Check Point
SOFTWARE TECHNOLOGIES LTD.

24 March 2019

GAIA

R80.10

Administration Guide

Classification: [Protected]

Check Point
SOFTWARE TECHNOLOGIES LTD
INFINITY

2019 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page https://www.checkpoint.com/copyright/ for a list of our trademarks.

Refer to the Third Party copyright notices https://www.checkpoint.com/about-us/third-party-trademarks-and-copyrights/ for a list of relevant copyrights and third-party licenses.

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.

For third party independent certification of Check Point Products, see the Check Point Certification page https://www.checkpoint.com/products-solutions/certified-check-point-solutions/.

Check Point R80.10

For more about this release, see the R80.10 home page http://supportcontent.checkpoint.com/solutions?id=sk111841.

Latest Version of this Document

Open the latest version of this document in a Web browser https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_Gaia_AdminGuide/html_frameset.htm.

Download the latest version of this document in PDF format http://supportcontent.checkpoint.com/documentation_download?ID=54824.

To learn more, visit the Check Point Support Center https://supportcenter.checkpoint.com.

Feedback

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

Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Gaia R80.10 Administration Guide.

Revision History

Date	Description
24 March 2019	Added: Configuring Gaia for the First Time (on page 46) Added: Resetting the Expert Mode Password on a Security Gateway (on page 351) Updated: Showing System Overview Information - Gaia Portal (on page 18) - added the description of the widgets "Packet Rate" and "Throughput". Removed: *Emergendisk* section (because this tool is not supported)

Date	Description
10 June 2018	Improved formatting and document layout. Added a note in the applicable sections that before configuring IPv6 addresses and IPv6 routes, administrator must enable the IPv6 Support and reboot. Updated: Configuring System Logging - Gaia Portal (on page 190). Updated: Configuring System Logging - Gaia Clish (on page 192). Removed: Configuring Link State Propagation (LSP) - this information is documented in the *Installation and Upgrade Guide*.
09 May 2018	Added: Terms section. Added: Summary of Gaia Clish Commands (on page 38). Updated: Download SmartConsole (on page 332). Updated: Configuring Log Volume (on page 196). Updated: Users (on page 205). Updated: DHCP Server (on page 111). Updated: Domain Name Service (on page 121). Updated: Hardware Health Monitoring (on page 333). Updated: Showing Hardware Information (on page 334). Updated: Roles (on page 213). Added: List of Available Features in Roles (on page 221). Added: List of Available Extended Commands in Roles (on page 233). Added: Configuring Link State Propagation (LSP).
05 February 2018	Updated: CPUSE - Software Updates (on page 352). Removed: • Security Management Server and Firewall Commands • Expand VPN Commands • Expand SmartView Monitor Commands • Expand ClusterXL Commands • CoreXL and Multi-queue Commands
30 August 2017	Updated: License Activation (on page 323). Updated: Snapshot Image Management (on page 325). Updated: To import a package from your local drive to the list of available package. Added: Link to Check Point third party certifications was added to this Important Information page.
14 June 2017	Updated: Centrally Managing Gaia Device Settings (on page 62) (general updates).

Date	Description
15 May 2017	First release of this document.

Contents

Important Information ... 3
Terms ... 11
Gaia Overview ... 12
Introduction to the Gaia Portal ... 13
Gaia Portal Overview ... 13
Logging in to the Gaia Portal ... 15
Working with the Configuration Lock ... 15
Using the Interface Elements ... 16
Toolbar Accessories ... 16
Search Tool ... 16
Navigation Tree ... 16
Status Bar ... 17
Configuration Tab ... 17
Monitoring Tab ... 17
System Information Overview ... 18
Showing System Overview Information - Gaia Portal ... 18
Showing System Overview Information - Gaia Clish ... 20
Changing Gaia Kernel Edition ... 21
Introduction to the Command Line Interface ... 22
Saving Configuration Changes ... 22
Command Completion ... 23
Commands and Features ... 24
Command History ... 26
Command Reuse ... 27
Command Line Movement and Editing ... 28
Configuration Locks ... 29
32 and 64-bit Gaia Kernel Editions ... 31
Environment Commands ... 32
Client Environment Output Format ... 34
Expert Mode ... 35
User Defined (Extended) Commands ... 36
Summary of Gaia Clish Commands ... 38
List of All Available Gaia Clish Commands ... 38
List of Gaia Clish 'add' Commands ... 40
List of Gaia Clish 'set' Commands ... 41
List of Gaia Clish 'show' Commands ... 43
List of Gaia Clish 'delete' Commands ... 45
Configuring Gaia for the First Time ... 46
Running the First Time Configuration Wizard in Gaia Portal ... 46
Running the First Time Configuration Wizard in CLI Expert mode ... 54
Centrally Managing Gaia Device Settings ... 62
Overview of Gaia Central Management ... 62
Managing Gaia in SmartConsole ... 63
Running Command Scripts ... 63
Understanding One-Time Scripts ... 64
Running Repository Scripts ... 65

Backup and Restore 66
Opening Gaia Portal and Gaia Clish 68
Network Management 69
Network Interfaces 69
Interface Link Status 70
Physical Interfaces 71
Aliases 75
VLAN Interfaces 77
Bond Interfaces (Link Aggregation) 81
Bridge Interfaces 92
Loopback Interfaces 96
VPN Tunnel Interfaces 99
CLI Reference (interface) 105
ARP 107
Configuring ARP - Gaia Portal 107
Configuring ARP - Gaia Clish 109
DHCP Server 111
Configuring a DHCP Server - Gaia Portal 112
Configuring a DHCP Server - Gaia Clish 114
Hosts and DNS 118
Host Name 118
Host Addresses 119
Domain Name Service (DNS) 121
IPv4 Static Routes 124
Configuring IPv4 Static Routes - Gaia Portal 124
IPv6 Static Routes 131
Configuring IPv6 Static Routes - Gaia Portal 131
Configuring IPv6 Static Routes - Gaia Clish 132
Configuring IPv6 Neighbor-Entry - Gaia Clish 136
Netflow Export 137
Flow Records 138
Configuring Netflow Export - Gaia Portal 138
Configuring Netflow Export - Gaia Clish 139
Monitoring NetFlow Configuration 140
Advanced Routing 141
System Management 142
Time 142
Setting the Time and Date - Gaia Portal 143
Configuring NTP - Gaia Clish 144
Showing the Time & Date - Gaia Clish 145
Setting the Date - Gaia Clish 146
Setting the Time - Gaia Clish 146
Setting the Time Zone - Gaia Clish 147
Cloning Groups 148
Configuring Cloning Groups - Gaia Portal 148
Configuring Cloning Groups - Gaia Clish 152
SNMP 158
Configuring SNMP - Gaia Portal 162
Configuring SNMP - Gaia Clish 166
Interpreting Error Messages 170
Job Scheduler 173
Configuring Job Scheduler - Gaia Portal 173

Configuring Job Scheduler - Gaia Clish 175
Mail Notification 177
Configuring Mail Notification - Gaia Portal 177
Configuring Mail Notification - Gaia Clish 178
Messages 179
Configuring Messages - Gaia Portal 179
Configuring Messages - Gaia Clish 180
Display Format 182
Configuring Display Format - Gaia Portal 182
Configuring Display Format - Gaia Clish 183
Session 184
Configuring the Session - Gaia Portal 184
Configuring the Session - Gaia Clish 184
Core Dumps 185
Configuring Core Dumps - Gaia Portal 185
Configuring Core Dumps - Gaia Clish 186
System Configuration 188
Configuring IPv6 Support - Gaia Portal 188
Configuring IPv6 Support - Gaia Clish 189
System Logging 190
Configuring System Logging - Gaia Portal 190
Configuring System Logging - Gaia Clish 193
Configuring Log Volume - Expert Mode 197
Redirecting RouteD System Logging Messages 198
Network Access 199
Configuring Telnet Access - Gaia Portal 199
Configuring Telnet Access - Gaia Clish 199
Certificate Authority 200
Resetting the Certificate Authority - Gaia Portal 200
Changing the Name of the Internal Certificate Authority - Expert Mode 200
Host Access 201
Configuring Allowed Gaia Clients - Gaia Portal 201
Configuring Allowed Gaia Clients - Gaia Clish 201
User Management 203
Change My Password 204
Changing My Password - Gaia Portal 204
Changing My Password - Gaia Clish 204
Users 205
Managing User Accounts - Gaia Portal 206
Managing User Accounts - Gaia Clish 209
Roles 213
Configuring Roles - Gaia Portal 213
Configuring Roles - Gaia Clish 217
List of Available Features in Roles 221
List of Available Extended Commands in Roles 233
Password Policy 237
Configuring Password Policy - Gaia Portal 239
Configuring Password Policy - Gaia Clish 243
Monitoring Password Policy 249
Authentication Servers 250
Configuring RADIUS Servers - Gaia Portal 251
Configuring RADIUS Servers - Gaia Clish 253

Configuring Gaia as a RADIUS Client 256
Configuring RADIUS Servers for Non-Local Gaia Users 257
Configuring TACACS+ Servers - Gaia Portal 259
Configuring TACACS+ Servers - Gaia Clish 261
Configuring Gaia as a TACACS+ Client 264
Configuring TACACS+ Servers for Non-Local Gaia Users 266
System Groups 267
Configuring System Groups - Gaia Portal 267
Configuring System Groups - Gaia Clish 269
GUI Clients 271
Security Management GUI Clients - Gaia Portal 271
Security Management GUI Clients - Command Line 272
High Availability 273
VRRP 273
Understanding VRRP 273
Preparing a VRRP Cluster 280
Configuring Monitored Circuit/Simplified VRRP 283
Configuring Monitored Circuit/Simplified VRRP - Gaia Clish 283
Configuring Monitored Circuit/S 286
implified VRRP - Gaia Portal 287
Configuring the VRRP Security Gateway Cluster in SmartConsole 290
Configuring VRRP Rules for the Security Gateway 291
Configuring Advanced VRRP 292
Configuring Advanced VRRP - Gaia P 292
ortal 293
Configuring Advanced VRRP - Gaia Clish 296
Configuring VRRP Clusters in SmartConsole 302
Troubleshooting VRRP 303
Traces for VRRP 303
General Configuration Considerations 304
Firewall Policies 305
Monitored-Circuit VRRP in Switched Environments 305
Maintenance 306
Licenses 306
Configuring Licenses - Gaia Portal 307
cplic 308
License Activation - Gaia Portal 323
Snapshot Management 325
Snapshot Prerequisites 326
Working with Snapshot Management - Gaia Portal 326
Working with Snapshot Management - Gaia Clish 329
Restoring a Factory Default Image on Check Point Appliance 331
Download SmartConsole 332
Hardware Health Monitoring 333
Showing Hardware Health Information - Gaia Portal 333
Showing Hardware Health Information - Gaia Clish (show sysenv) 334
Showing Hardware Information 335
Monitoring RAID Synchronization 338
Showing RAID Information - Gaia Portal 338
Showing RAID Information - Command Line 338
Shutdown 339
Shutting Down and Rebooting - Gaia Portal 339

Shutting Down and Rebooting - Gaia Clish....339
System Backup....340
Backing Up and Restoring the System - Gaia Portal....340
Backing Up an....342
d Restoring the System - Gaia Clish....343
Configuring Scheduled Backups - Gaia Portal....345
Configuring Scheduled Backups - Gaia Clish....346
Working with System Configuration - Gaia Clish....349
Advanced Configuration....350
Configuring the Gaia Portal Web Server....350
Resetting the Expert Mode Password on a Security Gateway....351
CPUSE - Software Updates....352

Terms

BPDU

Bridge Protocol Data Units (BPDUs) are frames that contain information about the Spanning tree protocol (STP). Switches send BPDUs using a unique MAC address from its origin port and a multicast address as destination MAC. For STP algorithms to function, the switches need to share information about themselves and their connections. The switches send Bridge Protocol Data Units (BPDUs) as multicast frames, to which only other Layer 2 switches or bridges are listening. If any loops (multiple possible paths between switches) exist in the network topology, the switches will co-operate to disable a port or ports to make sure that there are no loops. Meaning, from one device to any other device in the Layer 2 network, only one path can be taken.

Expert Mode

The name of the full command line shell that gives full system root permissions in the Check Point Gaia operating system.

Warning - Expert Mode should be used with caution. The flexibility of an open shell, with root permission, exposes the system to the possibility of administrative errors.

First Time Configuration Wizard

GUI wizard that opens when you connect to the Gaia Portal for the first time, since the Gaia OS was installed. This wizard guides you through the initial configuration.

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

Gaia Portal

Web interface for Check Point Gaia operating system.

Management Interface

Interface on Gaia computer, through which users connect to Portal or CLI.

Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member.

Navigation Tree

A hierarchical tree of available pages in Gaia Portal.

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, and 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.

Introduction to the Gaia Portal

In This Section:

Gaia Portal Overview 13
Logging in to the Gaia Portal 14
Using the Interface Elements 15

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

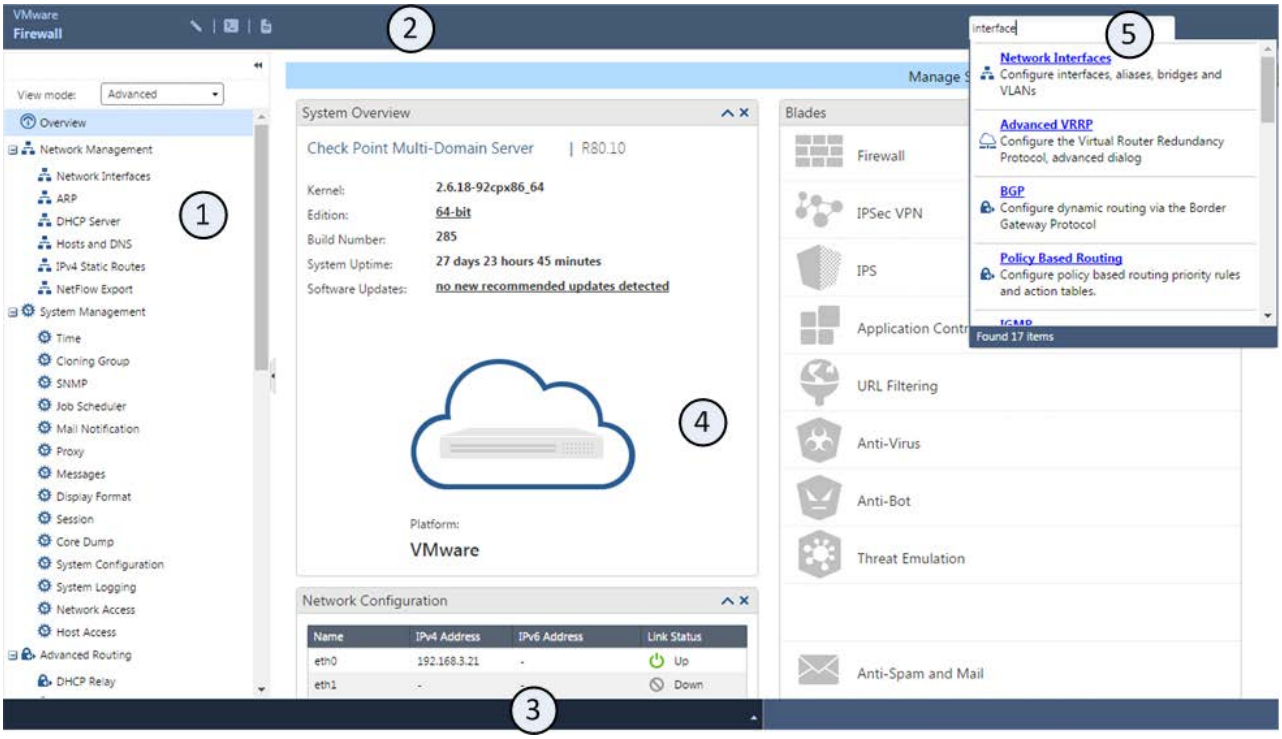
Gaia Portal Overview

- 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 to `https://<Gaia IP Address>`.
- 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 browser.

The Gaia Portal interface:

Example:



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	Description
1	Enter this URL in your browser: `https://<Gaia IP address>`
2	Enter your user name and password.

To log 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 (on page 213).

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.

To override 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 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. Available in the Read/Write mode only.
	Opens the **Scratch Pad** accessory for writing notes or for quick copy/paste operations. 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.

System Information Overview

In This Section:

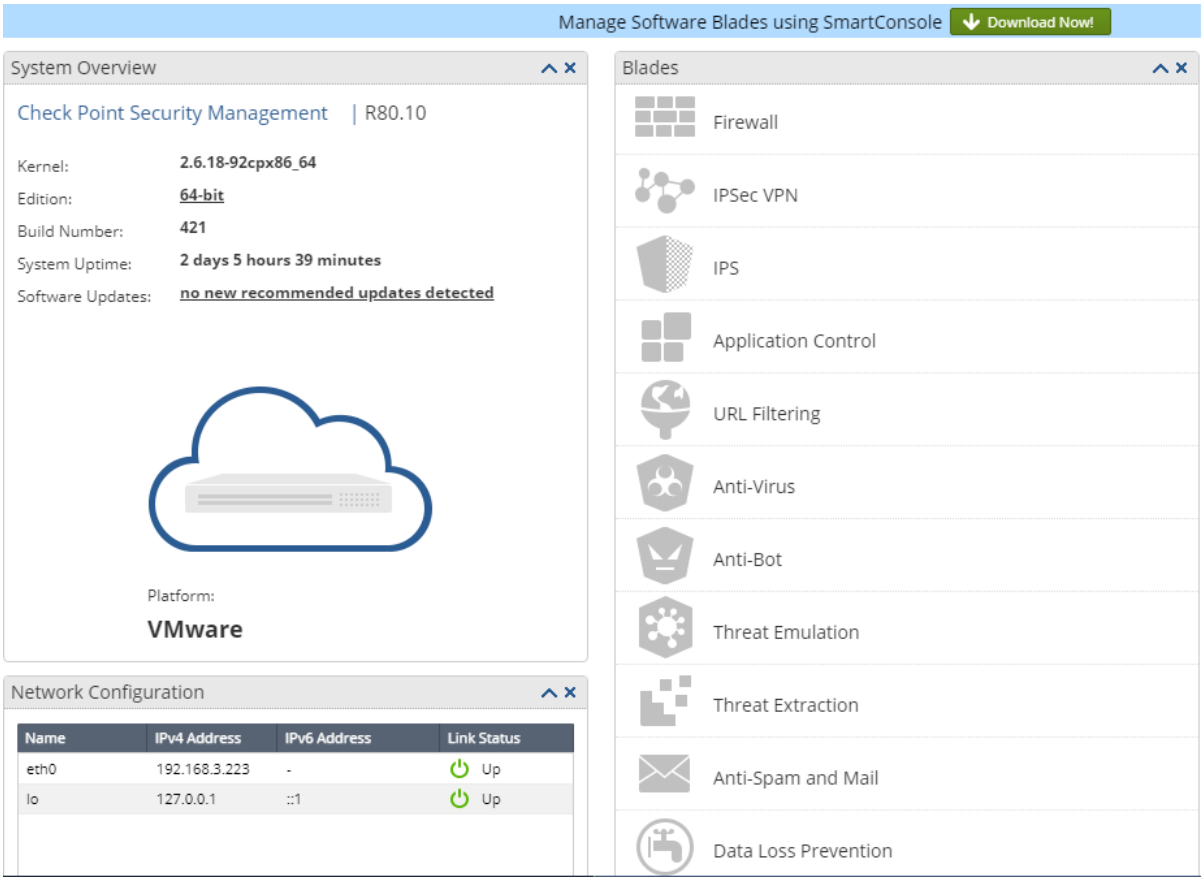
Showing System Overview Information - Gaia Portal.....18
Showing System Overview Information - Gaia Clish.....19
Changing Gaia Kernel Edition 21

This chapter shows you how to see system information using the Gaia Portal and some Gaia Clish commands.

Showing System Overview Information - Gaia Portal

The **Overview** page shows status widgets.

Example:



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

Widget	Description
System Overview	System information, including: • Installed product (for example: Check Point Security Management, Check Point Security Gateway) • Product version number (for example: R80.10) • Kernel edition (32-bit, or 64-bit) • Product build number • System uptime • hardware platform, on which Gaia is installed • Computer serial number (on Check Point appliances)
Blades	Installed Software Blades. Those that are enabled in SmartConsole, are colored. Those that are disabled in SmartConsole, are grayed out.
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.

To add a widget to the page:

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

To move a widget on the page:

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

Showing System Overview Information - Gaia Clish

You can use these commands to show system status.

uptime

Description Show how long the system has been running

Syntax
```
show uptime
```

Parameters None

version

Description Show 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

`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.

Comments:

If the Gaia appliance has more than 4 GB of memory, it automatically boots to the 64-bit edition. Otherwise, it boots to the 32-bit edition.

If you upgrade and the appliance has more than 4 GB, the appliance boots to the 32-bit edition. You can configure Gaia to automatically boot to the 64-bit edition.

To configure Gaia to automatically boot to the 64-bit edition:

Note - The appliance must have at least 6 GB of memory for this to work.

1. Configure the kernel edition:
   ```
   set edition default 64-bit
   ```
2. Save the changes:
   ```
   save config
   ```
3. Reboot:
   ```
   reboot
   ```

To see which edition Gaia is running:

- In the Gaia Portal:
  Click **System Overview** pane. The edition shows in the **System Overview** widget.
- In the Gaia Clish, run:
  `show version os edition`

Changing Gaia Kernel Edition

Description

Gaia automatically starts in the 32-bit kernel edition after an upgrade and on Open Servers that have less than the minimum RAM as described in the Release Notes. You can change the Gaia kernel edition to 32-bit or 64-bit.

Syntax

```
set edition {32-bit | 64-bit}
```

To make sure the edition change persists after reboot, run `save config`. For example:

```
gaia> set edition 64-bit

gaia> save config

gaia> reboot
```

Note - If the computer or appliance cannot support 64-bit, the command will not let you choose 64-bit.

Introduction to the Command Line Interface

In This Section:

Saving Configuration Changes 22
Command Completion 23
Commands and Features 24
Command History 26
Command Line Movement and Editing 28
Configuration Locks 29
32 and 64-bit Gaia Kernel Editions 31
Environment Commands 32
Expert Mode 35
User Defined (Extended) Commands 36
Summary of Gaia Clish Commands 38

This chapter introduces the Gaia command line interface. The default Gaia shell is called `clish`.

To use the Gaia Clish:

Step	Description
1	Connect to the Gaia platform using one of these options: • From SmartConsole (on page 67). • Using a command-line connection (SSH, or a console).
2	Log in using a user name and password. Immediately after installation, the default user name and password are `admin` and `admin`.

Saving 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 the `save config` command.

Command Completion

You can automatically complete a command. This saves time, and can help if you are not sure what to type next.

Press ...	To do this...

<TAB>	Complete or fetch the keyword.
	Example:
	`HostName> set in<TAB>`
	`inactivity-timeout - Set inactivity timeout`
	`interface - Displays the interface related parameters`
	`HostName> set in`

<SPACE><TAB>	Show the arguments that the command for that feature accepts.
	Example:
	`HostName> set interface<SPACE><TAB>`
	`eth0 eth1 lo`
	`HostName> set interface`

<ESC><ESC>	See possible command completions.
	Example:
	`HostName> set inter<ESC><ESC>`
	`set interface VALUE ipv4-address VALUE mask-length VALUE`
	`set interface VALUE ipv4-address VALUE subnet-mask VALUE`
	`set interface VALUE ipv6-address VALUE mask-length VALUE`
	`set interface VALUE { comments VALUE mac-addr VALUE mtu VALUE state VALUE speed VALUE duplex VALUE auto-negotiation VALUE}`
	`set interface VALUE { ipv6-autoconfig VALUE }`
	`HostName> set inter`

?	Get help on a feature or keyword.
	Example:
	`HostName> set interface <?>`
	`interface: specifies the interface name`
	`This operation configures an existing interface.`
	`HostName>`

UP/DOWN arrow	Browse the command history.
LEFT/RIGHT arrow	Edit command.
Enter	Run a command string. The cursor does not have to be at the end of the line. You can usually abbreviate the command to the smallest number of unambiguous characters.

Commands and Features

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

operation feature parameter

The most common operations are `add` (on page 40), `set` (on page 41), `show` (on page 43), and `delete` (on page 45).

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. 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.
`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

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

Command	Description
↓	Recall previous command.
↑	Recall next command.
`history`	Show the last 100 commands.
`!!`	Run the last command.
`!nn`	Run a specific previous command: the `nn` command in the commands history list.
`!-nn`	Run the `nn`th previous command. For example, entering `!-3` runs the third from last command in the commands history list.
`!str`	Run the most recent command that starts with `str`.
`!\?str\?`	Run the most recent command containing `str`. You may omit the trailing `?`, if a new line follows `str` immediately.
`!!:s/str1/str2`	Repeat the last command, replacing `str1` with `str2`.

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. Use this modified in conjunction with `s`, as in `gs/str1/str2`.

Command Line Movement and Editing

You can back up in a command you are typing to correct a mistake. To edit a command, use the left and right arrow keys to move around and the Backspace key to delete characters. You can enter commands that span more than one line.

You can use these keystroke combinations:

Keystroke combination	Meaning
Alt D	Delete next word (to the right of the cursor).
Alt F	Go to the next word (to the right of the cursor).
Ctrl Alt H	Delete the previous word (to the left of the cursor).
Ctrl Shift -	Repeat the previous word (from the left of the cursor).
Ctrl A	Move to the beginning of the line.
Ctrl B	Move to the previous character (to the right of the cursor).
Ctrl E	Move to the end of the line.
Ctrl F	Move to the next character (to the right of the cursor).
Ctrl H	Delete the previous character (to the left of the cursor).
Ctrl L	Clear the screen and show the current line at the top of the screen.
Ctrl N	Next history item.
Ctrl P	Previous history item.
Ctrl R	Redisplay the current line.
Ctrl U	Delete the current line.

Configuration Locks

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 (on page 213).

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.

Use the *database* feature to obtain the configuration lock.

The commands do the same thing: obtain the configuration lock from another administrator.

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.

Configuring Lock Behavior

The behavior of the configuration lock command is configured using: `config-lock`.

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. The default timeout value is 300 seconds.
`timeout <5-900>`	Optional parameter. 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.

32 and 64-bit Gaia Kernel Editions

The 64-bit support for a Gaia device depends on the appliance type (for a Check Point appliance) and hardware capabilities (for Open Servers).

For more on supported platforms and kernels, see the *R80.10 Release Notes*.

Note - The Open Server hardware must support 64-bit for the Edition feature to work.

Description

Use the Edition feature to change the default between 32- and 64-bit versions of Gaia.

Syntax

```
set edition default {32-bit | 64-bit}
```

Comments

- Run the command from *Gaia Clish*.
- The hardware platform must have at least 6 GB of memory for this to work.
- Remember to reboot the device.

To see which edition is running:

- Go to the Gaia Portal **System Overview** pane. The edition shows in the **System Overview** widget.
- In the Gaia Clish, run: `show version os edition`

Environment Commands

Description

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

Syntax

To show the client environment:

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

To configure 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 <Row Number>
      syntax-check {on | off}
```

To save the client environment configuration permanently:

```
save clienv
```

Parameters

Parameter	Description
`config-lock {on | off}`	Default value of the Clish `config-lock` parameter. If set to `on`, Gaia Clish will lock the configuration when invoked, otherwise continue without a configuration lock. When the configuration is locked by Clish, no configuration changes are possible in Gaia Portal, until the lock is released.
`debug {0-6}`	Debug level. Predefined levels are: • `0` - (Default) Do not debug, display error messages only • `5` - Show `confd` daemon requests and responses • `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. The default is `off`.

Parameter	Description
`on-failure {continue | stop}`	Action performed on failure: • `continue` - Show error messages, but continue running commands from a file or a script • `stop` - (Default) Stop running commands from a file or a script
`output {pretty | structured | xml}`	Command line output format (on page 34). The default is `pretty`.
`prompt` <*Prompt String*>	Command prompt string. A valid prompt string can consist of any printable characters and a combination of these variables: • `%H` - Replaced with the Command number • `%I` - Replaced with the User ID • `%M` - Replaced with the Hostname • `%P` - Replaced with the Product ID • `%U` - Replaced with the Username To set the prompt back to the default, use the keyword `default`.
`rows` <*Row Number*>	Number of rows to show in your terminal window. If the window size is changed, the number of rows will also change, unless the value is set to 0 (zero).
`syntax-check {on | off}`	Put the shell into syntax-check mode. Commands you enter are checked syntactically and are not executed, but values are validated. 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

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.

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

Note - If a command is supported in Gaia Clish, it is not possible to run it in Expert mode.

For example, you cannot run `ifconfig` in Expert mode. Use the `set interface` command in Clish instead.

Description

The Expert mode password protects the Expert shell against authorized access.

Use these commands to set the Expert password by plain text or MD5 salted hash.

Use the MD5 salted hash option when upgrading or restoring using backup scripts.

Syntax

```
set expert-password
set expert-password hash <Hash String>
```

Important - You must run `save config` to set the new Expert password permanently.

Parameters

Parameter	Description
`hash` <*Hash String*>	The password as an MD5 salted `hash instead` of plain text. Use `this` option when upgrading or restoring using backup scripts.

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
```

User Defined (Extended) Commands

Description

Manage user defined (extended) commands in Gaia Clish. Extended commands include:

1. Built in extended commands. These are mostly for configuration and troubleshooting of Gaia and Check Point products.
2. User defined commands.

