "name" : "gw-832546"
  }
}
```

### Gaia API command "show-interface"

In this example, we identify the managed Security Gateway by the object name.

#### Request

```
POST https://<IP Address of Management Server>/gaia-
api/v1.4/show-interfaces
Content-Type: application/json
X-chkp-sid: <Session ID>
{
  "target" : "gw-832546",
  "name" : "eth0"
}
```

#### Response

```
{
  "command-name" : "v1.4/show-interfaces",
  "response-message" : {
    "ipv6-local-link-address": "Not Configured",
    "type": "physical",
    "name": "eth0",
    "ipv6-mask-length": "Not-Configured",
    "ipv6-address": "Not-Configured",
    "ipv6-autoconfig": "Not configured",
    "ipv4-address": "192.168.1.1",
    "enabled": true,
    "comments": "",
    "ipv4-mask-length": "24"
  }
}
```

### Gaia API command "show-diagnostics"

In this example, we identify the managed Security Gateway by the object UID.

#### Request

```
POST https://<IP Address of Management Server>/gaia-
api/v1.4/show-diagnostics
Content-Type: application/json
X-chkp-sid: <Session ID>
{
  "target" : "52048978-c507-8243-9d84-074d11154616",
  "category" : "os",
  "topic" : "disk"
}
```

#### Response

```
{
  "command-name" : "v1.4/show-diagnostics",
  "response-message" : {
    "to": 3,
    "total": 3,
    "from": 1,
    "objects": [
      {
      "total": "34342961152",
      "partition": "/",
      "used": "5718065152",
      "free": "28624896000"
      },
      {
      "total": "304624640",
      "partition": "/boot",
      "used": "26991616",
      "free": "277633024"
      },
      {
      "total": "34342961152",
      "partition": "/var/log",
      "used": "455684096",
      "free": "33887277056"
      }
    ]
  }
}
```

# Running Check Point Commands in Shell Scripts

To run Check Point commands in your shell scripts, it is necessary to add the calls to the required Check Point shell scripts.

You must add these calls below the top line "`#!/bin/bash`".

## On a Security Management Server / Log Server / SmartEvent Server

You must add the call to the `/etc/profile.d/CP.sh` script.

```
#!/bin/bash

source /etc/profile.d/CP.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

# On a Multi-Domain Server / Multi-Domain Log Server

You must add the calls to these scripts (in the order listed below):

1. `/etc/profile.d/CP.sh`
2. `$MDSDIR/scripts/MDSprofile.sh`
3. `$MDS_SYSTEM/shared/mds_environment_utils.sh`
4. `$MDS_SYSTEM/shared/sh_utilities.sh`

```
#!/bin/bash

source /etc/profile.d/CP.sh
source $MDSDIR/scripts/MDSprofile.sh
source $MDS_SYSTEM/shared/mds_environment_utils.sh
source $MDS_SYSTEM/shared/sh_utilities.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

# On a Security Gateway / Cluster Members (non-VSX)

You must add the call to the `/etc/profile.d/CP.sh` script.

```
#!/bin/bash

source /etc/profile.d/CP.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

# On a VSX Gateway / VSX Cluster Members

You must add the calls to these scripts (in the order listed below):

1. `/etc/profile.d/CP.sh`
2. `/etc/profile.d/vsenv.sh`

```
#!/bin/bash

source /etc/profile.d/CP.sh
source /etc/profile.d/vsenv.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

# Appendix

This section contains various notes about the Gaia Operating System.

- The default value of the Linux kernel parameter */proc/sys/net/ipv6/conf/all/accept_dad* is set to '0'.

  The IPv6 Duplicate Address Detection (DAD) feature continues to be enabled by default ('*set neighbor duplicate-detection state on*').

# Glossary

## A

**Anti-Bot**
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

**Anti-Spam**
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

**Anti-Virus**
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

**Application Control**
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

**Audit Log**
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

## B

**Bridge Mode**
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

## C

**Cluster**
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

**Cluster Member**
Security Gateway that is part of a cluster.

**Compliance**
Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

**Content Awareness**
Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

**CoreXL**
Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

**CoreXL Firewall Instance**
On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

**CoreXL SND**
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

**CPUSE**
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

## D

**DAIP Gateway**
Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

**Data Loss Prevention**
Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

**Data Type**
Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

**Distributed Deployment**
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

**Dynamic Object**
Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

## E

**Endpoint Policy Management**
Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

**Expert Mode**
The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

## G

**Gaia**
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

**Gaia Clish**
The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

**Gaia Portal**
Web interface for the Check Point Gaia operating system.

## H

**Hotfix**
Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

**HTTPS Inspection**
Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

## I

**ICA**
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

**Identity Awareness**
Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

**Identity Logging**
Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

**Internal Network**
Computers and resources protected by the Firewall and accessed by authenticated users.

**IPS**
Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

**IPsec VPN**
Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

## J

**Jumbo Hotfix Accumulator**
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

## K

**Kerberos**
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

## L

**Log Server**
Dedicated Check Point server that runs Check Point software to store and process logs.

**Logging & Status**
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

## M

**Management Interface**
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

**Management Server**
Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

**Manual NAT Rules**
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

**Mobile Access**
Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

**Multi-Domain Log Server**
Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

**Multi-Domain Server**
Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

## N

**Network Object**
Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

**Network Policy Management**
Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

## O

**Open Server**
Physical computer manufactured and distributed by a company, other than Check Point.

## P

**Provisioning**
Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

## Q

**QoS**
Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

## R

**Rule**
Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

**Rule Base**
All rules configured in a given Security Policy. Synonym: Rulebase.

## S

**SecureXL**
Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

**Security Gateway**
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

**Security Management Server**
Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

**Security Policy**
Collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

**SIC**
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

**SmartConsole**
Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

**SmartDashboard**
Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

**SmartProvisioning**
Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

**SmartUpdate**
Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

**Software Blade**
Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

**Standalone**
Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

## T

**Threat Emulation**
Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

**Threat Extraction**
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

## U

**Updatable Object**
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

**URL Filtering**
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

**User Directory**
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

## V

**VSX**
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

**VSX Gateway**
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

## Z

**Zero Phishing**
Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.