You can do role-based administration (RBA) with extended commands by assigning extended commands to roles and then assigning 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 the *List of available Extended Commands in roles* (on page 233).

Example

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

Step	Description
1	To add the *free* command: `gaia> add command free path /usr/bin/free description "Display amount of free and used memory in the system"`
2	Save the configuration: `gaia> save config`
3	Log out of Gaia.
4	Log in to Gaia again.

Step	Description
5	To add the *free* command to the *systemDiagnosis* role: `gaia> add rba role systemDiagnosis domain-type System readwrite-features ext_free`
6	To assign the *systemDiagnosis* role to the user *john*: `gaia> add rba user john roles systemDiagnosis`
7	Save the configuration: `gaia> save config`

Summary of Gaia Clish Commands

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

List of All Available Gaia Clish Commands

To show the list of all available Gaia Clish commands:

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

List of all available Gaia Clish commands:

```
LSMcli                - SmartLSM command line
LSMenabler            - Enable SmartLSM
SnortConvertor        - IPS Snort conversion tool
add                   - Add operation.
api                   - Start, stop, or check status of API server
backup                - Start a backup of the system
clear                 - clear the screen
commit                - End transaction by committing changes.
config_system         - First Time Configuration tool
cp_conf               - Check Point system configuration utility
cpca                  - Run Check Point Internal CA
cpca_client           - Manage/configure Check Point Internal CA
cpca_create           - Create new Check Point Internal CA database
cpca_dbutil           - Print/convert Check Point Internal CA database
cpconfig              - Check Point software configuration utility
cphaprob              - Clustering commands
cphastart             - Enables the High Availability feature on the machine
cphastop              - Disables the High Availability feature
                          on the machine
cpinfo                - Show Check Point diagnostics information
cplic                 - Add/Remove Check Point licenses
cpshared_ver          - Show SVN Foundation version
cpstart               - Start Check Point products installed
cpstat                - Show Check Point statistics info
cpstop                - Stop Check Point products installed
cpview                - Show Check Point and system online statistics info
cpwd_admin            - Check Point watchdog administration tool
delete                - Delete operation.
diag                  - Send system diagnostics information
dtps                  - Endpoint Policy Server commands
etmstart              - Starts QoS
etmstop               - Stops QoS
exit                  - Exit from shell.
expert                - Execute system shell.
fgate                 - QoS commands
fips                  - Turns on/off FIPS mode
fw                    - Security Gateway commands
fw6                   - Security gateway IPv6 commands
fwaccel               - SecureXL commands
fwaccel6              - SecureXL IPv6 commands
fwm                   - Security Management commands
generate              - Generate operation.
halt                  - Use to halt the system
help                  - Global help page.
history               - Show command history.
```

```
ifconfig              - Deprecated.
                        Use 'show interface' or 'set interface'.
installer             - Perform actions
ips                   - IPS management commands
join                  - Sorry, no help available here.
leave                 - Sorry, no help available here.
load                  - Load operation.
lock                  - Enable exclusive access.
lomipset              - Setting LOM IP address
mgmt                  - Management commands
netstat               - Print network connections, routing tables and
                        interface statistics
patch                 - Install/Upgrade utility
ping                  - Ping a host
ping6                 - Ping a host using IPv6
quit                  - Exit from shell.
raid_diagnostic       - RAID Monitoring tool
raidconfig            - RAID Configuration and Monitoring tool
re-synch              - Force cloning-group re-synchronization
reboot                - Use to reboot the system
restore               - Restore the configuration of the system
rollback              - End transaction by discarding changes.
rtm                   - Monitoring blade commands
rtmstart              - Start Monitoring blade
rtmstop               - Stop Monitoring blade
rtmtopsvc             - Monitor top services
save                  - Save operation.
set                   - Set operation.
show                  - Show operation.
sim                   - SecureXL Implementation Module commands
start                 - Start operation.
tacacs_enable         - Enable current user with higher privileges
tecli                 - Threat Emulation Blade shell
top                   - Show the most active system processes
traceroute            - Trace the route to a host
unlock                - Disable exclusive access.
upgrade               - Start upgrade of Check Point OS and Products
ver                   - Display system versions
vpn                   - Control VPN
vpn6                  - VPN IPv6 commands
vsec_central_license - virtual edition licenses distribution utility
vsec_config           - vSEC management utility
vsx_util              - Control VSX gateways
```

List of Gaia Clish 'add' Commands

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

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

List of available Gaia Clish 'add' commands:

```
add aaa                - Authentication authorization and accounting
add allowed-client     - Add allowed client
add arp                - Add ARP entries
add backup             - Start a backup of the system
add backup-scheduled   - Determine the type of scheduled-backup
                           of the system
add bonding            - Configure bonding interfaces
add bridging           - Configure bridging interfaces
add cloning-group      - Configure Gaia Cloning Group
add command            - Add extended command.
add cron               - Add new scheduling for a command
add dhcp               - Configure or view DHCP settings.
add group              - Specify group name
add host               - Static host configuration
add instance           - Routing Instance
add interface          - Displays the interface related parameters
add mcvr               - Create a VRRP Virtual Router
add neighbor-entry     - Add or Delete a neighbor table entry
add netflow            - NetFlow export of traffic information
add pppoe              - Add PPPoE
add rba                - Role-based administration configuration
add snapshot           - Take snapshot
add snmp               - Simple Network Management Protocol Information
add syslog             - System log configuration
add upgrade            - Upgrade of Check Point OS and Products
add user               - A user name
add virtual-system     - Adds an instance to the system.
add vpn                - vpn configuration
```

List of Gaia Clish 'set' Commands

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

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

List of available Gaia Clish 'set' commands:

```
set aaa                          - Authentication authorization and
                                     accounting
set aggregate                    - Configure aggregate routes
set arp                          - Configure the parameters related to ARP
set as                           - Configure Autonomous System Number
set backup                       - Restore the configuration of the system
set backup-scheduled             - Set an existing scheduling of a backup
set bgp                          - Configure Border Gateway Protocol (BGP)
set bonding                      - Configure bonding interfaces
set bootp                        - Configure BOOTP/DHCP Relay
set clienv                       - CLI environment variables.
set cloning-group                - Configure Gaia Cloning Group
set cloning-group-management     - Enable/disable Cloning Group CLI mode.
set config-lock                  - Enable / Disable exclusive config access.
set core-dump                    - Set core dumps manager settings
set cron                         - Edit the scheduling of the command
set date                         - Set current date
set dhcp                         - Configure or view DHCP settings.
set dns                          - Set or delete DNS related values
set domainname                   - Stores the system's domain name
set edition                      - Default operating system edition
                                     configuration
set expert-password              - Set expert password
set expert-password-hash         - Set expert password md5 salted hash
set fcd                          - Factory Defaults
set format                       - Configure format
set group                        - Specify group name
set host                         - Static host configuration
set hostname                     - Hostname configuration
set igmp                         - Configure IGMP
set inactivity-timeout           - Set inactivity timeout
set inbound-route-filter         - Configure route import policy
set installer                    - Set policies
set instance                     - Routing Instance
set interface                    - Displays the interface related parameters
set interface-name               - Interface Naming
set iphelper                     - Configure IP Broadcast Helper
set ipv6                         - Configure IPv6 routing protocols
set ipv6-state                   - IPv6 enable/disable
set kernel-routes                - Configure kernel routes
set mail-notification            - Configure facility that relays mail
                                     to a mail hub via SMTP
set management                   - management interface configuration
set max-path-splits              - Configure maximum number of equal-cost
                                     routing paths
set mcvr                         - Configure VRRP using simplified
                                     configuration mode
set message                      - Use to set various messages
set neighbor                     - Modifies and Displays neighbor table
                                     related parameters
```

```
set net-access                - Various network services access
set netflow                   - NetFlow export of traffic information
set ntp                       - NTP
set ospf                      - Open Shortest Path First (OSPF) version 2
set password-controls         - Password and account management controls
set pbr                       - Configure Policy Based Routing (PBR)
set pbrroute                  - PBR route lookup when packets enter/exit
                                  gateway more than once
set pim                       - Configure PIM
set ping                      - Configure ping parameters
set pppoe                     - Set PPPoE
set protocol-rank             - Configure relative rank of dynamic
                                  routing protocols
set proxy                     - Configure proxy
set rdisc                     - Configure ICMP Router Discovery
set rip                       - Configure Routing Information Protocol
set route-redistribution      - Configure route export policy
set routedsyslog              - Configure Routing Daemon log file output
set routemap                  - Configure Route Maps
set router-id                 - Configure the Router ID
set router-options            - Configure Router Options
set selfpasswd                - Change user's password
set snapshot                  - User snapshots
set snmp                      - Simple Network Management Protocol
set static-mroute             - Configure static multicast routes
set static-route              - Configure an IPv4 static route
set syslog                    - System log configuration
set time                      - Set current time
set timezone                  - Set system time zone
set trace                     - Configure trace file output
set tracefile                 - Configure trace file options
set user                      - A user name
set virtual-system            - Set virtual-system context
set volume                    - Set new logical volume size (GB)
set vrrp                      - Configure VRRP using advanced
                                  configuration mode
set vsx                       - set VSX mode
set web                       - Configure "web" service
```

List of Gaia Clish 'show' Commands

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

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

List of available Gaia Clish 'show' commands:

```
show aaa                  - Authentication authorization and accounting
show allowed-client       - Show allowed client
show arp                  - Display the parameters related to ARP
show as                   - Show Autonomous System Number
show asset                - Display hardware information
show backup               - Show the status of the latest backup/restore
show backup-scheduled     - Show the scheduling of backup defined
                              in the system
show backups              - List of local backups
show bgp                  - Show Border Gateway Protocol (BGP)
                              configuration
show bonding              - Display summary of bonding interfaces
show bootp                - Show BOOTP/DHCP Relay status and configuration
show bridging             - Display summary of bridging interfaces
show clienv               - CLI environment variables.
show clock                - Show current date and time
show cloning-group        - Configure Gaia Cloning Group
show command              - Display extended command path and description.
show commands             - Show All Commands.
show config-lock          - Show exclusive access settings.
show config-state         - Show state of configuration
show configuration        - Show Configuration
show core-dump            - Show core dumps manager settings
show cron                 - Show the scheduling of the commands
                              defined in the system
show date                 - Show current date
show dhcp                 - Configure or view DHCP settings.
show dns                  - Display DNS related values
show domainname           - Retrieves the system's domain name
show extended             - Display extended commands.
show fcd                  - Factory Defaults
show format               - Configure format
show group                - Specify group name
show groups               - All groups
show host                 - Static host configuration
show hostname             - Show host name
show igmp                 - Show IGMP state and configuration
show inactivity-timeout   - show inactivity timeout
show installer            - Show deployment agent information
show interface            - interface All
show interfaces           - Lists all interfaces
show iphelper             - Show IP Broadcast Helper status and configuration
show ipv6                 - Show IPv6 configuration and state
show ipv6-state           - IPv6 status
show lom                  - Show LOM information
show mail-notification    - Configure facility that relays mail
                              to a mail hub via SMTP
show management           - management interface configuration
show mcvr                 - Show the VRRP Virtual Router configuration
show message              - Use to set various messages
```

```
show mfc                - Show Multicast Forwarding Cache (MFC) State
show neighbor           - Modifies and Displays neighbor table
                            related parameters
show net-access         - Various network services access
show netflow            - NetFlow export of traffic information
show ntp                - NTP
show ospf               - Open Shortest Path First (OSPF) version 2
show password-controls  - Password and account management controls
show pbr                - Show PBR configuration and state
show pbrroute           - PBR route lookup when packets enter/exit
                            gateway more than once
show pim                - Protocol Independent Multicast (PIM)
show ping               - Show ping parameters
show pppoe              - Show PPPoE
show protocol-rank      - Show relative ranks of dynamic
                            routing protocols
show proxy              - Configure proxy
show rba                - Role-based administration configuration
show rdisc              - Show ICMP Router Discovery configuration
                            and state
show restore            - Restore the configuration of the system
show rip                - Show Routing Information Protocol (RIP)
show route              - Show routing table information
show routed             - Show version, state, etc. of the Routing Daemon
show routemap           - Show Route Map configuration
show routemaps          - Show configuration of all Route Maps
show router-id          - Show the Router ID
show router-options     - Show Router Options configuration state
show snapshot           - Show snapshot data
show snapshots          - List of local snapshots
show snmp               - Simple Network Management Protocol
show static-mroute      - Show active static multicast routes
show sysenv             - show system/hardware status
show syslog             - System log configuration
show tacacs_enable      - Show enable privilege level
show time               - Show current time
show timezone           - Show system time zone
show trace              - Print the contents of the Routing Daemon
                            trace file
show upgrade            - Show upgrade information
show uptime             - show system uptime
show user               - A user name
show users              - Show information about system users
show version            - Display system versions
show virtual-system     - Show virtual-systems configured
show volume             - Show logical volume status
show vpn                - vpn configuration
show vrrp               - Show VRRP Virtual Router configuration
show vsx                - Show VSX status
show web                - Configure "web" service
```

List of Gaia Clish 'delete' Commands

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

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

List of available Gaia Clish 'delete' commands:

```
delete aaa               - Authentication authorization and accounting
delete allowed-client    - Delete allowed client
delete arp               - Delete ARP entries
delete backup            - Delete the local backup
delete backup-scheduled  - Delete the scheduled backup
delete bonding           - Configure bonding interfaces
delete bridging          - Configure bridging interfaces
delete cloning-group     - Configure Gaia Cloning Group
delete command           - Delete extended command.
delete cron              - Delete the scheduling of the command
delete dhcp              - Configure or view DHCP settings.
delete dns               - Set or delete DNS related values
delete domainname        - Removes the system's domain name
delete group             - Specify group name
delete host              - Static host configuration
delete installer         - Delete mail notifications
delete instance          - Routing Instance
delete interface         - Displays the interface related parameters
delete mcvr              - Remove a VRRP Virtual Router or
                             Virtual IP Address
delete message           - Use to set various messages
delete neighbor-entry    - Add or Delete a neighbor table entry
delete netflow           - NetFlow export of traffic information
delete ntp               - NTP
delete pppoe             - Delete PPPoE
delete proxy             - Delete proxy settings
delete rba               - Role-based administration configuration
delete snapshot          - Delete a snapshot
delete snmp              - Simple Network Management Protocol
delete syslog            - System log configuration
delete upgrade           - Delete upgrade version bindings and
                             locally saved .tgz files if they are
                             stored in /var/log/upload
delete user              - A user name
delete virtual-system    - Deletes an instance from the system.
delete vpn               - vpn configuration
```

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.

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. 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: `https://<IPv4_Address_of_Gaia>`
4	Enter the default username and password: `admin` and `admin`.
5	Click **Login**. The **Check Point First Time Configuration Wizard** opens.
6	Follow the instructions on the First Time Configuration Wizard windows. 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.

Deployment Options window:

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

Section	Options	Description
Setup	**Continue with R80.10 configuration**	Use this option to configure the installed Gaia and Check Point products.
Install	**Install from Check Point Cloud** **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 let you choose and install major versions available on Check Point Cloud. The Gaia CPUSE performs the installation.
- **Pull appliance configuration** - This option lets you to apply initial deployment configuration including different OS version on the appliance. You must prepare the initial deployment configuration with the Zero Touch Cloud Service. For more information, see sk116375 http://supportcontent.checkpoint.com/solutions?id=sk116375.

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**). **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: • **Manually** - You configure the IPv4 settings in the next fields. • **Off** - None.
IPv4 address	Enter the desired 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: • **Manually** - You configure the IPv6 settings in the next fields. • **Off** - None.
IPv6 Address	Enter the desired IPv6 address.
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 configure the interface that connects the Gaia computer to the Internet.

Field	Description
Interface	Select the applicable interface on this computer.
Configure IPv4	Select how the applicable interface gets its IPv4 address: • **Manually** - You configure the IPv4 settings in the next fields. • **Off** - None.
IPv4 address	Enter the desired IPv4 address.
Subnet mask	Enter the applicable IPv4 subnet mask.
Configure IPv6	Optional. Select how the applicable interface gets its IPv6 address: • **Manually** - You configure the IPv6 settings in the next fields. • **Off** - None.
IPv6 Address	Enter the desired IPv6 address.
Subnet	Enter the applicable IPv6 subnet mask.

Device Information window:

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

Field	Description
Host Name	Enter the desired 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 on the Gaia computer.

Field	Description
Set the 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: • A Single Security Gateway. • A Cluster Member. • A Security Management Server, including Management High Availability. • An Endpoint Security Management Server. • An Endpoint Policy Server. • CloudGuard Controller. • A dedicated single Log Server. • A dedicated single SmartEvent Server. • A Standalone.

Field	Description
Multi-Domain Server	Select this option to install: • A Multi-Domain Security Management Server, including Management High Availability. • A dedicated single Multi-Domain Log Server.

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: • A single Security Gateway. • A Cluster Member. • A Standalone.
Security Management	Select this option to install: • A Security Management Server, including Management High Availability. • An Endpoint Security Management Server. • An Endpoint Policy Server. • CloudGuard Controller. • A dedicated single Log Server. • A dedicated single SmartEvent Server. • A Standalone.
Unit is a part of a cluster	This option is available only if you selected **Security Gateway**. Select this option to install a cluster of dedicated Security Gateways, or a Full High Availability Cluster. Select the cluster type: • **ClusterXL** - For a cluster of dedicated Security Gateways, or a Full High Availability Cluster. • **VRRP Cluster** - For a VRRP Cluster on Gaia.

Field	Description
Define Security Management as	Select **Primary** to install: • A Security Management Server. • An Endpoint Security Management Server. • An Endpoint Policy Server. • CloudGuard Controller. Select **Secondary** to install: • A Secondary Management Server in Management High Availability. Select **Log Server / SmartEvent only** to install: • A dedicated single Log Server. • A dedicated single SmartEvent Server.

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 and other important data** is enabled. See sk111080 http://supportcontent.checkpoint.com/solutions?id=sk111080.

Dynamically Assigned IP window:

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).
No	Select this option, if you wish to configure this Security Gateway with a static IP address.

Secure Internal Communication (SIC) window:

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 the desired one-time activation key (between 4 and 127 characters long).

Field	Description
Confirm Activation Key	Enter the same one-time activation key again.

Security Management Administrator window:

In this window, you configure the main administrator for this Security Management Server.

Field	Description
Use Gaia administrator: admin	Select this option, if you wish to use the default Gaia administrator (`admin`).
Define a new administrator	Select this option, if you wish to configure an administrator username and password manually.

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. By default, the First Time Configuration Wizard uses the IPv4 address of your computer. You can change it to another IP address.
Network	Select this option to allow an entire IPv4 subnet of computers to connect. 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. Enter the applicable start and end IPv4 addresses.

Leading VIP Interfaces Configuration window:

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

Field	Description
Select leading interface	Select the desired interface.

Multi-Domain Server GUI Clients window:

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. By default, the First Time Configuration Wizard uses the IPv4 address of your computer. 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.

By default, the option **Improve product experience by sending data to Check Point** is enabled. See sk111080 http://supportcontent.checkpoint.com/solutions?id=sk111080.

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 verify that the configuration is finished:
  a) Connect to the command line on the Gaia computer.
  b) Log in to the Expert mode.
  c) Check that the bottom section of the `/var/log/ftw_install.log` file contains one of these sentences: "*installation succeeded*" or "*FTW: Complete*".

  Run:

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

  Example output from a Security Gateway or Cluster Member:

```
[Expert@GW:0]# cat /var/log/ftw_install.log | egrep --color "installation succeeded|FTW: Complete"
Apr 06, 18 19:19:51 FTW: Complete
[Expert@GW:0]#
```

  Example output from a Security Management Server or a Standalone:

```
[Expert@SA:0]# cat /var/log/ftw_install.log | egrep --color "installation succeeded|FTW: Complete"
May 01, 2018 03:48:38 PM installation succeeded.
05/01/18 15:48:39 FTW: Complete
[Expert@SA:0]#
```

  Example output from a Multi-Domain Server:

```
[Expert@MDS:0]# cat /var/log/ftw_install.log | egrep --color "installation succeeded|FTW: Complete"
Apr 08, 2018 07:43:15 PM installation succeeded.
[Expert@MDS:0]#
```

Running the First Time Configuration Wizard in CLI Expert mode

Description

Use this command in 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.

Syntax

- To list the command options, run one of these:

Form	Command
Short form	`config_system -h`
Long form	`config_system --help`

- To run the First Time Configuration Wizard from a specified configuration file, run one of these:

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

- To run the First Time Configuration Wizard from a specified configuration string, run one of these:

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

- To create a First Time Configuration Wizard Configuration file template in a specified path, run one of these:

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

- To verify that the First Time Configuration file is valid, run:

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

- To list configurable parameters, run one of these:

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

To run the First Time Configuration Wizard from a configuration string:

Step	Description

1	Run this command in Expert mode:
	`config_system --config-string <`*String of Parameters and Values*`>`
	A configuration string must consist of *parameter=value* pairs, separated by the ampersand (&).
	You must enclose the whole string between quotation marks.
	For example:
	`"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"`
	For more information on valid parameters and values, see the *config_system*.

2	Reboot the system.

To run the First Time Configuration Wizard from a configuration file:

Step	Description
1	Run this command in Expert mode: `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.

To create a configuration file:

Step	Description
1	Run this command in Expert mode: `config_system -t <`*File Name*`>`
2	Open the file you created in a text editor.
3	Edit all parameter values as necessary.
4	Save the updated configuration file.

To validate a configuration file:

Run this command in Expert mode:

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

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 `config_system --help` to see the available parameters.

Parameter	Description	Valid values
`install_security_gw`	Installs Security Gateway, if set to `true`.	• `true` • `false`
`gateway_daip`	Configures the Security Gateway as Dynamic IP (DAIP) Security Gateway, if set to `true`.	• `true` • `false` **Note** - Must be set to `false`, if ClusterXL or Security Management Server is enabled.
`gateway_cluster_member`	Configures the Security Gateway as member of ClusterXL, if set to `true`.	• `true` • `false`
`install_security_managment`	Installs Security Management Server, if set to `true`.	• `true` • `false`
`install_mgmt_primary`	Makes the installed Security Management Server the Primary one. **Note** - The `install_security_managment` must be set to `true`.	• `true` • `false` **Note** - Can only be set to `true`, if the `install_mgmt_secondary` is set to `false`.
`install_mgmt_secondary`	Makes the installed Security Management Server a Secondary one. **Note** - The `install_security_managment` must be set to `true`.	• `true` • `false` **Note** - Can only be set to `true`, if the `install_mgmt_primary` is set to `false`.

Parameter	Description	Valid values
`install_mds_primary`	Makes the installed Security Management Server the Primary Multi-Domain Server. **Note** - The `install_security_managment` must be set to `true`.	• `true` • `false` **Note** - Can only be set to `true`, if the `install_mds_secondary` is set to `false`.
`install_mds_secondary`	Makes the installed Security Management Server a Secondary Multi-Domain Server. **Note** - The `install_security_managment` must be set to `true`.	• `true` • `false` **Note** - Can only be set to `true`, if the `install_mds_primary` is set to `false`.
`install_mlm`	Installs Multi-Domain Log Server, if set to `true`.	• `true` • `false`
`install_mds_interface`	Specifies Multi-Domain Server management interface.	Name of the interface exactly as it appears in the device configuration. Examples: `eth0`, `eth1`
`download_info`	Downloads Check Point Software Blade contracts and other important information, if set to `true` (**Best Practice -** Optional, but highly recommended). For more information, see sk94508 http://supportcontent.checkpoint.com/solutions?id=sk94508.	• `true` • `false`

Parameter	Description	Valid values
`upload_info`	Uploads data that helps Check Point provide you with optimal services, if set to `true` (**Best Practice -** Optional, but highly recommended). For more information, see sk94509 http://supportcontent.checkpoint.com/solutions?id=sk94509.	• `true` • `false`
`mgmt_admin_radio`	Configures Management Server administrator. **Note** - Must be provided, if you install a Management Server.	Set to `gaia_admin`, if you wish to use the Gaia `admin` account. Set to `new_admin`, if you wish to configure a new admin account.
`mgmt_admin_name`	Sets management administrator's username. **Note** - Must be provided, if `install_security_managment` is set to `true`.	A string of alphanumeric characters.
`mgmt_admin_passwd`	Sets management administrator's password. **Note** - Must be provided, if `install_security_managment` is set to `true`.	A string of alphanumeric characters.
`mgmt_gui_clients_radio`	Specifies SmartConsole clients that can connect to the Security Management Server.	• `any` • `range` • `network` • `this`
`mgmt_gui_clients_first_ip_field`	Specifies the first address of the range, if `mgmt_gui_clients_radio` is set to `range`.	Single IPv4 address of a host. Example: 192.168.0.10

Parameter	Description	Valid values
`mgmt_gui_clients_last_ip_field`	Specifies the last address of the range, if `mgmt_gui_clients_radio` is set to `range`.	Single IPv4 address of a host. Example: 192.168.0.20
`mgmt_gui_clients_ip_field`	Specifies the network address, if `mgmt_gui_clients_radio` is set to `network`.	IPv4 address of a network. Example: 192.168.0.0
`mgmt_gui_clients_subnet_field`	Specifies the netmask, if `mgmt_gui_clients_radio` is set to `network`.	A number from 1 to 32.
`mgmt_gui_clients_hostname`	Specifies the netmask, if `mgmt_gui_clients_radio` is set to `this`.	Single IPv4 address of a host. Example: 192.168.0.15
`ftw_sic_key`	Sets a secure Internal Community key, if `install_security_managment` is set to `false`.	A string of alphanumeric characters.
`admin_hash`	Sets administrator's password.	A string of alphanumeric characters, enclosed between single quotation marks.
`iface`	Interface name (optional).	Name of the interface exactly as it appears in the device configuration. Examples: `eth0`, `eth1`
`ipstat_v4`	Turns on static IPv4 configuration, if set to `manually`.	• `manually` • `off`
`ipaddr_v4`	Sets IPv4 address of the management interface.	Single IPv4 address.
`masklen_v4`	Sets IPv4 mask length for the management interface.	A number from 0 to 32.

Parameter	Description	Valid values
`default_gw_v4`	Specifies IPv4 address of the default gateway.	Single IPv4 address.
`ipstat_v6`	Turns static IPv6 configuration on, if set to `manually`.	• `manually` • `off`
`ipaddr_v6`	Sets IPv6 address of the management interface.	Single IPv6 address.
`masklen_v6`	Sets IPv6 mask length for the management interface.	A number from 0 to 128.
`default_gw_v6`	Specifies IPv6 address of the default gateway.	Single IPv6 address.
`hostname`	Sets the name of the local host (optional).	A string of alphanumeric characters.
`domainname`	Sets the domain name (optional).	Fully qualified domain name. Example: `somedomain.com`

`timezone`	Sets the Area/Region (optional).	The Area/Region must be enclosed between single quotation marks.
		Examples:
		`'America/New_York'`
		`'Asia/Tokyo'`
		Note - To see the available Areas and Regions, connect to any Gaia computer, log in to Gaia Clish, and run (names of Areas and Regions are case-sensitive):
		`set timezone Area`<SPACE><TAB>

`ntp_primary`	Sets the IP address of the primary NTP server (optional).	IPv4 address.

Parameter	Description	Valid values
`ntp_primary_version`	Sets the NTP version of the primary NTP server (optional).	• 1 • 2 • 3 • 4
`ntp_secondary`	Sets the IP address of the secondary NTP server (optional).	IPv4 address.
`ntp_secondary_version`	Sets the NTP version of the secondary NTP server (optional).	• 1 • 2 • 3 • 4
`primary`	Sets the IP address of the primary DNS server (optional).	IPv4 address.
`secondary`	Sets the IP address of the secondary DNS server (optional).	IPv4 address.
`tertiary`	Sets the IP address of the tertiary DNS server (optional).	IPv4 address.
`proxy_address`	Sets the IP address of the proxy server (optional).	IPv4 address, or Hostname.
`proxy_port`	Sets the port number of the proxy server (optional).	A number from 1 to 65535.
`reboot_if_required`	Reboots the system after the configuration, if set to `true` (optional).	• `true` • `false`

Centrally Managing Gaia Device Settings

In This Section:

Overview of Gaia Central Management 62
Managing Gaia in SmartConsole 62

Overview 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 operations

  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 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 changes

  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 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.

To run a one-time script:

Step	Description
1	Right-click the Security Gateway.
2	Select **Scripts > Run One Time Script**.
3	The **Run One Time Script** window opens You can: • Enter the command in the **Script Body** text box and specify script arguments, or • Load the complete command from a text file **Notes:** ▪ By default, the maximum size of a script is: 8 kilobytes. ▪ 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**. The output from the script shows in the **Tasks** tab **> Results** column. • Double-clicking the task shows the output in a larger window • You can also right-click the task, and select **View**, and then **Copy to Clipboard** **Notes:** ▪ The **Run One Time Script** window does not support interactive or continuous scripts. To run interactive or continuous scripts, open a command shell. ▪ If the gateways are not part of a Cloning Group, you can run a script on multiple gateways at the same time.

To run a Repository script:

Step	Description
1	Right-click the Security Gateway.
2	Select **Scripts > Run Repository Script**.
3	The **Select Script** window opens. You can: • Select a script from the drop-down box, or click **New** to create a new script for the repository. • Enter script arguments. **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**. The output from the script shows in the **Tasks** tab **> Results** column. • Placing the mouse in the **Details** column shows the output in a larger window. • 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.

To manage scripts:

Step	Description
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.

To run a script from the repository:

Step	Description
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**. The **Scripts Repository** window opens.
3	Do one of these steps: • Select an existing script from the list, click **Run**, enter **Arguments** if needed, and click **Run**. • 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 changes you made on the Security Gateway before you do a system backup operation.

To back up the system:

Step	Description
1	In the **Gateways & Servers** view, right-click the Security Gateway object you want to back up.
2	Select **Actions** > **System Backup**. The **System Backup** window opens.
3	Select the backup location. Use one of these options: • 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** • Enter the details of the backup server **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. The file name must be according to this convention: `backup_<`*Name of Security Gateway object*`>_<`*Date of Backup*`>.tgz`
4	Click **OK**. 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. **Notes:** • This name is necessary to do a system restore. • You can do backup on multiple Security Gateways at the same time. • When you back up a cluster, the system does backup on all members.

Restoring the System

To restore the system:

Step	Description
1	In the **Gateways & Servers** view, right-click the Security Gateway object you want to restore.
2	Select **Actions** > **System Restore**. The **System Restore** window opens.

3	Enter the required information.
	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:
	a) Right-click the Security Gateway object.
	b) Select **Actions** > **Open Shell**.
	c) On the Security Gateway, run the Gaia Clish command:
	`show backup logs`
	d) Find the name of the compressed backup file.
	The file is named according to this convention:
	`backup_<`*Name of Security Gateway object*`>_<`*Date of Backup*`>.tgz`

4	Click **OK**. a) Connectivity to the Security Gateway is lost. b) The Security Gateway automatically reboots.
5	Install the policy on the Security Gateway object. The status of the restore operation shows in **Tasks** tab.

Opening Gaia Portal and Gaia Clish

From 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.

To open a command line window on the Security Gateway:

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

To open a Security Gateway Gaia Portal:

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

Network Management

In This Section:

Network Interfaces 69
ARP 107
DHCP Server 111
Hosts and DNS 118
IPv4 Static Routes 124
IPv6 Static Routes 131
Configuring IPv6 Neighbor-Entry - Gaia Clish 136
Netflow Export 137

This chapter includes configuration procedures and examples for network management.

Network Interfaces

Gaia supports these network interface types:

- Ethernet physical interfaces
- Alias (Secondary IP addresses for different interface types. This is not supported in ClusterXL.)
- VLAN
- Bond
- Bridge
- Loopback
- 6in4 tunnel
- PPPoE

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, the incorrect topology is shown. If this occurs, run `cpstop` and then `cpstart` in Expert mode.

Interface Link Status

You can see the status of physical and logical interfaces in the Gaia Portal or the Gaia Clish.

To see interface status in the 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 (grey)	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 the Gaia Clish:

Run one of these commands:

```
show interfaces all
show interface <Name of Interface>
```

Physical Interfaces

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

To add or remove an interface card:

Step	Description
1	Turn off the Gaia computer: • In Gaia Portal: Click **Maintenance > Shut Down**, and click **Halt** • In Gaia Clish: 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 - Gaia Portal

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

To configure a physical interface:

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:
   - Select **Obtain IPv4 address automatically** to get the IPv4 address from the DHCPv4 server.
   - Enter the IPv4 address and subnet mask in the applicable fields.
6. On the **IPv6** tab (optional), do one of these:
   - Select **Obtain IPv6 address automatically** to get the IPv6 address from the DHCPv6 server.
   - Enter the IPv6 address and mask length in the applicable fields.

   Important - First, you must enable the IPv6 Support (on page 188) and reboot.

7. On the **Ethernet** tab:
   - Select **Auto Negotiation**, or select a link speed and duplex setting from the list.
   - In the **Hardware Address** field, enter the Hardware MAC address (if not automatically received from the NIC).

     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.
   - In the **MTU** field, enter the applicable Maximum Transmission Unit (MTU) value (minimal value is 68, maximal value is 16000, and default value is 1500).
   - Select **Monitor Mode**, if needed. For more information, see sk101670 http://supportcontent.checkpoint.com/solutions?id=sk101670.
8. Click **OK**.

Configuring Physical Interfaces - Gaia Clish

Description

Configure physical interfaces.

Syntax

- To configure a physical interface:

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

- To see the configuration of a physical interface:

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

```
show interfaces all
```

- To delete a physical interface configuration:

```
delete interface <Name of Physical Interface>
      6in4 "<6in4 ID>"
      alias
      ipv4-address
      ipv6-address
      loopback
      vlan
```

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

Parameters

Parameter	Description
`interface` *<Name of Physical Interface>*	Specifies a physical interface.
`auto-negotiation {on | off}`	Configures automatic negotiation of interface link speed and duplex settings: • `on` - Enabled • `off` - Disabled
`comments` "*<Text>*"	Configures an optional free text comment. • Write the text in double-quotes. • Text must be up to 100 characters. • This comment appears in the Gaia Portal and in the output of the show configuration command.
`ipv4-address` *<IPv4 Address>*	Assigns the IPv4 address.
`mask-length` *<Mask Length>*	Configures the IPv4 or IPv6 subnet mask length using CIDR notation (/xx).
`subnet-mask` *<Mask>*	Configures the IPv4 subnet mask using dotted decimal notation (X.X.X.X).
`ipv6-address` *<IPv6 Address>*	Assigns the IPv6 address. **Important -** First, you must enable the IPv6 Support (on page 188) and reboot.
`ipv6-autoconfig {on | off}`	Configures if this interface gets an IPv6 address from a DHCPv6 Server: • `on` - Gets an IPv6 address from a DHCPv6 Server • `off` - Does not get an IPv6 address from a DHCPv6 Server (you must assign it manually) **Important -** First, you must enable the IPv6 Support (on page 188) and reboot.
`link-speed` *<Speed_Duplex>*	Configures the interface link speed and duplex status. Available speed and duplex combinations are: • `10M/half` • `10M/full` • `100M/half` • `100M/full` • `1000M/full` • `10000M/full`

Parameter	Description
`mac-addr <MAC Address>`	Configures the interface hardware MAC address.
`monitor-mode {on | off}`	Configures Monitor Mode on this interface: • `on` - Enabled • `off` - Disabled For more information, see sk101670 http://supportcontent.checkpoint.com/solutions?id=sk101670.
`mtu <68-16000 | 1280-16000>`	Configures the Maximum Transmission Unit size for an interface. For IPv4: • **Range:** 68 - 16000 bytes • **Default:**1500 bytes For IPv6: • **Range:** 1280 - 16000 bytes • **Default:**1500 bytes
`rx-ringsize <0-4096>`	Configures RX ring buffer size. • **Range:** 0 - 4096 bytes • **Default:** Depends on the interface driver
`state {on | off}`	Configures interface's state: • `on` - Enabled • `off` - Disabled
`tx-ringsize <0-4096>`	Configures TX ring buffer size. • **Range:** 0 - 4096 bytes • **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 1500

gaia> set interface eth2 link-speed 1000M/full

gaia> set interface eth2 state on

gaia> show interface eth2
```

Note - There are some command options and parameters, which you cannot configure in the Gaia Portal.

Aliases

Interface aliases let you assign more than one IPv4 address to physical or virtual interfaces (Bonds, Bridges, VLANs and Loopbacks). This section shows you how to configure an alias using the Gaia Portal and the Gaia Clish.

Configuring Aliases - Gaia Portal

To add an interface alias:

Step	Description
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 interface, to which this alias is assigned.
5	Click **OK**.

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.

Note - You cannot change the interface alias settings.

To delete an interface alias:

Step	Description
1	In the navigation tree, click **Network Management** > **Network Interfaces**.
2	Select an interface alias and click **Delete**.
3	When the confirmation message shows, click **OK**.

Configuring Aliases - Gaia Clish

Description

Configure an alias IPv4 address on a physical or virtual interface.

Syntax

- To add an alias:
  ```
  add interface <Name of Interface> alias <IPv4 Address>/<Mask Length>
  ```
- To see the configured aliases:
  ```
  show interface <Name of Interface> aliases
  ```
- To delete 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.

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.

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
```

VLAN Interfaces

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.

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

Configuring VLAN Interfaces - Gaia Portal

Step	Description
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**. To configure an existing VLAN interface, select the VLAN interface and click **Edit**.
4	In the **Add VLAN** (or **Edit VLAN**) window, select the **Enable** option to set the VLAN interface to UP.
5	On the **IPv4** tab, enter the IPv4 address and subnet mask. You can optionally select the **Obtain IPv4 Address automatically** option.
6	On the **IPv6** tab, enter the IPv6 address and mask length. You can optionally select the **Obtain IPv6 Address automatically** option. **Important -** First, you must enable the IPv6 Support (on page 188) and reboot.
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 physical interface related to this VLAN.

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.

Configuring VLAN Interfaces - Gaia Clish

This section is a reference for the VLAN interface commands.

Description

Use these commands to configure bridge interfaces.

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

Syntax

Note - This syntax shows only options that VLAN interfaces support.

- To add a VLAN interface:

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

- To configure a VLAN interface:

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

- To remove the configuration of a VLAN interface:

```
delete interface <Name of VLAN Interface>
      alias <Name of Alias Interface>
      ipv4-address
      ipv6-address
```

- To see the configured VLAN interfaces:

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

```
show interfaces all
```

- To delete 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

Parameter	Description
`interface` <*Name of Physical Interface*>	Configures a physical interface.
`comments` "*Text*"	Defines the optional comment. • Write the text in double-quotes. • Text must be up to 100 characters. • This comment appears in the Gaia Portal and in the output of the `show configuration` command.

Parameter	Description
`interface` <*Name of VLAN Interface*>	Configures a VLAN interface.
<*VLAN ID*>	Configures the ID of the VLAN interface (integer between 2 and 4094).
`ipv4-address` <*IPv4 Address*>	Assigns an IPv4 address.
`mask-length` <*Mask Length*>	Configures the IPv4 or IPv6 subnet mask length using CIDR notation (/xx) - integer between 2 and 32.
`subnet-mask` <*Mask*>	Configures the IPv4 subnet mask using dotted decimal notation (X.X.X.X).
`ipv6-address` <*IPv6 Address*>	Assigns an IPv6 address. **Important -** First, you must enable the IPv6 Support (on page 188) and reboot.
`ipv6-autoconfig {on | off}`	Configures if this interface gets an IPv6 address from a DHCPv6 Server: • `on` - Gets an IPv6 address from a DHCPv6 Server • `off` - Does not get an IPv6 address from a DHCPv6 Server (you must assign it manually) **Important -** First, you must enable the IPv6 Support (on page 188) and reboot.
`mtu <68-16000 | 1280-16000>`	Configures the Maximum Transmission Unit size for an interface. For IPv4: • **Range:** 68 - 16000 bytes • **Default:** 1500 bytes For IPv6: • **Range:** 1280 - 16000 bytes • **Default:** 1500 bytes
`state {on | off}`	Configures interface's state: • `on` - Enabled • `off` - Disabled

Example

```
gaia> add interface eth1 vlan 99

gaia> set interface eth1.99 ipv4-address 99.99.99.1 subnet-mask 255.255.255.0

gaia> delete interface eth1.99 ipv4-address

gaia> set interface eth1.99 ipv6-address 209:99:1 mask-length 64

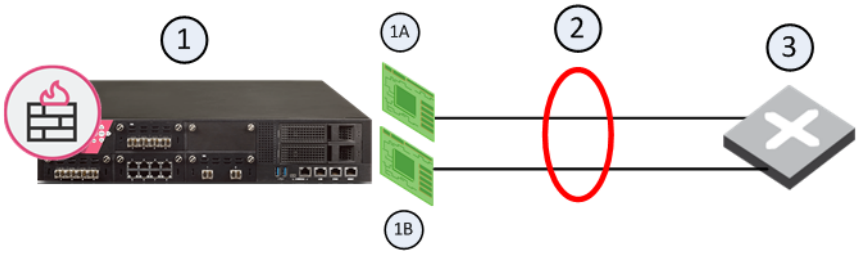
gaia> set interface eth1.99 state on

gaia> show interface eth1.99

gaia> delete interface eth1 vlan 99
```

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 (LCAP) for dynamic link aggregation.



Item No.	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 **slaves** and do not have IP addresses.

You can define 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 slave interface is down, the connection automatically fails over to the primary slave interface. If the primary slave interface is not available, the connection fails over to a different slave interface.
- **Load Sharing (Active/Active)**: All Active slave interfaces are used simultaneously. Traffic is distributed among the slave interfaces to maximize throughput. Bond Load Sharing does not support switch redundancy.

  Note - Link Aggregation 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:
  - **Round Robin** - Selects the active slave interface sequentially.
  - **802.3ad** - Dynamically uses Active slave interfaces to share the traffic load. This mode uses the LACP protocol, which fully monitors the interface between the gateway and a switch.
  - **XOR** - All UP slave interfaces are Active for Load Sharing. Traffic is assigned to Active interfaces based on the transmit hash policy (Layer2 or Layer3+4).

For Link Aggregation High Availability mode and for Link Aggregation Load Sharing mode:

- The number of bond interfaces that can be defined is limited by the maximal number of interfaces supported by each platform. See the *R80.10 Release Notes*.
- Up to 8 slave interfaces can be configured in a single High Availability or Load Sharing bond interface.

Configuring Bond Interfaces - Gaia Portal

To configure a bond interface:

Step	Description
1	In the navigation tree, click **Network Management** > **Network Interfaces**.
2	Make sure that the slave interfaces, which you wish to add to the Bond interface, do not have IP addresses.
3	For a new bond interface, select **Add** > **Bond**. 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. You can optionally select the **Obtain IPv4 Address automatically** option.
5	On the **IPv6** tab (optional), enter the IPv6 address and mask length. You can optionally select the **Obtain IPv6 Address automatically** option. **Important -** First, you must enable the IPv6 Support (on page 188) and reboot.
6	On the **Bond** tab: a) Select or enter a **Bond Group ID**. This parameter is an integer between 0 and 1024. b) Select the slave interfaces from the **Available Interfaces** list and then click **Add**. **Note -** Make sure that the slave interfaces do not have any IP addresses or aliases configured. c) Select an **Operation Mode**: ▪ **Round Robin** (default) - Bond uses all slave interfaces sequentially (High Availability + Load Sharing) ▪ **Active-Backup** - Bond uses one slave interface at a time (High Availability) ▪ **XOR** - Bond uses slave interfaces based on a hash function (High Availability + Load Sharing) ▪ **802.3ad** - Dynamic bonding according to IEEE 802.3ad (Load Sharing)

Step	Description
7	On the **Advanced** tab: a) Set the required **MTU** for your network (if not sure, leave the default value). b) Set the **Monitor Interval** - How much time to wait between checking each slave interface for link-failure. The valid range is 1-5000 ms. The default is 100 ms. c) Set the **Down Delay** - How much time to wait, after sending a monitor request to a slave interface, before bringing down the slave interface. The valid range is 1-5000 ms. The default is 200 ms. d) Set the **Up Delay** - How much time to wait, after sending a monitor request to a slave interface, before bringing up the slave interface. The valid range is 1-5000 ms. The default is 200 ms.
8	Additional configuration settings are available depending on the selected Bond Operation Mode: • If selected the **Round Robin** bond operation mode, then there are no additional configuration settings. • If selected the **Active-Backup** bond operation mode, then select the **Primary Interface** • If selected the **XOR** bond operation mode, then select the **Transmit Hash Policy** - the algorithm for slave interface selection according to the specified TCP/IP Layer. Select either **Layer 2** (uses XOR of the physical interface MAC address), or **Layer 3+4** (uses Layer 3 and Layer 4 protocol data). • If selected the **802.3ad** bond operation mode, then perform these two steps: Select the **Transmit Hash Policy** - the algorithm for slave interface selection according to the specified TCP/IP Layer. Select either **Layer 2** (uses XOR of the physical interface MAC address), or **Layer 3+4** (uses IP addresses and Ports). Select the **LACP Rate** - how frequently the LACP partner should transmit LACPDUs. Select either **Slow** (every thirty seconds), or **Fast** (every one second).
9	Click **OK**.

Configuring Bond Interfaces - Gaia Clish

In the CLI, bond interfaces are known as **bonding groups**.

Important: After you run a Gaia Clish command to add, configure, or delete an object, run the `save config` command to save the settings permanently.

To create a bond interface in the Gaia Clish:

Step	Description
1	Make sure that the slave interfaces do not have IP addresses.
2	Create the bond interface (on page 87).
3	Define the slave interfaces (on page 87) and set them to the UP state.
4	Set the bond operating mode (on page 87).
5	Define other bond parameters: primary interface (on page 87), media monitoring (on page 88), and delay rate (on page 88).

Link Aggregation (Bonding) - Quick Reference for Gaia Clish Commands

This is a quick reference for Link Aggregation commands. Use these commands to configure Link Aggregation.

Note - You configure an IP address on a Bonding Group in the same way as you do on a physical interface (on page 71).

Syntax

- To create a bonding group and add slave interfaces:

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

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

- To configure a bonding group:

  Note - All these parameters are optional. You can configure any of these parameters together.

```
set bonding group <Bond Group ID>
      [down-delay <Value in msec>]
      [mii-interval <Value in msec>]
      [mode
      round-robin
      active-backup [primary <Name of Slave Interface>]
      xor xmit-hash-policy {layer2 | layer3+4}
      8023AD [lacp-rate {slow | fast}]
      ]
      [up-delay <Value in msec>]
```

- To show the specific bonding group:

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

- To show the configured bonding groups:

```
show bonding groups
```

- To delete a slave interface from the bonding group:

```
delete bonding group <Bond Group ID> interface <Name of Slave Interface>
```

- To delete the bonding group:

  Note - You must delete all slave interfaces before you can delete the bonding group.

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

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

Parameters

Parameter	Description
<*Bond Group ID*>	Configures the Bond Group ID. • **Range:** 0 - 1024 • **Default:** No default value
`interface` <*Name of Slave Interface*>	Specifies the name of the slave physical interface, which you add to (or remove from) the bond group. Make sure that the slave interfaces do not have any IP addresses or aliases configured.
`down-delay` <*Value in msec*>	Configures how much time to wait, after sending a monitor request to a slave interface, before bringing down the slave interface. • **Range:** 1 - 5000 ms • **Default:** 200 ms
`mii-interval` <*Value in msec*>	Configures how much time to wait between checking each slave interface for link-failure. • **Range:** 0 (to disable), 1 - 5000 ms (to enable) • **Default:** 100 ms
`mode {round-robin | active-backup | xor | 8023AD}`	Configures the Bond operating mode (on page 87): • `round-robin`: Bond uses all slave interfaces sequentially (High Availability + Load Sharing). This is the default mode. • `active-backup [primary` <*Name of Slave Interface*>`]`: Bond uses one slave interface at a time (High Availability) • `xor xmit-hash-policy {layer2 | layer3+4}`: Bond uses slave interfaces based on a hash function (High Availability + Load Sharing) • `8023AD [lacp-rate {slow | fast}]`: Dynamic bonding according to IEEE 802.3ad (Load Sharing)

Parameter	Description
`primary` <*Name of Slave Interface*>	Applies only to Active-Backup bond operation mode. Select one of the interfaces as primary interface for the bonding group. Default: The first interface added to the bond group becomes the primary.
`xmit-hash-policy {layer2 | layer3+4}`	Applies only to XOR and 8023AD bond operation modes. Configures the Transmit Hash Policy - the algorithm for slave interface selection according to the specified TCP/IP Layer: • `layer2` - Uses XOR of the physical interface MAC address • `layer3+4` - Uses Layer 3 and Layer 4 protocol data
`lacp-rate {slow | fast}`	Applies only to 8023AD bond operation mode. Configures how frequently the LACP partner should transmit LACPDUs: • `slow` - Every thirty seconds • `fast` - Every one second
`up-delay` <*Value in msec*>	Configures how much time to wait, after sending a monitor request to a slave interface, before bringing up the slave interface. • **Range:** 1 - 5000 ms • **Default:** 200 ms

Example

```
Gaia> add bonding group 20 interface eth2

Gaia> add bonding group 20 interface eth3

Gaia> show bonding groups
Bonding Interface: 20
    Bond Configuration
        xmit_hash_policy Not configured
        down-delay 200
        primary Not configured
        mode round-robin
        up-delay 200
        mii-interval 100
        lacp_rate Not configured
        Bond Interfaces
            eth2
            eth3

Gaia> delete bonding group 20 interface eth3

Gaia> delete bonding group 20 interface eth2

Gaia> delete bonding group 20
```

Creating a Bond Interface

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.

Configuring the Bond Operating Mode

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

Syntax

```
set bonding group <Bond Group ID> mode
      round-robin
      active-backup [primary <Name of Slave Interface>]
      xor xmit-hash-policy {layer2 | layer3+4}
      8023AD [lacp-rate {slow | fast}]
```

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 slave interface.
- The XOR mode requires the configuration of the transmit hash policy.
- The 8023AD mode supports the configuration of the LACP packet transmission rate.

Adding Slave Interfaces to a Bond

Syntax

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

Example

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

Notes:

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

Defining the Primary Slave Interface

With the **Active-Backup** operating mode, the system automatically fails over to the primary slave interface, if available. If the primary interface is not available, the system fails over to a different slave interface. By default, the first slave interface that you define is the primary interface. You must define the slave interfaces and set the operating mode as Active-Backup before doing this procedure.

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

To define the primary slave interface:

```
set bonding group <Bond Group ID> mode active-backup primary <Name of Slave Interface>
```

Example

```
gaia> add bonding group 777 interface eth4

gaia> add bonding group 777 interface eth5

gaia> set bonding group 777 mode active-backup primary eth5
```

Defining the Monitoring Interval

This configures how much time to wait between checking each slave interface for link-failure. The valid range is 1-5000 ms. The default is 100 ms.

To configure the monitoring interval:

```
set bonding group <Bond Group ID> mii-interval <Value in msec>
```

Example:

```
gaia> set bonding group 777 mii-interval 500
```

To disable monitoring:

```
set bonding group <Bond ID> mii-interval 0
```

Configuring the Up Delay and Down Delay Times

The **Up-Delay** specifies show much time in milliseconds to wait before enabling a slave 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.

The **Down-Delay** specifies how much time in milliseconds to wait before disabling a slave 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.

Defining Load Sharing Parameters

When using Load Sharing modes (XOR or 802.3ad), you can configure these parameters:

- **LACP Rate** (802.3ad mode only) - Set the Link Aggregation Control Protocol packet transmission rate. Valid values are **slow** (every 30 seconds) and **fast** (every 1 second).
- **Transmit Hash Policy** - Set the algorithm for slave interface selection according to the specified TCP/IP layer. Valid values are **layer2** (uses XOR of the physical interface MAC address) and **layer3+4** (uses Layer 3 and Layer 4 protocol data).

To set the LACP rate:

```
set bonding group <Bond Group ID> mode 8023AD lacp-rate {slow | fast}
```

Example:

```
gaia> set bonding group 777 mode 8023AD lacp-rate slow
```

To set the Transmit Hash Policy:

```
set bonding group <Bond Group ID> mode xor xmit-hash-policy {layer2 | layer3+4}
```

Example:

```
gaia> set bonding group 777 mode xor xmit-hash-policy layer2
```

Making Sure that Bond Interface is Working

To make sure that a Bond interface is working, run this command in Expert mode:

```
[Expert@Gaia:0]# cat /proc/net/bonding/<Bond Group ID>
```

Example output for **Round Robin** mode:

```
[Expert@Gaia: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@Gaia:0]#
```

Example output for **Active-Backup** mode:

```
[Expert@Gaia: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@Gaia:0]#
```

Example output for **XOR** mode:

```
[Expert@Gaia: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@Gaia:0]#
```

Example output for **802.3ad** mode:

```
[Expert@Gaia: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@Gaia:0]#
```

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.

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.

You can configure bridge mode with one Security Gateway or with a cluster. The bridge functions without an assigned IP address. Bridged Ethernet interfaces (including aggregated interfaces) to work like ports on a physical bridge. You can 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:

- Gaia does not support Spanning Tree Protocol (STP) bridges.
- A slave interface that is a part of a bond interface cannot be a part of a bridge interface.

Check Point supports bridge interfaces that implement native, Layer-2 bridging. 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 - Gaia Portal

Step	Description
1	In the navigation tree, click **Network Management** > **Network Interfaces**.
2	Make sure that the slave interfaces, which you wish to add to the Bridge interface, do not have IP addresses.
3	Click **Add** > **Bridge**. 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**. **Notes:** • Make sure that the slave interfaces do not have any IP addresses or aliases configured. • A Bridge interface in Gaia can contain only two slave interfaces.
6	On the **IPv4** tab, enter the IPv4 address and subnet mask. You can optionally select the **Obtain IPv4 Address automatically** option.

Step	Description
7	On the **IPv6** tab (optional), enter the IPv6 address and mask length. You can optionally select the **Obtain IPv6 Address automatically** option. **Important -** First, you must enable the IPv6 Support (on page 188) and reboot.
8	Click **OK**.

Configuring Bridge Interfaces - Gaia Clish

Description

Bridge interfaces are known as Bridging Groups in Gaia Clish commands. You can assign an IPv4 or IPv6 address to a bridge interface.

Syntax

- To add a new bridging group:
```
add bridging group <Bridge Group ID>
```
- To add a slave interface to the bridging group:
```
add bridging group <Bridge Group ID> interface <Name of Slave Interface>
```
Note - Make sure that the slave interfaces do not have any IP addresses or aliases configured.
- To add a fail-open interface to the bridging group:
```
add bridging group <Bridge Group ID> fail-open-interfaces <Name of Slave Interface>
```
- To configure a bridge interface settings:
```
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>
```
- To show the slave interfaces of a specific bridging group:
```
show bridging group <Bridge Group ID>
```
- To show the configured bridging groups:
```
show bridging groups
```
- To remove a slave interface from the bridging group:
```
delete bridging group <Bridge Group ID> interface <Name of Slave Interface>
```
- To remove a fail-open interface from the bridging group:
```
delete bridging group <Bridge Group ID> fail-open-interfaces <Name of Slave Interface>
```
- To delete a bridging group:
```
delete bridging group <Bridge Group ID>
```

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

Parameters

Parameter	Description
<*Bridge Group ID*>	Configures the Bridge Group ID. • **Range:** 0 - 1024 • **Default:** No default value
<*Name of Slave Interface*>	Specifies a physical slave interface.
<*Name of Bridge Interface*>	Configures the name of the Bridge interface.
`comments "`*Text*`"`	Configures an optional free text comment. • Write the text in double-quotes. • Text must be up to 100 characters. • 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. **Important -** First, you must enable the IPv6 Support (on page 188) and reboot.
`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: • `on` - Gets an IPv6 address from a DHCPv6 Server • `off` - Does not get an IPv6 address from a DHCPv6 Server (you must assign it manually) **Important -** First, you must enable the IPv6 Support (on page 188) and reboot.
`mac-addr` <*MAC Address*>	Configures the hardware MAC address.
`mtu <68-16000 | 1280-16000>`	Configures the Maximum Transmission Unit size for an interface. For IPv4: • **Range:** 68 - 16000 bytes • **Default:** 1500 bytes For IPv6: • **Range:** 1280 - 16000 bytes • **Default:** 1500 bytes

Parameter	Description
`rx-ringsize <0-4096>`	Configures the receive buffer size. • **Range:** 0 - 4096bytes • **Default:** 4096 bytes
`tx-ringsize <0-4096>`	Configures the transmit buffer size. • **Range:** 0 - 4096 bytes • **Default:** 4096 bytes

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
```

Notes:

- Make sure that the slave interfaces do not have any IP addresses or aliases configured.
- Only Ethernet, VLAN, and Bond interfaces can be added to a bridge group.
- A bridge interface in Gaia OS can contain only two slave interfaces.
- Do not change the state of bond interface manually using the `set interface <Bridge Group ID> state {on|off}` command. This is done automatically by the bridging driver.
- You must delete all slave interfaces from the bridge before you remove the bridge interface.

Loopback Interfaces

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 using the Gaia Portal and the Gaia Clish.

Configuring Loopback Interfaces - Gaia Portal

To add a loopback interface:

Step	Description
1	In the navigation tree, click **Interface Management** > **Network Interfaces**.
2	Click **Add** > **Loopback**.
3	In the **Add loopback** window: a) The **Enable** option is selected by default to set the loopback interface status to UP. b) In the **Comment** field, enter the applicable comment text (up to 100 characters). c) On the **IPv4** tab, enter the IPv4 address and subnet mask. These IPv4 addresses are **not** allowed: ▪ 0.x.x.x ▪ 127.x.x.x ▪ 224.x.x.x - 239.x.x.x (Class D) ▪ 240.x.x.x - 255.x.x.x (Class E) ▪ 255.255.255.255 d) On the **IPv6** tab (optional), enter the IPv6 address and mask length. **Important -** First, you must enable the IPv6 Support (on page 188) and reboot.
4	Click **OK**.

The new loopback interface name is automatically created with the addition of a sequence number to the string '**loop**'. For example, the name of first loopback interface is **loop00**. The second loopback interface is **loop01**, and so on.

To configure a loopback interface:

Step	Description
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: a) If required, change the IPv4 address and subnet mask. b) If required, change the IPv6 address and mask length.
4	Click **OK**.

To delete a loopback interface:

Step	Description
1	In the navigation tree, click **Network Management** > **Network Interfaces**.
2	Select a loopback interface and click **Delete**.
3	When the confirmation message shows, click **OK**.

Configuring Loopback Interfaces - Gaia Clish

Description

Configure loopback interfaces.

Syntax

- To add a loopback interface:
```
add interface lo loopback <IP Address>/<Mask>
```
- To see the configured loopback interface:
```
show interface <Name of Loopback Interface>
```
```
show interfaces all
```
- To delete a loopback interface:
```
delete interface lo loopback <Name of Loopback Interface>
```

Parameters

Parameter	Description
`loopback`	Configures a loopback interface.
`lo`	You must use the `lo` (local interface) keyword to define a loopback interface.
<*IP Address*>	Assigns an IPv4 or IPv6 address.
<*Mask*>	Configures an IPv4 subnet mask or IPv6 mask length using CIDR (/xx) notation.
<*Name of Loopback Interface*>	Name of Loopback Interface (`loop`XX)

Example

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

gaia> add interface lo loopback 2010:10:99::1/64

gaia> show interface loop01

gaia> delete interface lo loopback loop01
```

Comment

When you create a new loopback interface, Gaia automatically assigns a name in the format `loop`XX, where XX is a sequence number starting from 00.

Important - After using Gaia Clish commands to add, configure or delete features, you must run the `save config` command. This makes sure that the new configuration settings remain after reboot.

VPN Tunnel Interfaces

Virtual Tunnel Interface. A virtual interface that is a member of an existing, Route-Based, VPN tunnel. Each peer Security Gateway has one VTI that connects to the tunnel.

The VPN tunnel and its properties are defined by the VPN community that contains the two gateways. You must define the VPN community and its member Security Gateways before you can create a VTI. To learn more about Route Based VPN, see *Route Based VPN* in the *R80.10 Site to Site VPN Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=60371.

The procedure for configuring a VTI includes these steps:

1. Make sure that the IPsec VPN Software Blade is enabled on the applicable Security Gateways.
2. Create and configure the Security Gateways.
3. Define a VPN community in SmartDashboard (on page 99) that includes the two peer Security Gateways.
4. Make Route Based VPN the default option (on page 100). Do this procedure one time for each Security Management Server.
5. Define the VTI (on page 101) using the Gaia Portal, or Gaia Clish.
6. Define Route Based VPN Rules (on page 103).
7. Save the configuration and install the policy.

Defining the VPN Community

You must define 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 *R80.10 Site to Site VPN Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=60371.

To define a VPN Community for Site to Site VPN:

1. In SmartConsole, click the VPN Communities tab  in the navigation tree.
2. Right-click **Site To Site** and select **New Site To Site** > **Meshed** or **Star**.
3. In the **Community Properties** window **General** tab, enter the VPN community name.
4. Select **Accept all encrypted traffic**.

   This option automatically adds a rule to encrypt all traffic between gateways in a VPN community.
5. On the **Participating Gateways** tab, select member gateways from the list.

   For star communities, use the **Center Gateways** and **Satellite Gateways** tabs to do this.
6. Configure other community parameters as necessary.
7. Publish your session.

Making Route Based VPN the Default Option

When Domain Based VPN and Route Based VPN are defined 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 defines 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.

To define an empty group:

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

To make Route Based VPN the default choice:

Step	Description
1	In SmartConsole, double-click the applicable Security Gateway.
2	In the **Gateway** pane, click **Topology**.
3	In the **VPN Domain** section, select **Manually define** and then select the empty group you created earlier.
4	Install the Access Policy.

Do these steps for each Security Gateway.

Configuring VPN Tunnel Interfaces

You can configure the VPN Tunnel Interfaces using Gaia Portal or Gaia Clish.

Configuring VPN Tunnel Interfaces - Gaia Portal

This section shows you how to configure a VPN Tunnel interface using the Gaia Portal.

To configure a VPN Tunnel Interface:

Step	Description
1	In the Gaia Portal, select **Network Management** > **Network Interfaces**.
2	Click **Add** > **VPN Tunnel**. To configure an existing VTI interface, select the VTI interface and click **Edit**.
3	In the **Add/Edit** window, configure these parameters: • **VPN Tunnel ID** - Unique tunnel name (integer from 1 to 99). Gaia automatically adds the prefix 'vpnt' to the tunnel name. • **Remote Peer Name** - Remote peer name as defined in the VPN community. You must define the two peers in the VPN community before you can define the VTI. The Peer ID is an alphanumeric character string. • **VPN Tunnel Type** - Select **Numbered** or **Unnumbered**. • **Local Address** - Defines the local peer IPv4 address (numbered VTI only). • **Remote Address** - Defines the remote peer IPv4 address (numbered VTI only). • **Physical Device** - Local peer interface name (unnumbered VTI only).

Configuring VPN Tunnel Interfaces - Gaia Clish

This section summarizes the Gaia Clish commands for VPN Tunnel Interface (VTI).

Description

Add or delete a VPN Tunnel Interface (VTI).

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 <Name of VTI>
```
- To see the 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.

Parameters

Parameter	Description
<Tunnel ID>	Defines the unique Tunnel ID (integer from 1 to 99). Gaia automatically adds the prefix '`vpnt`' to the Tunnel ID. Example: `vnpt10`
`type numbered`	Defines a **numbered** VTI that uses a specified, static IPv4 addresses for local and remote connections.
`type unnumbered`	Defines an **unnumbered** VTI that uses the interface and the remote peer name to get addresses.
`local` *<Local IP address>*	Defines the local peer IPv4 address in dotted decimal format (numbered VTI only).
`remote` *<Remote IP address>*	Defines the remote peer IPv4 address in dotted decimal format (numbered VTI only).
`peer` *<Peer Name*	Specifies the name of the remote peer as defined in the VPN community. You must define the two peers in the VPN community before you can define the VTI. The Peer Name is an alphanumeric character string.
`dev` *<Name of Local Interface>*	Defines the name of the local interface (unnumbered VTI only).

Example

```
gaia> add vpn tunnel 20 type numbered local 10.10.10.1 remote 20.20.20.1 peer
MyPeer

gaia> add vpn tunnel 10 type unnumbered peer MyPeer dev eth1

gaia> show vpn tunnels

gaia> delete vpn tunnel 10
```

Defining 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. This section includes procedures for configuring security rules to do this.

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`

MyIntranet is the name of a VPN Community.

Internal_Clear refers to all traffic from IP addresses to and from the specified VPN community.

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

Note - It is not necessary to define bidirectional matching rules if the VPN column contains the **Any** value.

To enable VPN directional matching:

Step	Description
1	In SmartConsole, click **Menu** > **Global properties** > expand **VPN** > **Advanced**.
2	Select the **Enable VPN Directional Match in VPN Column** option.
3	In SmartConsole, double-click each member gateway and click the **Topology** page. a) Click **Get** > **Interfaces with Topology** to update the topology to include the newly defined VTIs. b) Click **Accept**.

To define a VPN directional matching rule:

Step	Description
1	Double-click the VPN cell in the applicable rule.
2	In the **VPN Match Conditions** window, select **Match traffic in this direction only**.
3	Click **Add** to define sets of matching conditions.
4	In the **Direction VPN Match Condition** window, select the source and destination matching conditions. Do this step for each set of matching conditions.

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. This section shows you how to allow OSPF traffic in a VPN community.

To learn about configuring OSPF, see the *R80.10 Gaia Advanced Routing Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=54803.

To Allow OSPF traffic for a VPN Community:

1. Using the Gaia Portal or Gaia Clish, add the applicable VPN Tunnel Interfaces to the OSPF configuration page.
2. In SmartConsole, add an access rule that allows traffic to the VPN community (or all communities) using the OSPF service.

Name	Source	Destination	VPN	Service	Action
Allow OSPF	Any	Any	MyIntranet	ospf	Accept

Completing the VTI Configuration

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

To complete the VTI configuration:

Step	Description
1	Save the configuration to the database.
2	Install the policy on the Security Gateways.
3	Make sure that the VTI tunnel and the rules are working correctly.

CLI Reference (interface)

This section summarizes the Gaia Clish `interface` command and its parameters.

Description

Add, delete and configure interface properties.

Syntax

- To add an interface:

```
add interface
      <Name of Interface> 6in4 "<Tunnel ID>" remote <IPv4 Address> [ttl <Time>]
      <Name of Interface> alias <IPv4 Address>/<Mask Length>
      <Name of Interface> vlan <VLAN ID>
      lo loopback <IP Address>/<Mask>
```

- To configure an interface:

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

- To see the configuration of an interface:

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

```
show interfaces all
```

- To delete an interface:

```
delete interface <Name of Interface>
      6in4 "<Tunnel ID>"
      6to4 "<Tunnel ID>"
      alias <Name of Alias Interface>
      ipv4-address <IPv4 Address>
      ipv6-address <IPv6 Address>
      ipv6-autoconfig
      loopback <IP Address>
      vlan <VLAN ID>
```

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

Parameters

See the specific sections:

- Configuring Physical Interfaces - Gaia Clish (on page 72)
- Configuring Aliases - Gaia Clish (on page 75)
- Configuring VLAN Interfaces - Gaia Clish (on page 77)
- Configuring Bond Interfaces - Gaia Clish (on page 83)
- Configuring Bridge Interfaces - Gaia Clish (on page 93)
- Configuring Loopback Interfaces - Gaia Clish (on page 97)
- Configuring VPN Tunnel Interfaces - Gaia Clish (on page 101)

Comment

There are some command options and parameters, which you cannot configure in the Gaia Portal.

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 - Gaia Portal

To show dynamic ARP entries:

1. In the navigation tree, click **Network Management > ARP**.
2. In the upper right corner, click the **Monitoring** tab.

To show static ARP entries:

1. In the navigation tree, click **Network Management > ARP**.
2. In the upper right corner, click the **Configuration** tab.

To change static and dynamic ARP parameters:

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:
   a) Enter the **Maximum Entries.** This is the maximal number of entries in the ARP cache.

      Range: 1024 - 16384 entries

      Default: 4096 entries

      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.

   b) Enter the **Validity Timeout.** This is the time, in seconds, to keep resolved dynamic ARP entries. If the entry is not referred to and is not used by traffic before the time elapses, it is deleted. Otherwise, a request will be sent to verify the MAC address.

      Range: 60 - 86400 seconds (24 hours)

      Default: 60 seconds

To add a static ARP entry:

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**.

To delete a static ARP entry:

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**.

To flush all dynamic ARP entries:

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 - Gaia Clish

Description

Commands to configure the Address Resolution Protocol (ARP).

Syntax

- To show dynamic and static ARP entries:

```
show arp
      dynamic all
      static all
```

- To add a static ARP entry:

```
add arp static ipv4-address <IPv4 Address> macaddress <MAC Address>
```

- To delete dynamic and static ARP entries:

```
delete arp
      dynamic all
      static ipv4-address <IPv4 Address>
```

- To configure ARP parameters:

```
set arp table
      validity-timeout <Time in sec>
      cache-size <Number of ARP entries>
```

- To show ARP parameters:

```
show arp table
      validity-timeout
      cache-size
```

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

Parameters

Parameter	Description
`ipv4-address <IPv4 Address>`	Configures the IPv4 Address of the static ARP entry. • **Range:** Dotted-quad ([0-255].[0-255].[0-255].[0-255]). • **Default:** No default value
`macaddress <MAC Address>`	Configures the hardware address (six hexadecimal octets separated by colons) of the static ARP entry. • **Range:** 00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF • **Default:** No default value
`validity-timeout <Time in sec>`	Configures the time, in seconds, to keep resolved dynamic ARP entries in the ARP cache table. If the ARP entry is not referred to and is not used by traffic before the time elapses, it is deleted. Otherwise, Gaia sends an ARP Request to verify the MAC address. • **Range:** 60 - 86400 seconds (24 hours) • **Default:** 60 seconds
`cache-size <Number of ARP entries>`	Configures the maximal number of ARP entries in the ARP cache table. • **Range:** 1024 - 16384 • **Default:** 4096 **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.

DHCP Server

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

This is the general workflow for allocating DHCP parameters to hosts (for the details, see the next section):

Step	Description
1	To define a DHCP subnet on a Gaia interface: a) Enable DHCP Server on the Gaia network interface. b) Define the network IPv4 address of the subnet on the interface. c) Define an IPv4 address pool. 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 - Gaia Portal

To allocate DHCP parameters to hosts:

Step	Description
1	In the navigation tree, click **Network Management** > **DHCP Server**.
2	1. In the **DHCP Server Subnet Configuration** section, click **Add**. The **Add DHCP** window opens. 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: Define the DHCP offer and lease settings:
4A	In the **Network IP Address** field, enter the IPv4 address of the applicable interface's subnet. In the **Subnet mask** field, enter the subnet mask. Note - To do this automatically, click **Get from interface**, select the applicable interface and click **OK**.
4B	In the **Address Pool** section, click **Add** to define the range of IPv4 addresses that the server assigns to hosts. a) In the **Type** field, select **Include** or **Exclude**. This specifies whether to include or exclude this range of IPv4 addresses in the IP pool. b) In the **Status** field, select **Enable** of **Disable**. This enables or disables the DHCP Server for this subnet, or the DHCP Server process (depending on the context). c) In the **Start** field, enter the first IPv4 address of the range. d) In the **End** field, enter the last IPv4 address of the range. e) Click **OK**.
4C	In the **Lease Configuration** section, configure the DHCP lease settings: a) **Optional:** In the **Default lease** field, enter the default lease time (in seconds), for host IPv4 addresses. This applies only if DHCP clients do not request a unique lease time. The default is 43,200 seconds. b) **Optional:** In the **Maximum Lease** field, enter the maximal lease time (in seconds), for host IPv4 addresses. The default is 86,400 seconds.

Step	Description
5	**Optional:** On the **Routing & DNS** tab: Define routing and DNS parameters for DHCP clients: • In the **Default Gateway** field, enter the IPv4 address of the default gateway for the DHCP clients. • In the **Domain Name** field, enter the domain name for the DHCP clients (for example, `example.com`). • In the **Primary DNS Server** field, enter the IPv4 address of the Primary DNS server for the DHCP clients. • 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). • 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**.

The DHCP server on Gaia is now configured and enabled.

You can now configure your network hosts to get their network parameters from the DHCP server on Gaia.

To change DHCP parameters in a subnet:

Step	Description
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**.

To disable DHCP server on all interfaces:

Step	Description
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**.

To delete DHCP subnet:

Step	Description
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 deleting the last DHCP subnet, you must disable DHCP server on all interfaces.

Configuring a DHCP Server - Gaia Clish

Description

Configure the Gaia device as DHCP Server for your network hosts.

Syntax

- To add a DHCP Server subnet:

```
add dhcp server subnet <Subnet Entry>
      netmask <Mask>
      include-ip-pool start <First IPv4 Address> end <Last IPv4 Address>
      exclude-ip-pool start <First IPv4 Address> end <Last IPv4 Address>
```

- To configure a DHCP Server subnet:

```
set dhcp server subnet <Subnet Entry>
      enable
      disable
      include-ip-pool <First IPv4 Address-Last IPv4 Address> {enable | disable}
      exclude-ip-pool <First IPv4 Address-Last IPv4 Address> {enable | disable}
      default-lease <Lease in Seconds>
      max-lease <Maximal Lease in Seconds>
      default-gateway <Gateway IPv4 Address>
      domain <Domain Name for the DHCP Clients>
      dns <DNS Server IPv4 Address>
```

- To delete a DHCP Server subnet:

```
delete dhcp server subnet <Subnet Entry>
      include-ip-pool <First IPv4 Address-Last IPv4 Address>
      exclude-ip-pool <First IPv4 Address-Last IPv4 Address>
```

- To enable or disable the DHCP Server process:

```
set dhcp server {enable | disable}
```

- **To show DHCP Server configuration:**

```
show dhcp server
      all
      status
      subnet <Subnet Entry> ip-pools
      subnets
```

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

Parameters

Parameter	Description
`subnet` *<Subnet Entry>*	Specifies the IPv4 address of the DHCP subnet on an Ethernet interface of the Gaia device. Hosts behind the Gaia interface get IPv4 addresses from address pools in the subnet. For example: `192.0.2.0`
`netmask` *<Mask>*	Specifies the IPv4 subnet mask in CIDR notation. 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. 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. 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. 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. For example: `192.0.2.155-192.0.2.254`
`enable`	Enables the DHCP Server subnet, or the DHCP Server process (depending on the context).
`disable`	Disables the DHCP Server subnet, or the DHCP Server process (depending on the context).
`default-lease` *<Lease in Seconds>*	Specifies the default DHCP lease in seconds, for host IPv4 addresses. Applies only if DHCP clients do not request a unique lease time. If you do not enter a value, the default is 43,200 seconds.
`max-lease` *<Maximal Lease in Seconds>*	Specifies the maximal DHCP lease in seconds, for host IPv4 addresses. This is the longest lease available. If you do not enter a value, the configuration default is 86,400 seconds.
`default-gateway` *<Gateway IPv4 Address>*	Optional. Specifies the IPv4 address of the default gateway for the network hosts
`domain` *<Domain Name for the DHCP Clients>*	Optional. Specifies the domain name of the network hosts. For example: `example.com`

`dns` *<DNS Server IPv4 Address>*	Optional. Specifies the DNS servers that the network hosts will use to resolve hostnames. Optionally, specify a primary, secondary and tertiary server in the order of precedence. For example: `192.0.2.101, 192.0.2.102, 192.0.2.103`
`all`	Shows all DHCP Server's configuration settings.
`subnets`	Configures the DHCP Server subnet settings.
`subnet` *<Subnet Entry>* `ip-pools`	The IP addresses pools in the DHCP Server subnet, and their status: Enabled or Disabled.
`status`	The status of the DHCP Server process: Enabled or Disabled.

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>
```

Hosts and DNS

Host Name

You set the host name (system name) during initial configuration. You can change the name.

Configuring Host Name - Gaia Portal

To show the host name:

The host name appears in the header of the Gaia Portal.

To change the host name:

Step	Description
1	In the navigation tree, click **Network Management > Host and DNS**.
2	In the **System Name** section, enter: • **Host Name** - The network name of the Gaia device. • **Domain Name** - Optional. For example, `example.com`.

Configuring Host Name - Gaia Clish

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
```

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

Host Addresses

You should add host addresses for systems that will communicate frequently with the 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 - Gaia Portal

To add a static host entry:

Step	Description
1	In the navigation tree, click **Network Management > Hosts and DNS**.
2	In the **Hosts** section, click **Add**.
3	Enter: • **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 in a dash or a period. There is no default value. • **IPv4 address** • **IPv6 address**

To edit a static host entry:

Step	Description
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: • **Host Name** • **IPv4 address** • **IPv6 address**

To delete a static host entry:

Step	Description
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 - Gaia Clish

Description

Add, edit, delete and show the name and IP addresses for hosts that will communicate frequently with the system.

Syntax

- To add a host name and its IP address:

```
add host name <Name of Host>
      ipv4-address <IPv4 Address of Host>
      ipv6-address <IPv6 Address of Host>
```

- To edit the host name and its IP address:

```
set host name <Name of Host>
      ipv4-address <IPv4 Address of Host>
      ipv6-address <IPv6 Address of Host>
```

- To delete a host name and its IP address:

```
delete host name <Name of Host> {ipv4 | ipv6}
```

- To show the configured IP address for a specified host:

```
show host name<SPACE><TAB>
```

```
show host name <Name of Host> {ipv4 | ipv6}
```

- To show 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

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.

Domain Name Service (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.

Configuring DNS - Gaia Portal

To configure the DNS Servers:

Step	Description
1	In the navigation tree, click **Network Management > Hosts and DNS**.
2	In the **System Name** section: In the **Domain Name** field, enter the domain name (for example, `example.com`).
3	In the **DNS** section: a) In the **DNS Suffix** field, enter the domain name suffix. Gaia will add it at the end of all DNS searches, if they fail. By default, it must be the local domain name configured in the **Domain Name** field above. A valid domain name suffix is made up of subdomain strings separated by periods. Subdomain strings must begin with an alphabetic letter and can consist only of alphanumeric characters and hyphens. The domain name syntax is described in RFC 1035 (modified slightly in RFC 1123). **Note -** Domain names that are also valid numeric IP addresses, for example 10.19.76.100, although syntactically correct, are not permitted. Example: You configured the DNS Suffix `example.com` and try to ping a host `foo` (with the command `ping foo`). If Gaia cannot resolve `foo`, then Gaia tries to resolve `foo.example.com`. b) In the **Primary DNS Server** field, enter the IPv4 or IPv6 address of the Primary DNS server. 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). 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). e) Click **Apply**.

Configuring DNS - Gaia Clish

Description

Configure, show and delete the DNS servers and the DNS suffix for the Gaia computer.

Syntax

- To configure the DNS servers and the DNS suffix for the Gaia computer:

```
set dns
      primary <IPv4 or IPv6 Address>
      secondary <IPv4 or IPv6 Address>
      tertiary <IPv4 or IPv6 Address>
      suffix <Name for Local Domain>
```

- To show the DNS servers and the DNS suffix for the Gaia computer:

```
show dns
      primary
      secondary
      tertiary
      suffix
```

- To delete the DNS servers and the DNS suffix for the Gaia computer:

```
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

Parameter	Description
`primary` *<IPv4 or IPv6 Address>*	Specifies the IPv4 or IPv6 address of the primary DNS server, which resolve host names. 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. 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. This must be a host that runs a DNS server.

`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. A valid domain name suffix is made up of subdomain strings separated by periods. Subdomain strings must begin with an alphabetic letter and can contain only alphanumeric characters and hyphens. The domain name syntax is described in RFC 1035 (modified slightly in RFC 1123). **Note:** Domain names that are also valid numeric IP addresses, for example 10.19.76.100, although syntactically correct, are not permitted. For example, if you set the DNS Suffix to `example.com` and try to ping some host `foo` (by running `ping foo`), and foo cannot be resolved, then the resolving computer will try to resolve `foo.example.com`.

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 using the Gaia Portal, or the Gaia Clish `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, without sending 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 to configure the rank.

Configuring IPv4 Static Routes - Gaia Portal

You can configure IPv4 static routes one at a time, or many routes at once.

Configuring One IPv4 Static Route at a Time

Step	Description
1	In the navigation tree, click **Network Management > IPv4 Static Routes**.
2	In the **IPv4 Static Routes** section, click **Add**. 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: • **Normal** - To accept and forward packets • **Blackhole** - To drop packets, without sending ICMP *unreachable* packet to the traffic source • **Reject** - To drop packets, and send ICMP *unreachable* packet to the traffic source

Step	Description
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). 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. 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. This lets the cluster member accept static routes on the subnet of the Cluster Virtual IPv4 address. To make sure that the `scopelocal` attribute is set correctly, run the `cat /etc/routed.conf` command. For more information, see sk92799 http://supportcontent.checkpoint.com/solutions?id=sk92799.
8	In the **Comment** field, enter the applicable comment text (up to 100 characters).
9	Click **Add Gateway** and select one of these options: • Select **IP Address** to specify the next hop by its IPv4 address. In the **IPv4 Address** field, enter the IPv4 address of the next hop gateway. In the **Priority** field, either do not enter anything, or select an integer between 1 and 8. Click **OK**. • Select **Network Interface** to specify the next hop by the name of the local interface name that connects to it. In the **Local Interface** field, select an interface that connects to the next hop gateway. In the **Priority** field, either do not enter anything, or select an integer between 1 and 8. Click **Ok**. *Priority* defines which gateway to select as the next hop when multiple 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 using the same priority to specify a backup path with equal priority. Gateways with no priority configured are preferred over gateways with priority configured.
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`. The Ping feature sends ICMP Echo Requests to verify that the nexthop for a static route is working. Only nexthop gateways, which are verified as working are included in the kernel forwarding table. When Ping is enabled, an IPv4 static route is added to the kernel forwarding table only after at least one gateway is reachable.
11	Click **Save**.
12	In the **Advanced Options** section, you can adjust the Ping behavior. 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 configuring static routes using a logical interface option.

Step	Description
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**: • **Normal** - To accept and forward packets • **Blackhole** - To drop packets, without sending ICMP *unreachable* packet • **Reject** - To drop packets, and send ICMP *unreachable* packet

4	Add the routes in the text box, using this syntax:
	`<Destination IPv4 Address>/<Mask Length> <IPv4 Address of Next Hop Gateway> ["<Comment>"]`
	Where:
	• `<Destination IPv4 Address>/<Mask Length>` - Specifies the IPv4 address of destination host or network using the CIDR notation (IPv4_Address/MaskLength).
	Example: `192.168.2.0/24`
	You can use the `default` keyword instead of an IPv4 address when referring to the default route.
	• `<IPv4 Address of Next Hop Gateway>` - Specifies the IPv4 address of the next hop gateway
	• `"<Comment>"` - Optional. Free text comment for the static route.
	Write the text in double-quotes. Maximal length of the text string is 100 characters.
	Example:
	`default 192.0.2.100 192.0.2.1 "Default Route"`
	`192.0.2.200/24 192.0.2.18 "My Backup Route"`

5	Click **Apply**. The newly configured static routes show in the **IPv4 Static Routes** section. **Note** - The text box shows entries that contain errors with messages at the top of the page.
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 - Gaia Clish

Description

Configure, show and delete IPv4 static routes.

Note - There are no `add` commands for the static route feature.

Syntax

- To add or configure 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}
      gateway logical <Name of Local Interface> [priority <Priority>] {on | off}
      blackhole
      reject
      ping {on | off}
      rank <Rank>
      scopelocal {on | off}
```

- To add or configure a specific static IPv4 route:

```
set static-route <Destination IPv4 Address>
      comment {"Text" | off}
      nexthop
      gateway address <IPv4 Address of Next Hop Gateway> [priority <Priority>]
{on | off}
      gateway logical <Name of Local Interface> [priority <Priority>] {on | off}
      blackhole
      reject
      ping {on | off}
      rank <Rank>
      scopelocal {on | off}
```

- To show all configured static IPv4 routes:

```
show route static all
```

- To remove a default static IPv4 route:

```
set static-route default off
```

- To remove a specific static IPv4 route:

```
set static-route <Destination IPv4 Address> off
```

- To remove a specific path only, when multiple nexthops 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

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/MaskLength). Example: `192.168.2.0/24` 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. • Write the text in double-quotes. • Text must be up to 100 characters. • 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` *<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. Use this option only if the next hop gateway has an unnumbered interface.

Parameter	Description
`priority` *<Priority>*	Defines which gateway to select as the next hop when multiple 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 using the same priority to specify a backup path with equal priority. Gateways with no priority configured are preferred over gateways with priority configured.
`nexthop ... on`	Adds the specified next hop.
`nexthop ... off`	Deletes the specified next hop. If you specify a next hop, only the specified path is deleted. If no next hop is specified, the route and all related paths are deleted.
`ping {on | off}`	Enables (`on`) or disables (`off`) the ping of specified next hop gateways for IPv4 static routes. The Ping feature sends ICMP Echo Requests to verify that the nexthop for a static route is working. Only nexthop gateways, which are verified as working are included in the kernel forwarding table. When Ping is enabled, an IPv4 static route is added to the kernel forwarding table only after at least one gateway is reachable. To adjust the ping behavior, run: `set ping count` *<value>* `set ping interval` *<value>*
`rank` *<Rank>*	Selects a route, if there are many routes to a destination that use different routing protocols. The route with the lowest rank value is selected. Use the `rank` keyword in place of the `nexthop` keyword with no other parameters. Accepted values are: `default` (60), integer numbers from 0 to 255. In addition, see this command: `set protocol-rank protocol` *<Rank>*

Parameter	Description
`scopelocal {on | off}`	Defines a static route with a link-local scope. 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. This lets the cluster member accept static routes on the subnet of the Cluster Virtual IPv4 address. To make sure that the `scopelocal` attribute is set correctly, run the `cat /etc/routed.conf` command. For more information, see sk92799 http://supportcontent.checkpoint.com/solutions?id=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
```

IPv6 Static Routes

Configuring IPv6 Static Routes - Gaia Portal

You can configure IPv6 static routes only one route at a time.

Important - First, you must enable the IPv6 Support (on page 188) and reboot.

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:
   - **Normal** - To accept and forward packets
   - **Blackhole** - To drop packets, without sending ICMP *unreachable* packet to the traffic source
   - **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).

   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).
7. In the **Add Gateway** section, click **Add**.

   The **Add Gateway** window opens.
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.

   Priority defines the order for selecting the next hop among many gateways. The lower the priority, the higher the preference - priority 1 means the highest preference, and priority 8 means the lowest preference. Gateways with no priority configured are preferred over gateways with priority configured. Two gateways cannot be configured 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`.

    The Ping6 feature sends ICMPv6 Echo Requests to verify that the nexthop for a static route is working. Only nexthop gateways, which are verified as working are included in the kernel forwarding table. When Ping6 is enabled, an IPv6 static route is added to the kernel forwarding table only after at least one gateway is reachable.
12. Click **Save**.
13. In the **Advanced Options** section, you can adjust the Ping6 behavior. If you changed the default settings, click **Apply**.

Note - Make sure to enable the IPv6 feature. See the *System Configuration* (on page 188).

Configuring IPv6 Static Routes - Gaia Clish

Description

Configure, show and delete IPv6 static routes.

Important - First, you must enable the IPv6 Support (on page 188) and reboot.

Note - There are no `add` commands for the static route feature.

Syntax

- **To add or configure a default static IPv6 route:**

```
set ipv6 static-route default
      comment {"Text" | off}
      nexthop
      gateway <IPv6 Address of Next Hop Gateway> [priority <Priority>] {on |
off}
      gateway <IPv6 Address of Next Hop Gateway> interface <Name of Local
Interface> [priority <Priority>] {on | off}
      blackhole
      reject
      ping6 {on | off}
      rank <Rank>
```

- To add or configure a specific static IPv6 route:

```
set ipv6 static-route <Destination IPv6 Address>
      comment {"Text" | off}
      nexthop
      gateway <IPv6 Address of Next Hop Gateway> [priority <Priority>] {on |
off}
      gateway <IPv6 Address of Next Hop Gateway> interface <Name of Local
Interface> [priority <Priority>] {on | off}
      blackhole
      reject
      ping6 {on | off}
      rank <Rank>
```

- To show all configured static IPv6 routes:

```
show ipv6 route static all
```

- **To remove a default static IPv6 route:**

```
set ipv6 static-route default off
```

- To remove a specific static IPv6 route:

```
set ipv6 static-route <Destination IPv6 Address> off
```

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

Parameters

Parameter	Description
`default`	Defines the default static IPv6 route.

Parameter	Description
<Destination IPv6 Address>	Defines the IPv6 address of destination host or network using the CIDR notation (IPv6_Address/MaskLength). Example: `fc00::/64` Mask length must be in the range 8-128.
`comment {"`*Text*`" | off}`	Defines of removes the optional comment for the static route. • Write the text in double-quotes. • Text must be up to 100 characters. • 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. Use this option only if the next hop gateway has an unnumbered interface.
`priority` *<Priority>*	Defines which gateway to select as the next hop when multiple gateways are configured. The lower the priority, the higher the preference - priority 1 means the highest preference, and priority 8 means the lowest preference. Gateways with no priority configured are preferred over gateways with priority configured. Two gateways cannot be configured with the same priority because IPv6 Equal Cost Multipath Routes are not supported.

Parameter	Description
`nexthop ... on`	Adds the specified next hop.
`nexthop ... off`	Deletes the specified next hop. If you specify a next hop, only the specified path is deleted. If no next hop is specified, the route and all related paths are deleted.

`ping6 {on | off}`	Enables (`on`) or disables (`off`) the ping of specified next hop gateways for IPv6 static routes.
	The Ping6 feature sends ICMPv6 Echo Requests to verify that the nexthop for a static route is working. Only nexthop gateways, which are verified as working are included in the kernel forwarding table.
	When Ping6 is enabled, an IPv6 static route is added to the kernel forwarding table only after at least one gateway is reachable.
	To adjust the ping6 behavior, run:
	`set ping count <value>`
	`set ping interval <value>`

`rank <Rank>`	Selects a route, if there are many routes to a destination that use different routing protocols. The route with the lowest rank value is selected. Use the `rank` keyword in place of the `nexthop` keyword with no other parameters. Accepted values are: `default` (60), integer numbers from 0 to 255. In addition, see this command: `set protocol-rank protocol <Rank>`

Examples

```
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

Symptoms

You cannot enable the VPN Software Blade. This message shows:

`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.

Solution

1. In SmartConsole, open the Security Gateway object.
2. Click the **General Properties** page.
3. Configure the main IPv6 address.
4. Click **OK**.
5. Install the Access Policy on the Security Gateway object.

Configuring IPv6 Neighbor-Entry - Gaia Clish

Description

Adds and delete entries in the Gaia IPv6 Neighbor table.

Important - First, you must enable the IPv6 Support (on page 188) and reboot.

Note - You can add or delete Neighbor entries only from the Gaia Clish.

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
<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

NetFlow is an industry standard for traffic monitoring. It is a network protocol developed by Cisco for collecting network traffic patterns and volume. It lets one host (the *Exporter*) send information about network flows to another host (the *Collector)*. A network flow is a unidirectional stream of packets that share a set of characteristics.

You can configure Gaia as an Exporter of NetFlow records for all the traffic that is inspected by SecureXL. This includes Accelerated and Medium Path traffic, F2F traffic, and traffic dropped by Drop Templates.

For more information, see sk102041: NetFlow support by Gaia OS http://supportcontent.checkpoint.com/solutions?id=sk102041.

The Collector is supplied by a different vendor, and is configured separately.

NetFlow Export configuration is a list of collectors, to which the service sends records.

- To enable NetFlow, configure at least one collector.
- To disable NetFlow, make sure no collectors are configured.

You can configure up to three collectors. NetFlow records go to all configured collectors. If you configure three collectors, each record is sent three times.

Notes:

- The IP addresses and TCP/UDP ports reported by NetFlow are the ones, on which it expects to receive traffic. Therefore, for NATed connections, one of the two directions of flow is reported with the NATed address.
- If SecureXL is not enabled or not working, NetFlow packets are not sent.
- NetFlow sends the connection records after the connections have terminated. If the system is idle or the connections are long lasting, you may have to wait to see NetFlow packets.

Flow Records

You can configure Gaia operating system to export flow records using NetFlow versions 5 or 9 (RFC 3954). Regardless of which export format you choose, Gaia operating system exports values for the following 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).

Configuring Netflow Export - Gaia Portal

To configure NetFlow export:

1. In the navigation tree, click **Network Management** > **NetFlow Export**.
2. Click **Add**.
3. Enter the required data for each collector:

Parameter	Description
IP address	The IPv4 address, to which NetFlow packets are sent. This is mandatory.
UDP port Number	The UDP port number, on which the collector is listening. This is mandatory. There is no default or standard port number for NetFlow.
Export format	The NetFlow protocol version to send: **5** or **9**. Each has a different packet format. The default is **9**.
Source IP address	**Optional:** The IPv4 address of the NetFlow packets source. This must be an IPv4 address of the local host. The default (which is recommended) is an IPv4 address from the network interface, on which the NetFlow traffic is going out.

Configuring Netflow Export - Gaia Clish

Description

Configure Netflow.

Syntax

- To add a 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
```

- To change settings of a Netflow collector:

```
set netflow collector for-ip <IPv4 Address of Collector>
      ip <IPv4 Address of Collector>
      port <Destination Port on Collector>
      srcaddr <Source IPv4 Address> export-format {Netflow_V5 | Netflow_V9 | IPFIX}
      export-format {Netflow_V5 | Netflow_V9 | IPFIX}
      enable
      disable
```

- To show a Netflow collector:

```
show netflow collector
```

```
show netflow collector<SPACE><TAB>
```

```
show netflow all
```

- To delete a Netflow collector:

```
delete netflow collector for-ip <IPv4 Address of Collector> [for-port <Destination Port on Collector>]
```

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

Parameters

Parameter	Description
`ip` *<IPv4 Address of Collector>*	Specifies the IPv4 address of the NetFlow Collector, to which NetFlow packets are sent. This is mandatory.
`port` *<Destination Port on Collector>*	Specifies the UDP port number on the NetFlow Collector, on which the collector is listening. This is mandatory. There is no default or standard port number for NetFlow.
`srcaddr` *<Source IPv4 Address>*	**Optional:** Specifies the IPv4 address of the NetFlow packets source. This must be an IPv4 address that belongs to one of the local interfaces of the local host. The default (which is recommended) is an IPv4 address that belongs to the network interface that connects to the NetFlow Collector.

Parameter	Description
`export-format {Netflow_V5 | Netflow_V9 | IPFIX}`	The NetFlow protocol version to send: NetFlow v5, NetFlow v9, or IPFIX (known as "NetFlow v10"). Each has a different packet format. The default is NetFlow v9.
`for-ip` *<IPv4 Address of Collector>* `for-port` *<Destination Port on Collector>*	These parameters specify the configured NetFlow Collector. If you only have one collector configured, you do not need these parameters. If you have two or three collectors with different IP addresses, use `for-ip`. If you have two or three collectors with the same IP address and different UDP ports, you must use `for-ip` and `for-port` to identify the one you want to work on.

Monitoring NetFlow Configuration

To see NetFlow configuration:

`show netflow all`

`show netflow collector for-ip <IPv4 Address of Collector> [for-port <Destination Port on Collector>]`
`export-format`
`srcaddr`

`show netflow collector for-ip <IPv4 Address of Collector>] port`
`show netflow collector ip`

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 *R80.10 Gaia Advanced Routing Administration Guid*e http://downloads.checkpoint.com/dc/download.htm?ID=54803.

System Management

In This Section:

Time 142
Cloning Groups 148
SNMP 158
Job Scheduler 173
Mail Notification 177
Messages 179
Display Format 182
Session 184
Core Dumps 185
System Configuration 188
System Logging 190
Network Access 199
Certificate Authority 200
Host Access 201

This chapter includes procedures and reference information for system management tasks.

Time

All Security Gateways, Security Management Servers 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, using the Gaia Portal, or the Gaia Clish.

Network Time Protocol (NTP)

Network Time Protocol (NTP) is an Internet standard protocol used to synchronize the clocks of computers in a network to the millisecond.

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.

Setting the Time and Date - Gaia Portal

To set time and date automatically using NTP:

Step	Description
1	In the navigation tree, click **System Management** > **Time**.
2	Click **Set Time and Date**.
3	In the **Time and Date Settings** window, select **Set Time and Date automatically using Network Time Protocol (NTP)**.
4	Enter the Hostname or IP address of the primary and (optionally) secondary NTP servers.
5	Select the NTP version for the applicable server.
6	Click **OK**.

To set the system time and date:

Step	Description
1	In the navigation tree, click **System Management** > **Time**.
2	Click **Set Time and Date**.
3	Enter the time and date in the applicable fields.
4	Click **OK**.

To set the time zone:

Step	Description
1	In the navigation tree, click **System Management** > **Time**.
2	Click **Set Time Zone** and select the time zone from the list.
3	Click **OK**.

Configuring NTP - Gaia Clish

Description

Configure and show the Network Time Protocol (NTP).

Syntax

- To add a new NTP server:

```
set ntp
      active {on | off}
      server
      primary <IP address, or Hostname of NTP Server> version {1|2|3|4}
      secondary <IP address, or Hostname of NTP Server> version {1|2|3|4}
```

- To show NTP configuration:

```
show ntp
      active
      current
      servers
```

- To delete an NTP server:

```
delete ntp server <IP address, or Hostname of NTP Server>
```

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

Parameters

Parameter	Description
`active`	Shows the NTP status (enabled or disabled).
`current`	Shows the IP address or Host name of the NTP server Gaia uses right now.
`servers`	Shows the configured NTP servers.
`active {on | off}`	Enables (`on`) or disables (`off`) NTP.
`server`	Keyword that identifies the NTP server - time server, from which Gaia synchronizes its clock. The specified time server does **not** synchronize to the local clock of Gaia.
`primary`	Configures the IP address or Host name of the primary NTP server.
`secondary`	Configures the IP address or Host name of the secondary NTP server.
`version {1|2|3|4}`	Configures the version number of the NTP - 1, 2, 3 or 4. **Best Practice -** Check Point recommends that you run NTP version 3.

Example

```
gaia> set ntp server primary pool.ntp.org version 3

gaia> set ntp active on

gaia> show ntp servers
IP Address                Type              Version
pool.ntp.org              Primary           3
```

Showing the Time & Date - Gaia Clish

Description

Show current system date and time.

Syntax

```
show clock
```

Parameters

Parameter	Description
`clock`	The current system day, date, and time. The current system time is in the HH:MM:SS format.

Example

```
gaia> show clock
Thu Oct 6 15:20:00 2011 IST
gaia>
```

Setting the Date - Gaia Clish

Description

Set and show the system date.

Syntax

- To configure a date:
```
set date <Date>
```
- To configure the configured date:
```
show date
```

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

Parameters

Parameter	Description
<*date*>	The date in the YYYY-MM-DD format.

Example

To configure the 10th of August 2017, run:

```
gaia> set date 2017-08-10
```

Setting the Time - Gaia Clish

Description

Set and show the system time.

Syntax

- To configure the time:
```
set time <Time of the Day>
```
- To show the current time:
```
show time
```

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

Parameters

Parameter	Description
<*Time of the Day*>	The current system time in HH:MM:SS format.

Setting the Time Zone - Gaia Clish

Description

Configure and show the system time zone.

Syntax

- **To configure the time zone:**
  ```
  set timezone <Area> / <Region>
  ```
  Note - The spaces before and after the slash character (/) are mandatory.
- To show the configured time zone:
  ```
  show timezone
  ```

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

Parameters

Parameter	Description
<*Area*>	Continent or geographic area. Valid values: Africa, America, Antarctica, Asia, Atlantic, Australia, Europe, Indian, Pacific
<*Region*>	Region within the specified area.

Examples

```
gaia> set timezone America / Detroit

gaia> set timezone Asia / Tokyo
```

Cloning Groups

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. A configuration change in one of the members is automatically propagated to other members. This is useful in ClusterXL. If the ClusterXL members are also members of a Cloning Group, static routes can be synchronized.

You can:

- Manually define an independent Cloning Group through the Gaia Portal. To do this, use **Manual mode**. In manual mode, the administrator creates the Cloning Group and separately adds each member.
- Configure a ClusterXL cluster as a Gaia Cloning Group. To do this, use **ClusterXL mode**. All the ClusterXL members become members of the same Cloning Group.

  Note - A VRRP cluster has to be manually defined.

Important: Synchronization between members of a Cloning Group requires TCP Port 1129 to be open and communication through the port allowed by the firewall. When the Security Gateways are part of a cluster in SmartConsole, an implied rule in the rule base allows this connection. When the Security Gateways are not part of the same Cluster, the implied rule does not apply. If the Security Gateways are not part of the same cluster object in SmartConsole, make sure there is a rule that allows connections on TCP port 1129.

Configuring Cloning Groups - Gaia Portal

Cloning Groups are configured from the Security Gateway Portal.

To create a new Cloning Group:

1. In your web browser, connect to the Gaia Portal on a Security Gateway.
2. In **System Management > Cloning Group**, click **Start Cloning Group Creation Wizard**.

   The **Cloning Group Creation Wizard** opens.
3. Select **Create a new Cloning Group**.

   The **New Gaia Cloning Group** window opens.
   - Enter a name for the Cloning Group
   - Select an IP address for synchronizing settings between member Security Gateways. Select an address on a secure internal network.
   - Enter a password for the administration account (*cadmin*). This password is necessary to:
     - Manage the Cloning Group
     - Add other Security Gateways to the Cloning Group
     - Create encrypted traffic between members of the Cloning Group

4. In the **Shared Features** screen, select features to clone to other members of the group.

   Pay attention to the features you want to clone. For example, you might not want to clone static routes to Security Gateways that are members of a cluster.

   You can select any of these:

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.
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.
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.

Shared Feature	Description
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).
Route Redistribution	Configure advertisement of routing information from one protocol to another (supports IPv4 and IPv6).
Route Map	Configure dynamic routing route maps.
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.

5. Click **Next** for the **Wizard Summary** and then click **Finish**.

To manage the Cloning Group:

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.)
   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**.
   The shared features are propagated to all members of the group. 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.

A user that gets cloning group administration privileges (CloningGroupManagement RBA role), 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 Portal.

To manage a Cloning Group as an assigned administrator:

1. In your web browser, connect to the Gaia Portal on a Cloning Group member Security Gateway.
2. Click **Group Mode**.
   The Security Gateway switches to Cloning Group management mode.

To join a Cloning Group:

1. In your web browser, connect to the Gaia Portal on a Security Gateway.
2. In **System Management > Cloning Group**, click **Start Cloning Group Creation Wizard**.
   The **Cloning Group Wizard** opens.
3. Select **Join an existing Cloning Group**.
4. The **Join Existing Cloning Group** window opens.
   - Enter the IP address of a remote member of the Cloning Group.
   - Select an IP address for synchronizing the settings between Security Gateways. Select a secure internal address.
   - Enter the password of the Cloning Group administration account (*cadmin*). (The same password you entered when creating the group.) The *cadmin* password:
     - Lets you log in to the *cadmin* account
     - Is used to create authentication credentials for members during synchronization
5. Click **Next** for the **Wizard Summary** and then click **Finish**.

To create a Cloning Group that follows ClusterXL:

Select this option if the gateway is a member of a ClusterXL.

Note - If you select this option, you have to select it for all the members of the cluster.

1. In your web browser, connect to the Gaia Portal on a Security Gateway.
2. In **System Management > Cloning Group**, click **Start Cloning Group Creation Wizard**.
   The **Cloning Group Creation Wizard** opens.
3. Select **Cloning Group follows ClusterXL**.
   - Enter the Cloning Group name.
   - Enter a password for the Cloning Group administration account (*cadmin*).
4. Click **Next** for the **Wizard Summary** and then click **Finish**.
5. Repeat Steps 1-4 for all members of the cluster.

Configuring Cloning Groups - Gaia Clish

Cloning Groups can also be managed in Gaia Clish. When run from the *cadmin* account, these commands apply to all members of the Gaia group.

You can create Cloning Groups in manual, or in ClusterXL mode.

To create the first Cloning Group member in Manual mode:

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

To add other Security Gateways to the Cloning Group in Manual mode:

On each of those Security Gateways:

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

To create Cloning Group members in ClusterXL mode:

On all member Security Gateways:

1. Set the cloning group mode to `ClusterXL`
2. Set the cloning group password
3. Set the cloning group state to `on`

To create a Cloning Group:

```
set cloning-group
      local-ip <IPv4_address>
      mode {manual | cluster-xl}
      name <Cloning Group name>
      password <Password>
      state {on | off}
```

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` <*Cloning Group name*>	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}`	Turns the Cloning Group feature on or off. If you select `off`, the Security Gateway is removed from the Cloning Group.

To add Shared Features:

```
add cloning-group shared-feature <Feature>
```

Parameter	Description
<*feature*>	The name of the feature to be synchronized between the members of the Cloning Group.

Where:

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.

Name of Shared Feature	Description
`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).
`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.
`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.
`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.

Name of Shared Feature	Description
`pim`	Configure Protocol-Independent Multicast.
`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.
`static-mroute`	Configure static multicast routes.
`snmp`	Configure SNMP.
`backup`	Configure Gaia scheduled backups.

To delete Shared Features:

```
delete cloning-group shared-feature <Feature>
```

Parameter	Description
<*feature*>	The name of the feature to be deleted from the list of shared features. To see the list of the enabled Shared Features, enter: `delete cloning-group shared-feature`<SPACE><TAB>

To join a Cloning Group:

```
join cloning-group remote-ip <Cloning Group IPv4 address>
```

Parameter	Description
<*Cloning Group IPv4 address*>	The IPv4 address of the Cloning Group member, to which you join. **Note** - This option is not available if you are logged into the *cadmin* account.

To remove a member from a Cloning Group:

```
leave cloning-group
```

To remove an inaccessible Cloning Group member:

```
delete cloning-group disconnected-member <IPv4 address of Member>
```

Parameter	Description
<*IPv4 address of Member*>	The IPv4 address of the Cloning Group member that became inaccessible.

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.

To view Cloning Group configuration:

```
show cloning-group
      local-ip
      members
      mode
      name
      shared-feature
      state
      status
```

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. **Note** - This option is not available if you are logged into the *cadmin* account.

To re-synchronize a Cloning Group:

```
re-synch cloning-group
```

When a user (local or remote) receives Cloning Group management privileges, he can turn the Cloning Group management mode on, to create, delete, and edit Cloning Groups.

To turn on the Cloning Group management mode:

```
set cloning-group-management {on | off}
```

Parameter	Description
on	Enables the Cloning Group management mode.
off	Disables the Cloning Group management mode.

SNMP

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.

To view detailed information about each MIB that the Check Point implementation supports (also, see sk90470 http://supportcontent.checkpoint.com/solutions?id=sk90470):

MIB	Location
Standard MIBs	`/usr/share/snmp/mibs/*.txt`
Check Point MIBs	`$CPDIR/lib/snmp/chkpnt.mib` `$CPDIR/lib/snmp/chkpnt-trap.mib`
Check Point Gaia trap MIB	`/etc/snmp/GaiaTrapsMIB.mib`

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 have been made to the first version to address security and other fixes. For more information, see Net-SNMP (http://www.net-snmp.org).



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.

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.

SNMP on Check Point platforms, 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.

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 on the basis of 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 system 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. It is also advised to select SNMPv3, rather than the default v1/v2/v3, if your management station supports it.

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.

You can choose to use all versions of SNMP (v1, v2, and v3) on your system, or to grant SNMPv3 access only. If your management station supports v3, select to use only v3 on your Gaia system. SNMPv3 limits community access. Only requests from users with enabled SNMPv3 access are allowed, and all other requests are rejected.

SNMP Agent Address

An 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:

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. This trap is 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. 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`	Notify if one of the voltage sensors exceeds its maximum value.
`lowVoltage`	Notify if one of the voltage sensors falls below its minimum value.

Type of Trap	Description
`raidVolumeState`	Notify if the raid volume state is not optimal. This trap works only if RAID is supported on the Gaia appliance or computer. To make sure that RAID monitoring is supported, run the command `raid_diagnostic` and confirm that it shows the RAID status.
`biosFailure`	Notify when the Primary BIOS failure is detected. Sent once the event occurs.
`vrrpv2AuthFailure`	Notify when the VRRP member has got packet Authentication failure - VRRPv2 (IPv4) and VRRPv3 (IPv6). Sent each polling interval.
`vrrpv2NewMaster`	Notify when the VRRP member has transitioned to Master state - VRRPv2 (IPv4). Sent each polling interval.
`vrrpv3NewMaster`	Notify when the VRRP member has transitioned to Master state - VRRPv3 (IPv6). Sent each polling interval.
`vrrpv3ProtoError`	Notify when the VRRP member has got Protocol error - VRRPv2 (IPv4) and VRRPv3 (IPv6). Sent each polling interval.

Configuring SNMP - Gaia Portal

For detailed information, see sk90860: How to configure SNMP on Gaia OS http://supportcontent.checkpoint.com/solutions?id=sk90860.

To enable SNMP:

Step	Description
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: • **1/v2/v3 (any)** Select this option if your SNMP management station does not support SNMPv3. • **v3-Only** Select this option if your SNMP management station supports v3. 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. The maximum length for the string is 128 characters. That includes letters, numbers, spaces, special characters 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. The maximum length for the string is 128 characters. That includes letters, numbers, spaces, special characters. For example: `John Doe, Network Administrator, (111) 222-3333`
6	Click **Apply**.

To set an SNMP Agent interface:

Step	Description
1	In the navigation tree, click **System Management** > **SNMP**. 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.

To configure the SNMP community strings:

Step	Description
1	In the **V1/V2 Settings** section, in **Read Only Community String**, set a string other than **public**. You must always use this is a basic security precaution.
2	Optional. Set a **Read-Write Community String**. **Warning -** Set a read-write community string only if you have reason to enable set operations, and if your network is secure.

To add a USM user:

Step	Description
1	In the navigation tree, click **System Management** > **SNMP**.
2	In the **V3 - User-Based Security Model (USM)** section, click **Add**. The **Add New USM User** window opens.
3	In the **User Name**, enter the desired user name that is between 1 and 31 alphanumeric characters with no spaces, backslash, or colon characters. This can be the same as a user name for system access.
4	In the **Security Level**, select one of these options from the drop-down list: • **authPriv** - The user has authentication and privacy pass phrases and can connect with privacy encryption. • **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: • **read-only** • **read-write**
6	In the **Authentication Protocol**, select one of these options from the drop-down list: • **MD5** • **SHA1** The default is **MD5**.
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: • **DES** • **AES** The default is **DES**.

Step	Description
9	In the **Privacy Pass Phrase**, enter a pass phrase that is between 8 and 128 characters in length. Used for protection against disclosure of SNMP message payloads.
10	Click **Save**. The new user shows in the table.

To delete a USM user:

Step	Description
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**. The **Deleting USM User Entry** window opens.
3	The window shows this message: **Are you sure you want to delete "username" entry?** Click **Yes**.

To edit a USM user:

Step	Description
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**. 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**.

To enable or disable SNMP trap types:

Step	Description
1	In the navigation tree, click **System Management** > **SNMP**.
2	In the **Enabled Traps** section, click **Set**. The **Add New Trap Receiver** window opens. • To enable a trap: Select from the **Disabled Traps** list, and click **Add>** • To disable a trap: Select from the **Enabled Traps** list, and click **Remove>**
3	Click **Save**.
4	Add a USM user. You must do this even if you use only SNMPv1 or SNMPv2. In the **Trap User**, select an SNMP user.

Step	Description
5	In **Polling Frequency**, specify the number of seconds between polls.
6	Click **Apply**.

To configure SNMP trap receivers:

Step	Description
1	In the navigation tree, click **System Management** > **SNMP**.
2	In the **Trap Receivers Settings** section, click **Add**. 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**.

To edit SNMP trap receivers:

Step	Description
1	In the navigation tree, click **System Management** > **SNMP**.
2	In the **Trap Receivers Settings** section, select the SNMP receiver and click **Edit**. The **Edit Trap Receiver** window opens.
3	You can change the SNMP version or the SNMP community string.
4	Click **Save**.

To delete SNMP trap receivers:

Step	Description
1	In the navigation tree, click **System Management** > **SNMP**.
2	In the **Trap Receivers Settings** section, select the SNMP trap receiver and click **Remove**. The **Deleting Trap Receiver Entry** window opens.
3	The window shows this message: **Are you sure you want to delete "IPv4 address" entry?** Click **Yes**.

Configuring SNMP - Gaia Clish

For detailed information, see sk90860: How to configure SNMP on Gaia OS http://supportcontent.checkpoint.com/solutions?id=sk90860.

Description

Configure SNMP.

Syntax for the **set** commands

```
set snmp agent {on | off}

set snmp agent-version {any | v3-Only}

set snmp mode {default | vs}

set snmp community <String> {read-only | read-write}

set snmp contact <Contact Information>

set snmp location <Location Information>

set 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}

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} authentication-protocol {MD5 | SHA1}

set snmp usm user <UserName> security-level authNoPriv auth-pass-phrase <Pass
Phrase> authentication-protocol {MD5 | SHA1}

set snmp usm user <UserName> security-level authNoPriv auth-pass-phrase-hashed
<Hashed Pass Phrase>

set snmp usm user <UserName> {usm-read-only | usm-read-write}

set snmp usm user <UserName> vsid {all | <IDs of allowed Virtual Devices>}

set snmp clear-trap interval <Value> retries <Value>

set snmp custom-trap <Custom Trap Name> <Property> <Value>

set snmp vs-direct-access {on | off}

set snmp traps coldStart-threshold <Seconds>

set snmp traps polling-frequency <Seconds>

set snmp traps receiver <IPv4 address> version {v1 | v2 | v3} community <String>

set snmp traps trap {authorizationError | biosFailure | coldStart |
configurationChange | configurationSave | fanFailure | highVoltage |
linkUpLinkDown | lowDiskSpace | lowVoltage | overTemperature |
powerSupplyFailure | raidVolumeState | vrrpv2AuthFailure | vrrpv2NewMaster |
vrrpv3NewMaster | vrrpv3ProtoError}

set snmp traps trap-user <UserName>
```

Where:

Command	Description
`set snmp agent {on | off}`	Enables (`on`) or disables (`off`) the SNMP Agent.
`set snmp agent-version {any | v3-Only}`	Configures the supported SNMP version: • `all` - support SNMP v1, v2 and v3 • `v3-Only` - support SNMP v3 only

`set snmp mode {default | vs}`	Configures how to run the SNMP daemon:
	• `default`
	  • On non-VSX Gateway, this is the only supported mode
	  • On VSX Gateway, SNMP daemon runs only in the context of VS0
	• `vs`
	  • For VSX Gateway only
	  • Each Virtual Device has a separate SNMP daemon running in the context of that Virtual Device

`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 location ...`	Configures the contact location for the SNMP community
`set snmp usm user <UserName> ...`	Configures the SNMPv3 USM user
`set snmp clear-trap ...`	Configures the indication of a custom SNMP trap termination
`set snmp custom-trap ...`	Configures the custom SNMP trap
`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 This mode works only when SNMP `vs` mode is enabled See the *R80.10 VSX Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=54764
`set snmp traps coldStart-threshold <Seconds>`	Configures the threshold for the SNMP `coldStart` trap

`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 ...`	Configures the Gaia built-in SNMP traps
`set snmp traps trap-user <UserName>`	Configures the user, which will generate the SNMP traps

Syntax for the **add** commands

```
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>
```

Where:

Command	Description
`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 custom-trap ...`	Adds a customer SNMP trap
`add snmp usm user ...`	Adds an SNMPv3 USM user

Syntax for the **delete** commands

```
delete snmp community <String>

delete snmp interface <Name of Interface>

delete snmp contact <Contact Information>

delete snmp location <Location Information>
```

```
delete snmp usm user <UserName>

delete snmp clear-trap

delete snmp traps coldStart-threshold

delete snmp traps polling-frequency

delete snmp traps receiver <IPv4 address>

delete snmp traps trap-user <UserName>

delete snmp custom-trap <Custom Trap Name>
```

Where:

Command	Description
`delete snmp community` <*String*>	Removes the SNMP community password
`delete snmp interface` <*Name of Interface*>	Removes the local interface from the list of local interfaces, on which the SNMP daemon listens
`delete snmp contact ...`	Removes the contact name for the SNMP community
`delete snmp location ...`	Removes the contact location for the SNMP community
`delete snmp usm user` <*UserName*>	Removes the SNMPv3 USM user
`delete snmp clear-trap`	Removes the indication of a custom SNMP trap termination
`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
`delete snmp traps trap-user` <*UserName*>	Removes the user, which will generate the SNMP traps
`delete snmp custom-trap` <*Custom Trap Name*>	Removes the custom SNMP trap

Best Practice

For commands that include `auth-pass-phrase`, `privacy-pass-phrase`, or both, use the hashed commands.
To get the hashed password, run: `show configuration snmp`

Interpreting Error Messages

This section lists and explains certain common error status values that can appear in SNMP messages. Within the 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.

The subsequent, or 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.

The next, or fifth field, is the variable-bindings field. It consists of a sequence of pairs; the first is the identifier. The second element is one of these options: `value`, `unSpecified`, `noSuchOjbect`, `noSuchInstance`, or `EndofMibView`.
This table describes each element.

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.

Variable-bindings element	Description
`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 a `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 use Gaia Portal to access cron and schedule regular jobs. You can configure the jobs to run at the dates and times that you specify, or at startup.

Configuring Job Scheduler - Gaia Portal

To schedule jobs:

Step	Description
1	In the navigation tree, click **System Management** > **Job Scheduler**.
2	Click **Add**. The **Add A New Scheduled Job** window opens.
3	In the **Job Name**, enter the name of the job. Use alphanumeric characters only, and no spaces.
4	In the **Command to Run**, enter the name of the command. The command must be a UNIX command. **Note -** If you wish to run a Check Point command, then use this syntax (see sk90441 http://supportcontent.checkpoint.com/solutions?id=sk90441): `source /etc/profile.d/CP.sh ; <command>`
5	Below the **Schedule**, select the frequency (**Daily**, **Weekly**, **Monthly**, **At startup**) for this job. Where applicable, enter the **Time** of day for the job, in the 24-hour clock format (HH:MM).
6	Click **OK**. The job shows in the **Scheduled Jobs** table.
7	In **E-mail Notification**, enter the e-mail address, to which Gaia should send the notifications. **Note -** You must also configure a Mail Server (on page 177).
8	Click **Apply**.

To delete scheduled jobs:

Step	Description
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, or **Cancel** to abort.

To edit the scheduled jobs:

Step	Description
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**. The **Edit Scheduled Job** opens.
4	Enter the changes.
5	Click **OK**.

Configuring Job Scheduler - Gaia Clish

Description

Use these commands to configure your system 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.

Syntax

- To add scheduled jobs:

```
add cron job <Job Name> command <Command> recurrence
      daily time <HH:MM>
      monthly month <1-12> days <1-31> time <HH:MM>
      weekly days <1-31> time <HH:MM>
      system-startup
```

- To change existing scheduled jobs:

```
set cron job <Job Name>
      command <Command>
      recurrence
      daily time <HH:MM>
      monthly month <1-12> days <1-31> time <HH:MM>
      weekly days <1-31> time <HH:MM>
      system-startup
set cron mailto <Email Address>
```

- To monitor configured scheduled jobs:

```
show cron
      job <Job Name>
      command
      recurrence
      jobs
      mailto
```

- To delete scheduled jobs:

```
delete cron
      all
      job <Job Name>
      mailto
```

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

Note - Only the `show` commands provide an output.

Parameters

Parameter	Description
<*Job Name*>	The name of the job that will be scheduled.
<*Command*>	The command that will be scheduled.
`recurrence daily time` <*HH:MM*>	Specifies that the job should run once a day - every day, at specified time. Enter the time of day in the 24-hour clock format - <Hours>:<Minutes>. Example: 14:35
`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. Months are specified by numbers from 1 to 12: January = 1, February = 2, ..., December = 12. Dates of month are specified by numbers from 1 to 31. To specify several consequent months, enter their numbers separate by commas. Example: for January through March, enter 1,2,3 To specify several consequent dates, enter their numbers separate by commas. Example: for 1st, 2nd and 3rd day of month, enter 1,2,3
`recurrence weekly days <1-31> time` <*HH:MM*>	Specifies that the job should run once a week - on specified days of week, and at specified time. Days of week are specified by numbers from 0 to 6: Sunday = 0, Monday = 1, Tuesday = 2, Wednesday = 3, Thursday = 4, Friday = 5, Saturday = 6. To specify several consequent days of a week, enter their numbers separate by commas. 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. Enter one email address for each command. You must also configure a mail server (on page 178).

Mail Notification

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 - Gaia Portal

Step	Description
1	In the navigation tree, click **System Management** > **Mail Notification**.
2	In The **Mail Server** field, enter the IP Address or Hostname of the mail server. For example: `mail.example.com`
3	In the **User Name** field, enter the user name. For example: `user@mail.example.com`
4	Click **Apply**.

Configuring Mail Notification - Gaia Clish

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 <IP 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` <*IP Address or Hostname*>	The IP address or Hostname of the mail server, to which Gaia sends mail notifications. Example: `mail.company.com`
`username` <*User Name*>	The username on the mail server that receives the `admin` or `monitor` mail notifications. 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

You can configure Gaia to show a *Banner Message* and a *Message of the Day* to users when they log in.

	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 - Gaia Portal

Step	Description
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.
5	Click **Apply**.

These limits apply:

Message type	Maximal supported total number of characters in the message	Maximal supported total number of lines in the message	Maximal supported number of characters in each line
Banner	1600	20	80
Message of the day	1200	20	400

Configuring Messages - Gaia Clish

Description

Set or show a banner message, or a message of the day.

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>
```

  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:

  a. 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.`"

  b. 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>
```

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>
```

- 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:

  a. 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.`"

  b. Disable the default message of the day:

```
set message motd off
```

These limits apply:

Message type	Maximal supported total number of characters in the message	Maximal supported total number of lines in the message	Maximal supported number of characters in each line
Banner	1600	20	80
Message of the day	1200	20	400

Display Format

Configuring Display Format - Gaia Portal

Step	Description
1	In the navigation tree, click **System Management** > **Display Format**.
2	In **Time**, select one of these options: • **12-hour** • **24-hour**
3	In **Date**, select one of these options: • **dd/mm/yyyy** • **mm/dd/yyyy** • **yyyy/mm/dd** • **dd-mmm-yyyy**
4	In **IPv4 netmask**, select one of these options: • **Dotted-decimal notation** • **CIDR notation**
5	Click **Apply**

Configuring Display Format - Gaia Clish

Description

Configure and show the display format for the current time.

Syntax

- To show the current time format:

```
show format time
```

```
show format all
```

- To configure the time format:

```
set format time
      12-hour
      24-hour
```

Description

Configure and show the display format for the current date.

Syntax

- 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
```

Description

Configure and show display format for the IPv4 netmask.

Syntax

- To show the current IPv4 netmask format:

```
show format netmask
```

```
show format all
```

- To configure the IPv4 netmask format:

```
set format netmask
      dotted
      length
```

Session

Manage inactivity timeout (in minutes) for the command line shell and for the Gaia Portal.

Configuring the Session - Gaia Portal

Step	Description
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.

Note - The maximal value is 720 minutes.

Configuring the Session - Gaia Clish

Description

Manage inactivity timeout (in minutes) for the Gaia Clish.

Syntax

- To configure the timeout:
  ```
  set inactivity-timeout <Timeout>
  ```
- To show the configured timeout:
  ```
  show inactivity-timeout
  ```

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

Parameters

Parameter	Description
<*Timeout*>	The inactivity timeout (in minutes) for the Gaia Clish. • **Range:** 1 - 720 minutes • **Default:** 10 minutes

Core Dumps

A Gaia core dump consists of 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 file in the `/var/log/dump/usermode` directory.

If the `/log` partition has less than 200 MB, no dumps are created, and all dumps are deleted to create space. This prevents core dumps filling the `/log` partition.

Configuring Core Dumps - Gaia Portal

To configure core dumps, enable the feature and then configure parameters.

To configure core dumps:

Step	Description
1	In the navigation tree, click **System Management** > **Core Dumps**.
2	Configure the parameters.
3	Click **Apply**.

Parameters

Parameter	Description
Total space limit	The maximum amount of disk space in MB that is used for storing core dumps. If disk space is required for a core dump, the oldest core dump is deleted. The per-process limit is enforced before the space limit. • **Range**: 1 - 99999 MB • **Default**: 1000 MB

Dumps per process	The maximum number of dumps that are stored for each process executable (program) file. A new core dump overwrites the oldest core dump. The per-process limit is enforced before the space limit. • **Range**: 1 - 99999 • **Default**: 2 Example: There are two programs "A" and "B", and the per-process limit is limit is 2. Program "A" terminates 1 time and program "B" terminates 3 times. The core dumps that remain are: • 1 core dump for program "A" • 2 core dumps for program "B" • Core dump 3 for program "B" is deleted because of the per-process limit.

Configuring Core Dumps - Gaia Clish

Description

Configure Gaia core dumps.

Syntax

- To enable or disable core dumps:
```
set core-dump {enable | disable}
```
- To set the total disk space usage limit in MB:
```
set core-dump total <0-99999>
```
- To set the number of core dumps per process:
```
set core-dump per_process <0-99999>
```
- To show the total disk space usage limit:
```
show core-dump total
```
- To show the number of core dumps per 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 amount of space that is used for core dumps. If space is required for a dump, the oldest dump is deleted. The per-process limit is enforced before the space limit. • **Range:** 1 - 99999 MB • **Default:** 1000 MB
`per_process <0-99999>`	The maximum number of core dumps that are stored for each process executable (program) file. A new core dump overwrites the oldest core dump. The per-process limit is enforced before the space limit. • **Range:** 1 - 99999 • **Default:** 2 Example: There are two programs "A" and "B", and the per-process limit is limit is 2. Program "A" terminates 1 time and program "B" terminates 3 times. The core dumps that remain are: • 1 core dump for program "A" • 2 core dumps for program "B" • Core dump 3 for program "B" is deleted because of the per-process limit.

System Configuration

Before you can configure IPv6 addresses and IPv6 static routes on a Gaia Security Management Server or Security Gateway, you must:

1. Enable IPv6 support for the Gaia OS.
2. On the Security Management Server, install and enable an IPv6 license.
3. Create IPv6 objects in SmartConsole.
4. Create IPv6 Firewall rules in SmartConsole.

Configuring IPv6 Support - Gaia Portal

Step	Description
1	In the navigation tree, click **System Management > System Configuration**.
2	In the **IPv6 Support** area, click **On**.
3	Click **Apply**.
4	Confirm, when prompted to reboot.

After the reboot, you can configure IPv6 addresses (on page 69) and IPv6 static routes (on page 131).

Configuring IPv6 Support - Gaia Clish

Description

Configure and show IPv6 support.

Syntax

- To configure IPv6 support:
```
set ipv6-state {on | off}
```
- To show the state of IPv6 support:
```
show ipv6-state
```

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

Parameters

Parameter	Description
on	Enables IPv6 support. This change requires reboot. After the reboot, you can configure IPv6 addresses (on page 69) and IPv6 static routes (on page 131).
off	Disables IPv6 support. This change requires reboot.

System Logging

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 - 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 some command options and parameters, which you cannot configure in the Gaia Portal.

To configure System Logging:

Step	Description
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** Specifies if the Gaia sends the Gaia system logs to a Check Point Management Server. **Default:** Not selected Note - This option is configured in the Gaia Clish with the `set syslog cplogs {on | off}` command. • **Send audit logs to management server upon successful configuration** Specifies if the Gaia sends the Gaia audit logs (for configuration changes that authorized users make) to a Check Point Management Server. **Default:** Selected Note - This option is configured in the Gaia Clish with the `set syslog mgmtauditlogs {on | off}` command.

Step	Description
	• **Send audit logs to syslog upon successful configuration** Specifies if the Gaia saves the logs for configuration changes that authorized users make. **Default:** Selected To specify a desired Gaia configuration audit log file, run the `set syslog filename </Path/File>` command (otherwise, Gaia uses the default `/var/log/messages` file). Note - This option is configured in the Gaia Clish with the `set syslog auditlog {disable | permanent}` command.
3	Click **Apply**.

To configure Remote System Logging:

Step	Description
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. These are the accepted values (as defined by the RFC 5424 - Section-6.2.1): • **All** - All messages • **Debug** - Debug-level messages • **Info** - Informational messages • **Notice** - Normal but significant condition • **Warning** - Warning conditions • **Error** - Error conditions • **Critical** - Critical conditions • **Alert** - Action must be taken immediately • **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.

To edit Remote System Logging settings:

Step	Description
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**.

To delete Remote System Logging settings:

Step	Description
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**.

Configuring System Logging - Gaia Clish

Description

Configure the 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 server, to which Gaia sends its syslog messages.

Note - There are some command options and parameters, which you cannot configure in the Gaia Portal.

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
```

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

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>]
```

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

Parameters

Parameter	Description
`cplogs {on | off}`	Specifies if the Gaia sends the Gaia system logs to a Check Point Management Server: • `on` - Send Gaia system syslogs • `off` - Do not send Gaia syslogs **Default:** `off` **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: • `on` - Send Gaia audit logs • `off` - Do not send Gaia audit logs **Default:** on **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: • `disable` - Disables the Gaia audit log facility • `permanent` - Enables the Gaia audit log facility to save information about all successful changes in the Gaia configuration. To specify a desired destination file, run the `set syslog filename </Path/File>` command (otherwise, Gaia uses the default `/var/log/messages` file). **Default:** `permanent` **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. **Default:** `/var/log/messages` **Note -** 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. **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. **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. • **Range:** Dotted-quad ([0-255].[0-255].[0-255].[0-255]) • **Default:** No default value
<Severity>	Syslog severity level for the system logging. These are the accepted values (as defined by the RFC 5424 - Section-6.2.1): • `emerg` - System is unusable • `alert` - Action must be taken immediately • `crit` - Critical conditions • `err` - Error conditions • `warning` - Warning conditions • `notice` - Normal but significant condition • `info` - Informational messages • `debug` - Debug-level messages • `all` - All messages Notes: • Until you configure at least one severity level for a given remote server, Gaia does not send syslog messages. • 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>
```

Configuring Log Volume - Expert Mode

On condition that there is enough available disk space, you can enlarge the log partition.

Use the **lvm_manager** tool from Expert mode:

Step	Description
1	Connect to the Gaia system over console.
2	Reboot the Gaia system.
3	During boot, press any key to enter the **Boot menu**. 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 http://supportcontent.checkpoint.com/solutions?id=sk95566: `[Expert@HostName:0]# lvm_manager`

Note - Disk space is added to the log volume by subtracting it from the disk space used to store backup images.

Redirecting RouteD System Logging Messages

By default, Gaia writes the RouteD syslog messages (for example, OSPF or BGP errors) to the `/var/log/messages` file. You can configure Gaia to write the RouteD syslog messages to the `/var/log/routed_messages` file instead.

To configure the redirection in the Gaia Portal:

Step	Description
1	In the 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. The default is 1 MB.
4	In the **Maximum Number of Files** field, enter the maximal number of log files to keep. The default is 10 log files (`/var/log/routed_messages`, `/var/log/routed_messages.0`, `/var/log/routed_messages.1`, ..., `/var/log/routed_messages.9`).
5	Click **Apply**.

To configure the redirection in the Gaia Clish

Step	Description
1	Connect to the command line on Gaia.
2	Log in to Gaia Clish.

3	Run these commands:
	`HostName> set routedsyslog on`
	`HostName> set routedsyslog size <Number of MB between 1 and 2047>`
	`HostName> set routedsyslog maxnum <Number of Files between 1 and 4294967295>`
	`HostName> save config`

For more information, see sk116436
http://supportcontent.checkpoint.com/solutions?id=sk116436.

Network Access

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. However, you can allow Telnet access.

Configuring Telnet Access - Gaia Portal

Step	Description
1	In the navigation tree, click **System Management > Network Access**.
2	Select **Enable Telnet**.
3	Click **Apply**.

Configuring Telnet Access - Gaia Clish

Description

Configure and show the network access using Telnet to the Gaia computer.

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.

Certificate Authority

If this machine is configured as Security Management Server, it runs Check Point Internal Certificate Authority.

You can reset the Internal Certificate Authority.

Note - Resetting the Internal Certificate Authority requires reissuing all internal certificates in SmartConsole for VPN, users and portals.

Resetting the Certificate Authority - Gaia Portal

1. In the navigation tree, click **System Management > Certificate Authority**.
2. Click **Reset**.

Changing the Name of the Internal Certificate Authority - Expert Mode

Note - You must run these commands from Expert mode.

Procedure 1

1. Connect to the command line on Gaia.
2. Log in to Expert mode.
3. Run:
   ```
   cp_conf ca fqdn <New Name for ICA>
   ```
4. Follow the instructions on the screen.

Procedure 2

1. Connect to the command line on Gaia.
2. Log in to Expert mode.
3. Run:
   ```
   cpconfig
   ```
4. Select the option **Certificate Authority**.

   This output shows:
   ```
   Configuring Certificate Authority...
   ====================================
   The Internal CA is initialized with the following name: XXX

   Do you want to change it (y/n) [n] ?
   ```
5. Enter **y**

   This output shows:
   ```
   Please enter the name of this Internal CA:
   ```
6. Enter the new name for Internal CA.
7. Follow the instructions on the screen.

Host Access

The Allowed-Clients feature lets you specify hosts or networks that are allowed to connect to the Gaia Portal or Gaia Clish on the Gaia device.

Configuring Allowed Gaia Clients - Gaia Portal

Step	Description
1	In the navigation tree, click **System Management > Host Access**.
2	Click **Add**. The **Add a New Allowed Client** window opens.
3	Select one of these options: • **Any host** - All remote hosts can access the Gaia Portal, or Gaia Clish. • **Host** - Enter the IP address of one host. • **Network** - Enter the IP address of a network and subnet mask.
4	Click **OK**.

Configuring Allowed Gaia Clients - Gaia Clish

Description

Configure allowed clients for remote access to the Gaia Portal, or Gaia Clish.

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
```

User Management

In This Section:

Change My Password 203
Users 205
Roles 213
Password Policy 237
Authentication Servers 250
System Groups 267
GUI Clients 271

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.

Change My Password

A Gaia user can change their Gaia password.

Changing My Password - Gaia Portal

Step	Description
1	In the navigation tree, click **User Management** > **Change My 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 My Password - Gaia Clish

Description

Change your own Gaia 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.

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:

- **admin -** Has full read/write capabilities for all Gaia features, from the Gaia Portal and the Gaia Clish. 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. 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 by default. You must assign one or more roles before they 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 the *Role-Based Administration* (on page 213).



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 - Gaia Portal

To see a 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.

To add a new user:

1. In the navigation tree, click **User Management > Users**.
2. Click **Add**.
3. In the **Login Name** field, enter the username.
   The valid characters (between 1 and 32 characters) are alphanumeric characters, dash (-), and underscore (_).
4. In the **Password** field, enter the the user's password.
   All printable characters are allowed. Length is between 6 and 128 characters.
   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 the user's password again.
6. In the **Real Name** field, enter the user's real name or other informative text.
   This is an alphanumeric string that can contain spaces. The default is the user's Login Name with capitalized first letter.
7. In the **Home Directory** field, enter the user's home directory.
   This is the full Linux path name of a directory, to which the user will log in.
   Must be a subdirectory of `/home/` directory.
   If the subdirectory does not already exist, it is created.
8. In the **Shell** field, select the user's default login shell:

Shell	Description
`/etc/cli.sh`	This is the default option. Lets the user work with the full Gaia Clish. By default, some basic networking commands (such as `ping`) are also available. The *Extended Commands* (on page 213) in the assigned roles makes it possible to add more Linux commands that can be used. User can run the `expert` command to enter the Bash shell (Expert mode).
`/bin/bash`	BASH Linux shell. Lets the user work with the Expert mode. User can run the `clish` command to enter the Gaia Clish.
`/bin/csh`	CSH Linux shell. User can run the `clish` command to enter the Gaia Clish.

Shell	Description
`/bin/p1shell`	Check Point shell for Multi-Domain Server. Lets the administrator user run Multi-Domain Security Management CLI commands in the context of Multi-Domain Server and Domains, without root permissions. For more information, see the *R80.10 Multi-Domain Security Management Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=54841.
`/bin/sh`	SH Linux shell. User can run the `clish` command to enter the Gaia Clish.
`/bin/tcsh`	TCSH Linux shell. User can run the `clish` command to enter the Gaia Clish.
`/usr/bin/scponly`	User is not allowed to log in to Gaia. User can only connect to Gaia over SCP and transfer files to and from the system. No other commands are permitted.
`/sbin/nologin`	User is not allowed to log in to Gaia.

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.

   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:
    - **0** for administrator users (this is the default option)
    - between **103** and **65533** for non-administrator users
11. In the **Access Mechanisms** section:
    - Select **Web** to allow this user to access Gaia Portal.
    - Select **Clish Access** to allow this user to access Gaia Clish.
12. In the **Available Roles** list:
    a) Select the roles you wish to assign to this user.

       To select several roles:

       Press and hold the **Ctrl** key on the keyboard.

       Left-click the applicable roles. The selected roles become highlighted.

    b) Click **Add >**. The selected roles move to the **Assigned Roles** list.
13. Click **OK**.

To change a user:

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.
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.

To delete a user:

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 - Gaia Clish

Description

Manage user accounts. You can add users, edit the home directory of the user, edit the default shell for a user, give a password to a user, and give privileges to users.

Note - You can use the `add user` command to add new users, but you must use the `set user` <*username*> `password` command to set the password and allow the user to log on to the system.

Syntax

- To add a local user account:
```
add user <UserName> uid <User ID> homedir <Path>
```
- To add a RADIUS user account:
```
add user <UserName> uid 0 homedir <Path>
```
- To modify 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>}
```
- To show summary information about all users:
```
show users
```
- To shows information about a specific user:
```
show user <UserName>
      [force-password-change]
      [gid]
      [homedir]
      [lock-out]
      [realname]
      [shell>]
      [uid]
```
- To delete a configured user:
```
delete user <User ID>
```

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

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.
`uid <User ID>`	Optional. Configures unique User ID to identify permissions of the user: • `0` for administrator users (this is the default option) • between `103` and `65533` for non-administrator users If a value is not specified, a sequential number is assigned automatically.
`homedir <Path>`	Configures user's home directory. This is the full Linux path name of a directory, to which the user will log in. Must be a subdirectory of `/home/` directory. If the subdirectory does not already exist, it is created.
`force-password-change {yes | no}`	If you wish to force the user to change the configured password during the next login, set the value to `yes`. **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. The default is `100`. You can add the user to several groups. Use the `add group` and `set group` commands to manage the groups.
`lock-out off`	Unlocks the user, if the user was locked-out. The password expiration date is adjusted, if necessary.
`newpass <Password>`	Configures a new password for the user. You will not be asked to verify the new password. 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. The command runs in interactive mode. You must enter the password twice, to verify it. The password you enter will not be visible on the terminal command line.

Parameter	Description
`password-hash` <*Password Hash*>	Configures the password using an encrypted representation of the password. The password is not visible as text on the terminal command line, or in the command history. Use this option if you want to change passwords using a script. You can generate the hash version of the password using standard Linux hash generating utilities.
`realname` <*Name*>	Configures user's description - most commonly user's real name. This is an alphanumeric string that can contain spaces. The default is the username with capitalized first letter.

Parameter	Description
`shell` <*Login Shell*>	Configures the user's default login shell. • `/etc/cli.sh`: This is the default option. Lets the user work with the full Gaia Clish. By default, some basic networking commands (such as `ping`) are also available. The *Extended Commands* (on page 213) in the assigned roles makes it possible to add more Linux commands that can be used. User can run the `expert` command to enter the Bash shell (Expert mode). • `/bin/bash`: BASH Linux shell. Lets the user work with the Expert mode. User can run the `clish` command to enter the Gaia Clish. • `/bin/csh`: CSH Linux shell. Gives the user Expert mode access. User can run the `clish` command to enter the Gaia Clish. • `/bin/p1shell`: Check Point shell for Multi-Domain Server. Lets the administrator user run Multi-Domain Security Management CLI commands in the context of Multi-Domain Server and Domains, without root permissions. For more information, see the *R80.10 Multi-Domain Security Management Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=54841 . • `/bin/sh`: SH Linux shell. Gives the user Expert mode access. User can run the `clish` command to enter the Gaia Clish. • `/bin/tcsh`: TCSH Linux shell. Gives the user Expert mode access. User can run the `clish` command to enter the Gaia Clish. • `/usr/bin/scponly`: User is not allowed to log in to Gaia. User can only connect to Gaia over SCP and transfer files to and from the system. No other commands are permitted. • `/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:

- **adminRole -** Gives the user read/write access to all features.
- **monitorRole -** Gives the user read-only access to all features.

You cannot delete or change the predefined roles.

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 Roles - Gaia Portal

Roles are defined in the **User Management > Roles** page of the Gaia Portal.

To see a list of existing roles, select **User Management > Roles** in the navigation tree.

To add new role:

Step	Description
1	In the navigation tree, click **User Management > Roles**.
2	Click **Add**.
3	In the **Role Name** field, enter the desired name. 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: 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**. **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. See the *List of available Features in roles* (on page 221).

Step	Description
5	On the **Extended Commands** tab: Select the commands you wish to configure in this role. • To select several commands: Press and hold the **Ctrl** key on the keyboard. Left-click the applicable commands (in the **Name**, **Description**, or **Path** column). The selected commands become highlighted. In the top right corner, select the option **Check selected as**. The checkboxes of the selected commands become checked. • To clear several selected commands: Press and hold the **Ctrl** key on the keyboard. Left-click the applicable commands (in the **Name**, **Description**, or **Path** column). The selected commands become highlighted. In the top right corner, clear the option **Check selected as**. The checkboxes of the selected commands become cleared. See the *List of available Extended Commands in roles* (on page 233).
6	Click **OK**.

To change features and commands in an existing role:

Step	Description
1	In the navigation tree, click **User Management > Roles**.
2	Select the role.
3	Click **Edit**.
4	On the **Features** tab: 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**. **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

Step	Description
5	On the **Extended Commands** tab: Select the commands you wish to configure in this role. • To select several commands: Press and hold the **Ctrl** key on the keyboard. Left-click the applicable commands (in the **Name**, **Description**, or **Path** column). The selected commands become highlighted. In the top right corner, select the option **Check selected as**. The checkboxes of the selected commands become checked. • To clear several selected commands: Press and hold the **Ctrl** key on the keyboard. Left-click the applicable commands (in the **Name**, **Description**, or **Path** column). The selected commands become highlighted. In the top right corner, clear the option **Check selected as**. The checkboxes of the selected commands become cleared.
6	Click **OK**.

To delete a role:

Step	Description
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 **adminRole**, or **monitorRole** default roles.

To assign users to a role:

Step	Description
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. To select several users: a) Press and hold the **Ctrl** key on the keyboard. b) Left-click the applicable commands. The selected users become highlighted.
5	Click **Add >**. The selected users move to the **Users with Role** list.
6	Click **OK**.

To remove users from a role:

Step	Description
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. To select several users: a) Press and hold the **Ctrl** key on the keyboard. b) Left-click the applicable commands. The selected users become highlighted.
5	Click **Remove >**. The selected users move to the **Available Users** list.
6	Click **OK**.

Note - You can assign a user to many roles from the **Users** page (on page 205).

Configuring Roles - Gaia Clish

Description

- Add, change, or delete roles.
- Add or remove users to or from existing roles.
- Add or remove access mechanism permissions for a specified user.

Syntax

- To add 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.

- To choose 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
```

- To assign Gaia access mechanisms to a user:

```
add rba user <User Name>
      access-mechanisms Web-UI
      access-mechanisms CLI
      access-mechanisms Web-UI,CLI
```

- To assign an RBA role to a user:

```
add rba user <User Name> roles <Role1,Role2,...,RoleN>
```

- To show RBA roles information:

```
show rba
      all
      role <Role Name>
      roles
      user <User Name>
      users
```

- To delete an entire RBA role:

```
delete rba role <Role Name>
```

- To delete 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.

- To remove Gaia access mechanisms from a user:

```
delete rba user <User Name>
      access-mechanisms Web-UI
      access-mechanisms CLI
      access-mechanisms Web-UI,CLI
```

- To remove 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 configures roles.
- You cannot delete the **adminRole**, or **monitorRole** default roles.

Parameters

Parameter	Description
`role` <*Role Name*>	Role name as a character string that contains letters, numbers or the underscore (_) character. 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: • `0` - Access only to VSX itself (VS0). • `all` - Access to all Virtual Systems. • `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. **Important -** This role is equivalent to admin role!
`readonly-features` <*List of RO Features*>	A comma-separated list of Gaia features that have read-only permissions in the specified role. See the *List of available features* (on page 221) and *List of available Extended Commands in roles* (on page 233). Notes: • Press <SPACE><TAB> to see the list of available features. • You can add read-only and read-write feature lists in the same `add rba role <Role Name> domain-type System ...` command.

`readwrite-features` <*List of RW Features*>	A comma-separated list of Gaia features that have read-write permissions in the specified role. See the *List of available features* (on page 221) and *List of available Extended Commands in roles* (on page 233). Notes: • Press <SPACE><TAB> to see the list of available features. • You can add read-only and read-write feature lists in the same `add rba role <Role Name> domain-type System ...` command. 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}`	Defines the access mechanisms that users can work with to manage Gaia: • `Web-UI` - Access only to Gaia Portal • `CLI` - Access only to Gaia Clish • `Web-UI,CLI` - Access to both Gaia Portal and Gaia Clish (spaces are not allowed in this syntax)

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

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 *`
			`set aaa tacacs-servers *`
			`delete aaa radius-servers *`
			`delete aaa tacacs-servers *`
			`add aaa radius-servers *`
			`add aaa tacacs-servers *`
			`show aaa radius-servers *`
			`show aaa tacacs-servers *`

Advanced VRRP	`adv-vrrp`	Configure the Advanced Virtual Router Redundancy Protocol (VRRP)	`set vrrp *` `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 *`
			`delete arp *`
			`set arp *`
			`show arp *`

Banner Messages	`message`	Control Banner Message and Message of the Day.	`set message *`
			`delete message *`
			`show message *`

BGP	`bgp`	Configure dynamic routing through the Border Gateway Protocol (BGP).	`set as *`
			`set router-id *`
			`set bgp *`
			`show route bgp *`
			`show as *`
			`show router-id *`
			`show bgp *`

Blades Summary	`blades`	Show summary for enabled Software Blades.	
Certificate Authority	`certificate_authority`	Control Certificate Authority.	
Change My Password	`selfpasswd`	Change your user account password.	`set selfpasswd *`

Cloning Group	`CloningGroup`	Control Gaia Cloning Groups.	`set cloning-group *`
			`add cloning-group *`
			`delete cloning-group *`
			`join cloning-group *`
			`re-synch cloning-group *`
			`leave cloning-group *`
			`show cloning-group *`

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 *`

Cluster	`cluster`	Control clustering.	`add cluster *`
			`set cluster *`
			`delete cluster *`
			`show cluster *`

Core Dump	`core-dump`	Control core dumps.	`set core-dump *` `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 *` `show bootp *`

DHCP Server	`dhcp`	Control DHCP Server on Gaia.	`set dhcp service *`
			`delete dhcp service *`
			`set dhcp client *`
			`delete dhcp client *`
			`add dhcp client *`
			`set dhcp server *`
			`delete dhcp server *`
			`add dhcp server *`
			`show dhcp service *`
			`show dhcp client *`
			`show dhcp server *`

DHCPv6 Relay	`dhcp6relay`	Control Relay of DHCPv6 messages between DHCP clients and DHCP servers on different IPv6 Network.	`set ipv6 dhcp6relay *` `show ipv6 dhcp6relay *`
Display Configuration	`configuration`	Save and show Gaia configuration.	`save configuration *` `show configuration *`
Display Format	`format`	Control how the system displays time, date and netmask.	`set format *` `show format *`

DNS	`dns`	Control DNS servers on Gaia.	`set dns *`
			`delete dns *`
			`show dns *`

Domain Name	`domainname`	Control the domain name on Gaia.	`set domainname *`
			`delete domainname`
			`show domainname`

Download SmartConsole	`smart-console`	Download SmartConsole from Gaia Portal.	

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
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 *`
			`delete command *`
			`show command *`
			`show commands`
			`show extended *`

Factory Defaults	`fcd`	Restore Gaia to Factory Defaults.	`set fcd *` `show fcd *`
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 *` `show lcd *`
Hardware Health	`hw-monitor`	Hardware sensor monitoring.	`show sysenv *`
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 *`
			`delete allowed-client *`
			`show allowed-client *`

Host Address	`host`	Control known hosts and their IP addresses on Gaia.	`add host *`
			`set host *`
			`delete host *`
			`show host *`

Host Name	`hostname`	Control the Gaia hostname.	`set hostname *` `show hostname *`

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 *` `show igmp *`
Inactivity timeout	`inactto`	Control inactivity timeout for Gaia Portal and Gaia Clish.	`set inactivity-timeout *` `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.	
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 *` `show iphelper *`
IPv4 Static Routes	`static-route`	Configure IPv4 static routes on Gaia.	`set static-route *` `show route static *`
IPv6 Router Discovery	`ipv6rdisc6`	Control IPv6 router discovery.	`set ipv6 rdisc6 *` `show ipv6 rdisc6 *`
IPv6 State	`ipv6-state`	Control IPv6 stack on Gaia.	`set ipv6-state *` `show ipv6-state`

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
IPv6 Static Routes	`static6`	Control IPv6 static routes on Gaia.	`set ipv6 static-route *` `show ipv6 route static *`
IPv6 VRRP	`vrrp6`	Control the IPv6 Virtual Router Redundancy Protocol (VRRPv3).	`set ipv6 vrrp6 *` `show ipv6 vrrp6 *`

Job Scheduler	`cron`	Control scheduled automated tasks that perform actions at a specific time.	`add cron *`
			`set cron *`
			`delete cron *`
			`show cron *`

License Activation	`license_activation`	Access to "Activate Licenses".	
License Configuration	`license`	Access to "Manage License".	
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 *` `show mail-notification *`
Maintenance	`maintenance-group`	Overview page for Maintenance.	
Management Interface	`management_interface`	Control which interface is used for Gaia management (main interface).	`set management *` `show management *`

NDP	`neighbor`	Control IPv6 Neighbour Discovery Protocol.	`add neighbor-entry *`
			`set neighbor *`
			`delete neighbor-entry *`
			`show neighbor *`

NetFlow Export	`netflow`	Control NetFlow Export on Gaia.	`add netflow *`
			`set netflow *`
			`delete netflow *`
			`show netflow *`

Network Access	`netaccess`	Control TELNET access to Gaia.	`set net-access *` `show net-access *`

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 *`
			`add interface *`
			`delete interface *`
			`add bonding *`
			`set bonding *`
			`delete bonding *`
			`add bridging *`
			`set bridging *`
			`delete bridging *`
			`add pppoe *`
			`delete pppoe *`
			`set pppoe *`
			`add gre *`
			`delete gre *`
			`show interface *`
			`show interfaces`
			`show bonding *`
			`show bridging *`
			`show pppoe *`
			`show gre *`

Network Management	`interface-group`	Overview page for Network Management.	

NTP	`ntp`	Control Network Time Protocol for synchronizing the Gaia clock.	`add ntp *`
			`set ntp *`
			`delete ntp *`
			`show ntp *`

OSPF	`ospf`	Control IPv4 dynamic routing through the Open Shortest-Path First protocol (OSPFv2).	`set ospf *`
			`show ospf *`
			`show route ospf *`

OSPF v3	`ospf3`	Control IPv6 dynamic routing through the Open Shortest-Path First protocol v3 (OSPFv3).	`set ipv6 ospf3 *`
			`set router-id *`
			`show ipv6 ospf3 *`
			`show ipv6 route ospf3 *`
			`show router-id *`

Password Policy	`password-controls`	Control password and account policies on Gaia.	`set password-controls *` `show password-controls *`
Performance Optimization	`perf`	Control Multi-Queue on Security Gateway.	`set multi-queue *` `show multi-queue *`

PIM	`pim`	Control Protocol-Independent Multicast (PIM).	`set pim *`
			`show pim *`
			`show mfc *`

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 *`
			`set pbrroute *`
			`show pbr *`
			`show pbrroute *`

Policy Routing	`pbr-routing-group`	Overview page for Policy Based Routing.	
Prefix Lists and Prefix Trees	`prefix`	Control Prefix Lists and Prefix Trees used in routing policy.	`set prefix-tree *` `set prefix-list *`

Proxy Settings	`proxy`	Control Proxy server on Gaia.	`set proxy *`
			`delete proxy *`
			`show proxy *`

RAID Monitoring	`raid-monitor`	Overview page for RAID volumes monitoring.	
RIP	`rip`	Control dynamic routing through the Routing Information Protocol for IPv4 (RIP).	`set rip *` `show rip *`
RIPng	`ripng`	Control dynamic routing through the Routing Information Protocol for IPv6 (RIPng).	`set ipv6 ripng *` `show ipv6 ripng *`

Roles	`rba`	Control user roles on Gaia.	`add rba *`
			`delete rba *`
			`show rba *`

Route	`route`	Show IPv4 and IPv6 routing table on Gaia.	`show route *` `show ipv6 route *`
Route Aggregation	`aggregate`	Create a supernet network from the combination of networks with a common routing prefix.	`set aggregate *` `show route aggregate *`
Route Injection Mechanism	`route-injection`	Control the Route Injection Mechanism (RIM) on Gaia.	`set kernel-routes *` `show route kernel *`

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish

Route Map	`routemap`	Configure route maps on Gaia.	`set routemap *`
			`show routemap *`
			`show routemaps *`

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 *` `show routed-clusterxl *`
Router Discovery	`rdisc`	Control ICMP Router Discovery on Gaia.	`set rdisc *` `show rdisc *`
Router Service	`router-service-group`	Overview page for Routing Services.	
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 *`
			`set trace *`
			`set tracefile *`
			`set max-path-splits *`
			`set nexthop-selection *`
			`set protocol-rank *`
			`set router-options *`
			`show trace *`
			`show routed *`
			`show protocol-rank *`
			`show router-options *`

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
SAM (Accelerator Card)	`sam`	Deprecated - SAM card is not supported by R80.10. Monitor Security Acceleration Module for information on usage and connections.	`show sam *`

Scheduled Backup	`sceduled_backup`	Create scheduled backups of the Gaia for events of data loss.	`add backup-scheduled *`
			`set backup-scheduled *`
			`delete backup-scheduled *`
			`show backup-scheduled`

Scratchpad Configuration	`scratchpad`	Control Scratchpad in Gaia Portal.	
Security Management GUI Clients	`mgmt-gui-clients`	Control allowed Security Management GUI Clients.	
Shutdown	`reboot_halt`	Shut down and reboot the Gaia.	`halt *` `reboot *`

Snapshot	`snapshot`	Create full backups (snapshots) of the Gaia.	`add snapshot *`
			`set snapshot *`
			`delete snapshot *`
			`show snapshots`
			`show snapshot *`

SNMP	`snmp`	Control Gaia monitoring through the Simple Network Management Protocol (SNMP).	`add snmp *`
			`set snmp *`
			`delete snmp *`
			`show snmp *`

Software Updates Policy Management	`installer_conf`	CPUSE - Manage deployment policy and mail notifications for software updates.	`Note - See sk92449 for most updated information.`
			`installer restore_policy *`
			`set installer *`
			`set installer download_mode *`
			`set installer install_mode *`
			`set installer download_mode schedule *`
			`set installer install_mode schedule *`

Static Multicast Routes	`static-mroute`	Configure multicast static routes on Gaia.	`set static-mroute *` `show static-mroute *`

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 *`
			`set backup *`
			`backup *`
			`restore *`
			`delete backup *`
			`show backups`
			`show backup *`
			`show restore *`

System Configuration	`sysconfig`	System Configuration.	

System Groups	`group`	Control Gaia user groups, for advanced management of privileges.	`add group *`
			`set group *`
			`delete group *`
			`show groups`
			`show group *`

System Logging	`syslog`	Control system logging on Gaia.	`add syslog *`
			`set syslog *`
			`delete syslog *`
			`show syslog *`

System Management	`system-group`	Overview page for System Management.	
System Status	`sysenv`	Hardware sensor monitoring.	`show sysenv *`
TACACS_Enable	`tacacs_enable`	Control TACACS+ mechanism on Gaia.	`tacacs_enable *` `show tacacs_enable *`

Time	`clock-date`	Configure the time and date on the Gaia.	`set clock *`
			`set date *`
			`set time *`
			`set timezone *`
			`show clock *`
			`show date *`
			`show time *`
			`show timezone *`

Upgrade	`upgrade`	Deprecated - upgrade the Gaia.
		Use the CPUSE instead.
			`upgrade *`
			`add upgrade *`
			`delete upgrade *`
			`show upgrade *`

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish

Upgrades (CPUSE)	`installer`	CPUSE - Show the update packages status and manage package downloads and installations on Gaia.	`Note - See sk92449 for most updated information.`
			
			`show installer *`
			`show installer available_packages *`
			`show installer available_local_packages *`
			`show installer installed_packages *`
			`show installer package_status *`
			`add installer *`
			`add installer private_url *`
			`installer *`
			`installer download *`
			`installer install *`
			`installer upgrade *`
			`installer uninstall *`
			`installer stop *`
			`installer start *`
			`installer restore_policy *`
			`set installer *`
			`set installer download_mode *`
			`set installer install_mode *`
			`set installer download_mode schedule *`
			`set installer install_mode schedule *`

Upgrades (CPUSE)	`software-updates-group`	Overview page for CPUSE.	
User Management	`security-access-group`	Overview page for User Management.	

Users	`user`	Control user accounts on Gaia.	`add user *`
			`set user *`
			`delete user *`
			`show user *`
			`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 *`
			`set virtual-system *`
			`delete virtual-system *`
			`show virtual-system *`

VPNT	`vpnt`	Control VPN Tunneling on Gaia.	`add vpn *`
			`set vpn *`
			`delete vpn *`

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 *`
			`add mcvr *`
			`set mcvr *`
			`delete mcvr *`
			`show vrrp *`
			`show mcvr *`

VSX	`vsx`	Enable or Disable the VSX mode (to be used only by Check Point Support only).	`set vsx *` `show vsx *`

Web configuration	`web`	Control Gaia Portal.	`set web *`
			`generate web *`
			`show web *`

List of Available Extended Commands in Roles

Command name in Gaia Portal	Command name in Gaia Clish	Description
`api`	`ext_api`	Start, stop, or check status of API server
`config_system`	`ext_config_system`	Run Gaia First Time Configuration tool in Expert mode.
`cp_conf`	`ext_cp_conf`	Check Point configuration utility for some local settings.
`cpca`	`ext_cpca`	Run Check Point Internal Certificate Authority (ICA).
`cpca_client`	`ext_cpca_client`	Control Check Point Internal Certificate Authority (ICA).
`cpca_create`	`ext_cpca_create`	Create Check Point Internal Certificate Authority (ICA) database.
`cpca_dbutil`	`ext_cpca_dbutil`	Control Check Point Internal Certificate Authority (ICA) database.
`cpca_dbutil`	`ext_cpca_dbutil`	Control Check Point Internal Certificate Authority (ICA) database.
`cpconfig`	`ext_cpconfig`	Check Point software configuration utility for Security Management Server and Security Gateway.
`cphaprob`	`ext_cphaprob`	Access to clustering commands.
`cphastart`	`ext_cphastart`	Enable the clustering feature on Security Gateway.
`cphastop`	`ext_cphastop`	Disable the clustering feature on Security Gateway.
`cpinfo`	`ext_cpinfo`	Collect Check Point diagnostics information.
`cplic`	`ext_cplic`	Control Check Point licenses.

Command name in Gaia Portal	Command name in Gaia Clish	Description
cpshared_ver	ext_cpshared_ver	Show Check Point SVN Foundation version.
cpstart	ext_cpstart	Start the installed Check Point products.
cpstat	ext_cpstat	Show Check Point statistics history information for Software Blades and Gaia.
cpstop	ext_cpstop	Stop the installed Check Point products.
cpview	ext_cpview	Show advanced Check Point statistics information for Software Blades and Gaia in real-time.
cpwd_admin	ext_cpwd_admin	Control Check Point WatchDog administration tool.
diag	ext_diag	Send system diagnostics information.
dtps	ext_dtps	Control Endpoint Policy Server commands.
etmstart	ext_etmstart	Start QoS Software Blade.
etmstop	ext_etmstop	Stop QoS Software Blade.
fgate	ext_fgate	Control QoS Software Blade.
fips	ext_fips	Control 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.

Command name in Gaia Portal	Command name in Gaia Clish	Description
ifconfig	ext_ifconfig	Deprecated. Use "show interface", or "set interface" commands instead.
ips	ext_ips	Control IPS Software Blade.
lomipset	ext_lomipset	Configure LOM card IP address.
LSMcli	ext_LSMcli	Access to SmartProvisioning command line.
LSMenabler	ext_LSMenabler	Enable SmartProvisioning.
mds_backup	ext_mds_backup	Create backup of the Multi-Domain Server.
mds_restore	ext_mds_restore	Restore backup of the Multi-Domain Server.
mdscmd	ext_mdscmd	Access to Multi-Domain Server command line.
mdsconfig	ext_mdsconfig	Check Point software configuration utility for Multi-Domain Server.
mdsstart	ext_mdsconfig	Check Point software configuration utility for Multi-Domain Server.
mdsstart	ext_mdsstart	Start Multi-Domain Server.
mdsstart_customer	ext_mdsstart_customer	Start specific Domain Management Server.
mdsstat	ext_mdsstat	Show the status of Multi-Domain Server and all Domain Management Servers.
mdsstop	ext_mdsstop	Stop Multi-Domain Server.
mdsstop_customer	ext_mdsstop_customer	Stop specific Domain Management Server.
netstat	ext_netstat	Print network connections, routing tables and interface statistics.

Command name in Gaia Portal	Command name in Gaia Clish	Description
ping	ext_ping	Ping a host using IPv4.
ping6	ext_ping6	Ping a host using IPv6.
raid_diagnostic	ext_raid_diagnostic	Access to RAID Monitoring tool.
raidconfig	ext_raidconfig	Access to RAID Configuration and Monitoring tool.
rtm	ext_rtm	Control the Monitoring Software Blade.
rtmstart	ext_rtmstart	Start the Monitoring Software Blade.
rtmstop	ext_rtmstop	Stop the Monitoring Software Blade.
rtmtopsvc	ext_rtmtopsvc	Monitor 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 IPS Snort conversion tool.
tecli	ext_tecli	Access to Threat Emulation Blade shell.
top	ext_top	Show the most active system processes.
traceroute	ext_traceroute	Trace the route to a host.
vpn	ext_vpn	Control the VPN kernel module for IPv4.
vpn6	ext_vpn6	Control the VPN kernel module for IPv6.
vsx_util	ext_vsx_util	Control managed VSX Gateways 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 nonlocal 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* and *Change My Password* (on page 203).

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 from users 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.
- Passwords 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.

Deny 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.

Deny 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 - Gaia Portal

Step	Description
1	In the navigation tree, click **User Management** > **Password Policy**.
2	Configure the password policy options: • **Password Strength** (on page 239) • **Password History** (on page 240) • **Mandatory Password Change** (on page 240) • **Deny Access to Unused Accounts** (on page 241) • **Deny Access After Failed Login Attempts** (on page 241)
3	Click **Apply**.

Password Strength

Parameter	Description
Minimum Password Length	The minimum number of characters in a Gaia user, or an SNMP user password. Does not apply to passwords that were already configured. • **Range**: 6 - 128 • **Default**: 6
Disallow Palindromes	A palindrome is a sequence of letters, numbers, or characters that can be read the same in each direction. • **Default**: Selected
Password Complexity	The required number of character types: • `1 - Don't check` • `2 - Require two character types` • `3 - Require three character types` • `4 - Require four character types` **Default**: `2 - Require two character types` Character types are: • Upper case alphabetic (A-Z) • Lower case alphabetic (a-z) • Digits (0-9) • Other (everything else) 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. Enables or disables password history checking and password history recording. 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**. Does not apply to SNMP passwords. • **Default:** Selected
History Length	The number of former passwords to keep and check against when a new password is configured for a user. • **Range**: 1 - 1000 • **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. The count starts when the user changes the password. Users are required to change an expired password the next time they log in. Does not apply to SNMP users. • **Range**: 1 - 1827, or `Passwords never expires` • **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. A user that does not log in, will not see this warning. • **Range**: 1 - 366 • **Default**: 7

Lockout users after password expiration	Lockout users after password expiration. After a user's password has expired, user has this number of days to log in and change it. If a user does not change the password within that number of days, the user will be unable to log in - the user will be locked out. The administrator can unlock a user that is locked out from the **User Management > Users** page. • **Range**: 1 - 1827, or `Never lockout users after password expires` • **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. • **Default**: Not selected

Deny Access to Unused Accounts

Parameter	Description
Deny access to unused accounts	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. • **Default**: Not selected
Days of non-use before lock-out	Configures the number of days of non-use before locking out the unused account. This only takes effect, if **Deny access to unused accounts** is enabled. • **Range**: 30 - 1827 • **Default**: 365

Deny 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. **Warning -** Enabling this leaves you open to a "denial of service" - if an attacker makes unsuccessful login attempts often enough, the affected user account will be locked out. Consider the advantages and disadvantages of this option, in light of your security policy, before enabling it. • **Default**: Not selected
Block admin user	This option is available only if **Deny access after failed login attempts** is enabled. 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. The number of failed login attempts that a user is allowed before being locked out. After making that many successive failed attempts, future attempts will fail. When one login attempt succeeds, counting of failed attempts stops, and the count is reset to zero. • **Range**: 2 - 1000 • **Default**: 10
Allow access again after time	This only takes effect, if **Deny access after failed login attempts** is enabled. Allow access again after a user was locked out (due to failed login attempts). The user is allowed access after the configured time, if there were no login attempts during that time. • **Range**: 60 - 604800 seconds • **Default**: 1200 seconds (20 minutes) Examples: • 60 = 1 minute • 300 = 5 minutes • 3600 = 1 hour • 86400 = 1 day • 604800 = 1 week

Configuring Password Policy - Gaia Clish

Use these commands to configure a policy for managing user passwords.

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
```

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

Parameters

Parameter	Description
`complexity <1-4>`	The required number of character types: • `1 - Don't check` • `2 - Require two character types` • `3 - Require three character types` • `4 - Require four character types` Character types are: • Upper case alphabetic (A-Z) • Lower case alphabetic (a-z) • Digits (0-9) • Other (everything else) Changes to this setting do not affect existing passwords. • **Range**: `1 - 4` • **Default**: 2

`min-password-length <6-128>`	The minimum number of characters in a Gaia user, or an SNMP user password. Does not apply to passwords that were already configured. • **Range**: `6 - 128` • **Default**: 6
`palindrome-check {on | off}`	A palindrome is a sequence of letters, numbers, or characters that can be read the same in each direction. • **Range**: on, or `off` • **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
```

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

Parameters

Parameter	Description
`history-checking {on | off}`	Check for reuse of passwords for all users. Enables or disables password history checking and password history recording. 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`. Does not apply to SNMP passwords. • **Range**: on, or `off` • **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. • **Range**: `1 - 1000` • **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
```

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

Parameters

Parameter	Description
`expiration-lockout-days <1-1827 | never>`	Lockout users after password expiration. After a user's password has expired, user has this number of days to log in and change it. If a user does not change the password within that number of days, the user will be unable to log in - the user will be locked out. The administrator can unlock a user that is locked out from the **User Management > Users** page. • **Range**: `1 - 1827`, or `never` • **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. A user that does not log in, will not see this warning. • **Range**: `1 - 366` • **Default**: 7

`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.
	• **Range**:
	  • `no` - Disables this functionality.
	  • `password` - Forces users to change their password after their password was changed.
	• **Default**: `no`

`password-expiration <1-1827 | never>`	The number of days, for which a password is valid. After that time, the password expires. The count starts when the user changes the password. Users are required to change an expired password the next time they log in. Does not apply to SNMP users. • **Range**: `1-1827`, or `never` • **Default**: `never`

Deny 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
```

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

Parameters

Parameter	Description
`deny-on-nonuse allowed-days <30-1827>`	Configures the number of days of non-use before locking out the unused account. This only takes effect, if `set password-controls deny-on-nonuse enable` is set to `on`. • **Range**: `30 - 1827` • **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. • **Range**: on, or `off` • **Default**: `off`

Deny 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
```

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

Parameters

Parameter	Description
`allow-after <60-604800>`	Allow access again after a user was locked out (due to failed login attempts). The user is allowed access after the configured time, if there were no login attempts during that time. • **Range:** `60 - 604800` seconds • **Default:** `1200` seconds (20 minutes) Examples: • 60 = 1 minute • 300 = 5 minutes • 3600 = 1 hour • 86400 = 1 day • 604800 = 1 week

`block-admin {on | off}`	This only takes effect if `set password-controls deny-on-fail enable` is set to `on`. 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. • **Range:** `on`, or `off` • **Default:** `off`
`enable {on | off}`	If the configured limit is reached, the user is locked out (unable to log in) for a configured time. **Warning -** Enabling this leaves you open to a "denial of service" - if an attacker makes unsuccessful login attempts often enough, the affected user account will be locked out. Consider the advantages and disadvantages of this option, in light of your security policy, before enabling it. • **Range:** `on`, or `off` • **Default:** `off`
`failures-allowed <2-1000>`	This only takes effect if `set password-controls deny-on-fail enable` is set to `on`. The number of failed login attempts that a user is allowed before being locked out. After making that many successive failed attempts, future attempts will fail. When one login attempt succeeds, counting of failed attempts stops, and the count is reset to zero, • **Range:** `2 - 1000` • **Default:** `10`

Monitoring Password Policy

Description

Show password Policy configuration.

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
```

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
gaia>
```

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:

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.

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.

Gaia supports TACACS+ for authentication only. Challenge-response authentication, such as S/Key, is not supported.

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.

Note - For TACACs authentication to work on a Virtual System, see the *R80.10 VSX Administration Guide* https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_VSX_AdminGuide/html_frameset.htm.

Configuring RADIUS Servers - Gaia Portal

To configure a RADIUS server:

Step	Description
1	In the navigation tree, click **User Management** > **Authentication Servers**.
2	In the **RADIUS Servers** section, click **Add**. The **Add New RADIUS Server** window opens.
3	Enter the RADIUS Server parameters: • **Priority** - The RADIUS server priority is an integer between -999 and 999 (default is 0). When there two or more configured RADIUS servers, Gaia connects to the RADIUS server with the highest priority. Low numbers have the higher priority. • **Host** - Host name or IP address (IPv4 or IPv6) of RADIUS server. • **UDP Port** - UDP port used on RADIUS server. The default port is 1812 as specified by the RADIUS standard. 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. **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. • **Shared Secret** - Shared secret used for authentication between the RADIUS server and the Gaia client. Enter the shared secret text string up to 256 characters, without any whitespace characters and without a backslash. Make sure that the shared string defined on the Gaia matches the shared string defined on the RADIUS server. RFC 2865 recommends that the secret be at least 16 characters in length. Some RADIUS servers have a maximum string length for shared secret of 15 or 16 characters. See the documentation for your RADIUS server. • **Timeout in** - **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. If there is no response after the configured timeout, Gaia tries to connect to a different configured RADIUS server. Set this timeout, so that the sum of all RADIUS server timeouts is less than 50.
4	Click **OK**.

Step	Description
5	**Optional:** Select the **Network Access Server (NAS)** IP address. This setting applies to all configured RADIUS servers. This parameter records the IP address, from which Gaia sends the RADIUS packet. 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. The "NAS-IP-Address" is defined in RFC2865 http://freeradius.org/rfc/rfc2865.html#NAS-IP-Address. 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 the *Users* (on page 205)). This setting applies to all configured RADIUS servers.
7	**Optional:** Select the **Super User ID** - 0 or 96. This setting applies to all configured RADIUS servers. If the UID is 0, there is no need to run the sudo command to get super user permissions (on page 257).
8	Click **Apply**.

To edit a RADIUS server:

Step	Description
1	In the navigation tree, click **User Management** > **Authentication Servers**.
2	Select the RADIUS server.
3	Click **Edit**. The **Edit RADIUS Server** window opens.
4	You can edit only the **Host**, **UDP Port**, **Shared secret**, and **Timeout**.
5	Click **OK**.

To delete a RADIUS server:

Step	Description
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 - Gaia Clish

Description

Use the `aaa radius-servers` commands to add, configure, and delete Radius authentication servers.

Syntax

- To configure RADIUS 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>
```

- To change 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>
```

- To change 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>
```

- To show a list of all configured RADIUS servers associated with an authentication profile:

```
show aaa radius-servers list
```

- To show the configuration of a specific RADIUS server:

```
show aaa radius-servers priority <Priority>
      host
      port
      timeout
```

- To show the configuration that applies to all configured RADIUS servers:

```
show aaa radius-servers
      NAS-IP
      default-shell
      super-user-uid
```

- To delete a specific RADIUS server:

```
delete aaa radius-servers
      priority <Priority>
```

- To delete 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

Parameter	Description
`priority <Priority>`	Configures the RADIUS server priority. Enter an integer between -999 and 999 (default is 0). When there two or more configured RADIUS servers, Gaia connects to the RADIUS server with the highest priority. 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. The default port is 1812 as specified by the RADIUS standard. 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. **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.
`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. Enter the shared secret text string up to 256 characters, without any whitespace characters and without a backslash. Make sure that the shared string defined on the Gaia matches the shared string defined on the RADIUS server. RFC 2865 recommends that the secret be at least 16 characters in length. Some RADIUS servers have a maximum string length for shared secret of 15 or 16 characters. 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. The default value is 3. If there is no response after the configured timeout, Gaia tries to connect to a different configured RADIUS server. 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 the *Users* (on page 205)).
`super-user-uid <0 | 96>`	Optional. Configures the UID for the RADIUS super user. If the UID is 0, there is no need to run the sudo command to get super user permissions (on page 257).
`NAS-IP`<SPACE><TAB>	Optional. This parameter records the IP address, from which Gaia sends the RADIUS packet. 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. The "NAS-IP-Address" is defined in RFC2865 http://freeradius.org/rfc/rfc2865.html#NAS-IP-Address. 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.

To configure Gaia as a RADIUS Client

Step	Description
1	Define the role for the RADIUS client: • If no group is defined on the RADIUS server for the client, define this role: • `radius-group-any` • If a group is defined on RADIUS server for the client (group XXX, for example), define this role: `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 the *Roles* (on page 213).

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.

Note - If you define a RADIUS user with a null password (on the RADIUS server), Gaia cannot authenticate that user.

To configure a RADIUS server for non-local Gaia users:

In addition, see sk72940 http://supportcontent.checkpoint.com/solutions?id=sk72940.

Step	Instructions

1	Copy the applicable dictionary file to your RADIUS server.
	
	Examples:
	
	Steel-Belted RADIUS server:
	
	a) Copy this file from the Gaia to the RADIUS server:
	`/etc/radius-dictionaries/checkpoint.dct`
	
	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):
	`vendor-product = Check Point Gaia`
	`dictionary = nokiaipso`
	`ignore-ports = no`
	`port-number-usage = per-port-type`
	`help-id = 2000`
	
	c) Add this line to the `dictiona.dcm` file:
	`"@checkpoint.dct"`
	
	FreeRADIUS server:
	
	a) Copy this file from the Gaia to the RADIUS server to the `/etc/freeradius/` directory:
	`/etc/radius-dictionaries/dictionary.checkpoint`
	
	b) Add this line to the `/etc/freeradius/dictionary` file:
	`"$INCLUDE dictionary.checkpoint"`
	
	OpenRADIUS server:
	
	a) Copy this file from the Gaia to the RADIUS server to the `/etc/openradius/subdicts/` directory:
	`/etc/radius-dictionaries/dict.checkpoint`
	
	b) Add this line `/etc/openradius/dictionaries` file immediately after the `dict.ascend`:
	`$include subdicts/dict.checkpoint`

Step	Instructions

2	Define the user roles on Gaia.
	Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:
	`CP-Gaia-User-Role = "role1,role2,...`
	For example:
	`CP-Gaia-User-Role = "adminrole, backuprole, securityrole"`

3	Define the Check Point users that must have superuser access to the Gaia shell. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:
	• If this user should not receive superuser permissions:
	`CP-Gaia-SuperUser-Access = 0`
	• If this user can receive superuser permissions:
	`CP-Gaia-SuperUser-Access = 1`

To log in as a 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.

To get super user permissions (for users that have a UID of 96):

Step	Description
1	Connect to the command line on Gaia.
2	Log in to Expert mode.
3	Run: `sudo /usr/bin/su -` The user now has superuser permissions.

Configuring TACACS+ Servers - Gaia Portal

To configure a TACACS+ server:

Step	Description
1	In the navigation tree, click **User Management** > **Authentication Servers**.
2	In the **TACACS+ Configuration** section, select **Enable TACACS+ authentication**. This setting applies to all configured TACACS+ servers.
3	Click **Apply**.
4	In the **TACACS+ Servers** section, click **Add**.
5	Configure the TACACS+ parameters: • **Priority** - The priority of the TACACS+ server - from 1 to 20. Must be unique for this operating system. Gaia uses the priority: • To determine the order, in which Gaia connects to the TACACS+ servers. First, Gaia connects to the TACACS+ server with the lowest priority number. For example: Three TACACS+ servers have a priority of 1, 5, and 10 respectively. Gaia connects to these TACACS+ servers in that order, and uses the first TACACS+ server that responds. • To identify the TACACS+ server in commands. A command with `priority 1` applies to the TACACS+ server with priority 1. • **Server** - IPv4 address of the TACACS+ server. • **Shared Key** - The Shared Secret used for authentication between the TACACS+ server and Gaia. Enter the shared secret text string up to 256 characters, without any whitespace characters and without a backslash. Make sure that the shared string defined on the Gaia matches the shared string defined on the TACACS+ server. • **Timeout in Seconds** - Enter the timeout in seconds (from 1 to 60), during which Gaia waits for the TACACS+ server to respond. The default value is 5. 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**. This setting applies to all configured TACACS+ servers.

To disable TACACS+ authentication:

Step	Description
1	In the navigation tree, click **User Management** > **Authentication Servers**.
2	In the **TACACS+ configuration** section, clear **Enable TACACS+ authentication**. This setting applies to all configured TACACS+ servers.
3	Click **Apply**.

To delete a TACACS+ server:

Step	Description
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.

To verify if the logged in user is enabled for TACACS+:

Run in Gaia Clish: `show tacacs_enable`

Configuring TACACS+ Servers - Gaia Clish

Description

Configure TACACS+ authentication servers.

Syntax

- To configure 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>
```

- To change 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>
```

- To change the configuration that applies to all configured TACACS+ servers:

```
set aaa tacacs-servers
      state {on | off}
      user-uid <0 | 96>
```

- To show a list of all configured TACACS+ servers associated with an authentication profile:

```
show aaa tacacs-servers list
```

- To show the configuration of a specific TACACS+ server:

```
show aaa tacacs-servers priority <Priority>
      server
      timeout
```

- To show the configuration that applies to all configured TACACS+ servers:

```
show aaa tacacs-servers
      state
      user-uid
```

- To delete a specific RADIUS server:

```
delete aaa tacacs-servers
      priority <Priority>
```

- To delete 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

Parameter	Description
`priority` <*Priority*>	The priority of the TACACS+ server - from 1 to 20. Must be unique for this operating system. The priority is used: • To determine the order, in which Gaia connects to the TACACS+ servers. First, Gaia connects to the TACACS+ server with the lowest priority number. For example: Three TACACS+ servers have a priority of 1, 5, and 10 respectively. Gaia connects to these TACACS+ servers in that order, and uses the first TACACS+ server that responds. • To identify the TACACS+ server in commands. A command with `priority 1` applies to the TACACS+ server with priority 1. Values: • **Range:** `1 - 20` • **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. Enter the shared secret text string up to 256 characters, without any whitespace characters and without a backslash. Make sure that the shared string defined on the Gaia matches the shared string defined on the TACACS+ server.
`timeout <1-60>`	Enter the timeout in seconds, during which Gaia waits for the TACACS+ server to respond. If there is no response after the configured timeout, Gaia tries to connect to a different configured TACACS+ server. • **Range:** `1 - 60` • **Default:** `5`
`new-priority` <*New Priority*>	Configures the new priority for the TACACS+ server.
`state {on | off}`	Configures the state of TACACS+ authentication. • **Range:** `on`, or `off` • **Default:** `off`

Example

```
gaia> set aaa tacacs-servers priority 2 server 10.10.10.99 key MySharedSecretKey
timeout 10
```

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.

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.

To configure Gaia as a TACACS+ Client:

Step	Description
1	Connect to Gaia OS as the `admin` user.
2	Define the role `TACP-0`.
3	Define the features for the role. For instructions, see the *Roles* (on page 213).
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.

To raise TACP privileges using the Gaia Clish:

Step	Description
1	Connect to the command line.
2	Log in to the Gaia Clish using the username and password of the TACACS+ user.

Step	Description
3	After you are authenticated by the TACACS server, you will see the Gaia Clish prompt. At this point, you have the privileges of the TACP-0 role. Run: `tacacs_enable TACP-<N>` 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.

To show if the currently logged in user is authenticated by TACACS+, run:

```
show tacacs_enable
```

To raise privileges in the Gaia Portal:

Step	Description
1	In your web browser, connect to Gaia Portal.
2	Enter the username and password of the TACACS+ user. 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.

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 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 http://supportcontent.checkpoint.com/solutions?id=sk98733.

Note - sk98733 http://supportcontent.checkpoint.com/solutions?id=sk98733 is 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.

Note - If you define a TACACS user with a null password (on the TACACS server), Gaia cannot authenticate that user.

System Groups

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 "Role-Based Administration" (on page 213).

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 - Gaia Portal

To see a list of all groups:

In the navigation tree, click **User Management > System Groups**.

To add a System Group:

Step	Description
1	In the navigation tree, click **User Management > System Groups**.
2	Click **Add**.
3	In the **Group Name** field, enter the desired 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: • Group ID range 0-100 and range 65531-65535 are reserved for system use. • Group ID 0 is reserved for users with root permissions. • Group ID 10 is reserved for the predefined Users groups. If you specify a value in the reserved ranges, an error message is displayed.
5	Click **OK**.

To add a user to a System Group:

Step	Description
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. To select several users: a) Press and hold the **Ctrl** key on the keyboard. b) Left-click the applicable users. The selected users become highlighted.
5	Click **Add >**. The selected users move to the **Members of Group** list.
6	Click **OK**.

To remove a user from a System Group:

Step	Description
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. To select several users: a) Press and hold the **Ctrl** key on the keyboard. b) Left-click the applicable users. The selected users become highlighted.
5	Click **Add >**. The selected users move to the **Available Members** list.
6	Click **OK**.

To delete a System Group:

Step	Description
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 - Gaia Clish

Description

Manage System Groups.

Syntax

- To add a System Group:
```
add group <Group Name> gid <Group ID>
```
- To add a user to a System Group:
```
add group <Group Name> member<SPACE><TAB>
add group <Group Name> member <UserName>
```
- To change the Group ID of a System Group:
```
set group <Group Name> gid <Group ID>
```
- To show users in a System Group:
```
show group <Group Name>
```
- To show all configured System Groups:
```
show groups
```
- To remove a user from a System Group:
```
delete group <Group Name> member<SPACE><TAB>
delete group <Group Name> member <UserName>
```
- To delete 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

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: • Group ID range 0-100 and range 65531-65535 are reserved for system use. • Group ID 0 is reserved for users with root permissions. • Group ID 10 is reserved for the predefined Users groups. If you specify a value in the reserved ranges, an error message is displayed.
`member` <*UserName*>	Name of an existing user.

GUI Clients

If this machine is installed as a Security Management Server, you can define which computers can connect to this Security Management Server with SmartConsole.

This section does not show if this machine is installed as a Multi-Domain Server.

Security Management GUI Clients - Gaia Portal

Step	Description
1	In the navigation tree, click **User Management > GUI Clients**.
2	Click **Add**. The **Add GUI Client** window opens.
3	Define the GUI clients (trusted hosts). These are the values: • **Any IP Address** All clients are allowed to log in, regardless of their IP address. This option only shows if **Any** was not defined during the initial configuration. • **This machine - IP address** • **Network** • **Range of IPv4 addresses**

Security Management GUI Clients - Command Line

Step	Description

1	Run: `cpconfig`.
	A list of configuration options shows.
	For example:
	`Configuration Options:`
	`----------`
	`(1) Licenses and contracts`
	`(2) Administrator`
	`(3) GUI Clients`
	`(4) SNMP Extension`
	`(5) PKCS#11 Token`
	`(6) Random Pool`
	`(7) Certificate Authority`
	`(8) Certificate's Fingerprint`
	`(9) Configure Check Point CoreXL`
	`(10) Automatic start of Check Point Products`

2	Enter **3** for the **GUI Clients** option.
3	A list of hosts selected to be GUI clients shows. You can add or delete hosts, or create a new list. You can add new GUI clients in these formats: • **IP address** - One computer defined by its IPv4 or IPv6 address. • **Machine name** - One computer defined by its hostname. • **"Any"** - An IPv4 address without restriction. You must: a) Enter the word **Any** with capital letter "**A**" b) Press the Enter key c) Press the **CTRL+D** keys. • **IP/Netmask** - A range of IPv4 or IPv6 addresses (for example, 192.168.10.0/255.255.255.0 or 2001::1/128). • **A range of addresses** - A limited range of IPv4 or IPv6 addresses (for example, 192.168.10.8-192.168.10.16 or 2001::1-2001::10). • **Wild cards (IPv4 only)** - A limited range of IPv4 addresses only (for example, 192.168.10.*).

High Availability

In This Section:

VRRP 273
Configuring Monitored Circuit/Simplified VRRP 283
Configuring Advanced VRRP 292
Troubleshooting VRRP 303

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.

Understanding VRRP

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 via 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 defined in RFC 3768.

On Gaia, VRRP can be used with and without ClusterXL enabled.

With ClusterXL enabled, which is the most common use case, VRRP supports a maximum of one VRID with one Virtual IP Address (VIP) for each interface. In addition, only Active/Backup environments are supported. 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. You must also configure *priority deltas* to allow a failover to the VRRP Backup node, when the VRID on any on interface fails over.

With ClusterXL disabled, Active/Active environments can be deployed. You can configure two VRIDs on the same interface, with one VIP for each VRID. Only Static Routes are supported on the VRRP interfaces. In addition, you must disable *VRRP monitoring of the Check Point Firewall* (on page 281).

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 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 Configuration Methods

You can configure VRRP using one of these methods:

Method	Description
Monitored Circuit/Simplified VRRP	This method contains all of the basic parameters, and is applicable for most environments. It makes possible a complete node failover by automatically monitoring all VRRP-enabled interfaces. You can configure only one VRID, which is automatically added to all the VRRP interfaces. 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. To configure Monitored Circuit/Simplified VRRP in the Gaia Portal, click **High Availability > VRRP**.
Advanced VRRP	This method allows configuration of different VRIDs on different interfaces. With ClusterXL enabled, you must configure each VRID to monitor every other VRRP interface. You must also configure priority deltas that allow complete node failover. Advanced VRRP also makes it possible for a VRID to monitor interfaces that do not run VRRP. With ClusterXL disabled, active/active deployments are possible, and you can configure two VRIDs on each interface, with one VIP for each VRID (on page 278). To configure Advanced VRRP in the Gaia Portal, click **High Availability > Advanced VRRP**.

Note - You cannot use the Monitored Circuit/Simplified VRRP and Advanced VRRP types together on the same Cluster Member.

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 Backups. VRRP advertisements broadcast the operational status of the VRRP Master to the VRRP Backups. 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 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 defined priority value. You define a priority for each Security Gateway when you create a Virtual Router or change its configuration. If two 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 define 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.

In simplified *Monitored Circuit VRRP*, you configure each Virtual Router as one unit. Monitored-circuit VRRP automatically monitors all VRRP interfaces. The same VRID is configured on all interfaces.

In *Advanced VRRP*, the VRID is configured 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.

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

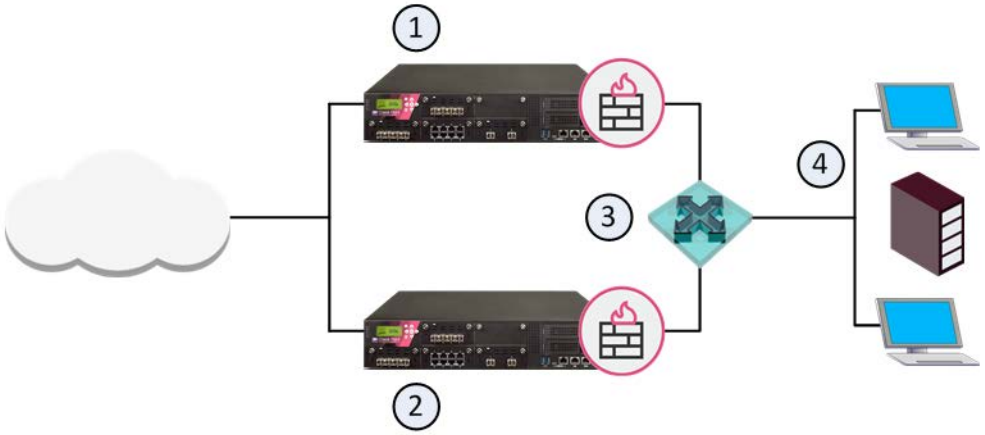
Master that handles the traffic, but is configured with a lower priority. Sometimes, interfaces that come up, take longer than the VRRP timeout to process incoming VRRP Hello packets. The interface delay extends the time that VRRP waits to receive VRRP Hello packets from the existing VRRP Master.

Typical VRRP Use Cases

This section shows examples of some use case VRRP environments.

Internal Network High Availability

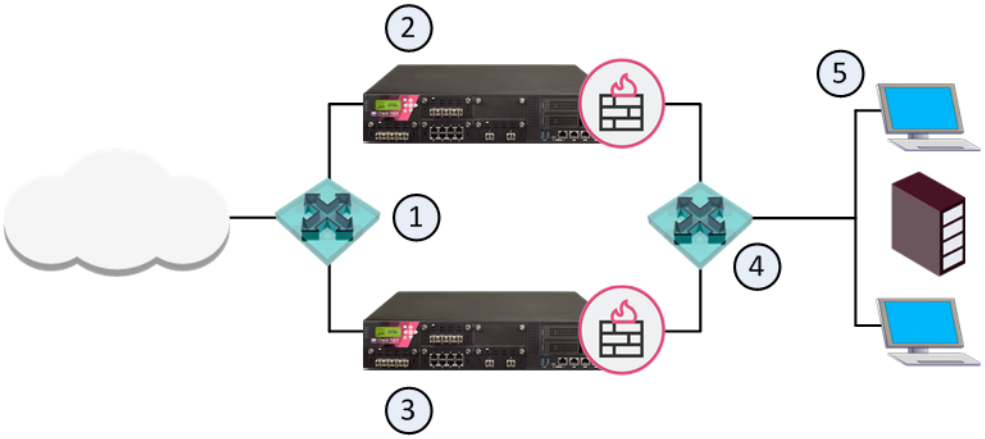
This is a simple VRRP use case, where Security Gateway 1 is the VRRP Master, and Security Gateway 2 is the VRRP Backup. Virtual Router redundancy is available only for connections to and from the internal network. There is no redundancy for external network traffic.



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

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. Define 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

Internal Network Load Sharing

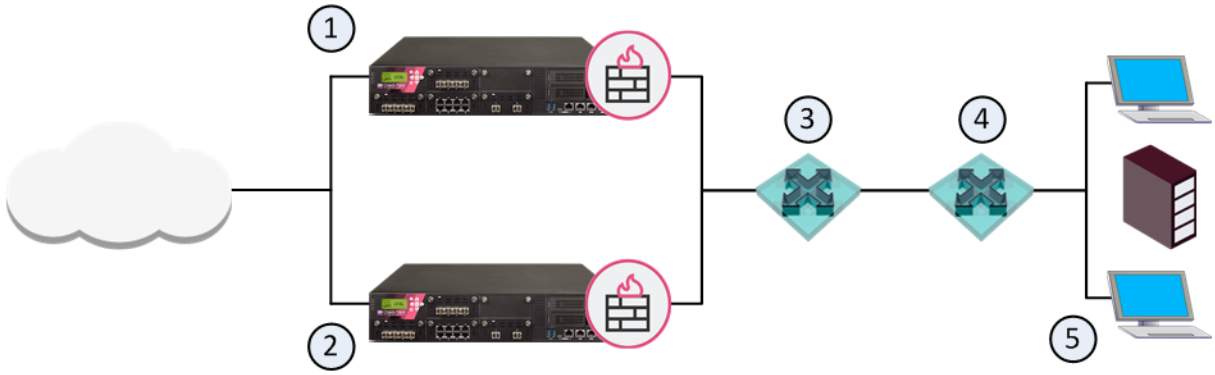
This use case shows an example of an Active/Active Load Sharing environment for internal network traffic. This environment gives load balancing, as well as full redundancy.

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

Do these steps before you start to define a Virtual Router (VRRP Group):

Step	Description
1	Synchronize the system time on all Security Gateways to be included in this Virtual Router. **Best Practice -** We recommend that you enable NTP (Network Time Protocol) (on page 142) on all Security Gateways. You can also manually change the time and time zone on each Security Gateway to match the other members. In this case, you must synchronize member times to within a few seconds.
2	**Optional:** Add host names and IP address pairs to the host table (on page 119) on each Security Gateway. This lets you use host names as an alternative to IP addresses or DNS servers.

Configuring Network Switches

Best Practice - If you use the Spanning Tree protocol on Cisco switches connected to Check Point VRRP clusters, we recommend that you enable PortFast. PortFast 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.

Enabling Virtual Routers

When you log into Gaia for the first time after installation, you must use the First Time Configuration Wizard to the initial configuration steps. To use VRRP Virtual Routers (clusters), you must first enable VRRP clustering in the First Time Configuration Wizard.

To enable VRRP clustering:

1. Install Gaia using the instructions in the *R80.10 Installation and Upgrade Guide* http://downloads.checkpoint.com/dc/download.htm?ID=60369.
2. On the First Time Configuration Wizard **Products** page, select Security Gateway.
   Do not select Security Management. The standalone environment (Security Gateway and Security Management Server) is not supported for VRRP.
3. Select **Unit is part of a cluster**.
4. Select **VRRP Cluster** from the list.
5. Continue with the next steps in the wizard.
6. When prompted to reboot the Security Gateway, click **Cancel**.
   Do not reboot.
7. Do one of these steps:
   - Run `cpconfig` on the Security Gateway. Select `Enable cluster membership for this` gateway to enable State synchronization.

     Note - This is the most common use and does not support active/active mode. You must configure VRRP so that the same cluster member is the VRRP master on all interfaces. Dynamic routing configuration must match on each cluster member.

     OR:

   - Do not enable ClusterXL.

     Note - This is useful when each cluster member is required to be the VRRP master at the same time. You can configure two VRRP Virtual Routers on the same interface. Each cluster member can be the VRRP master for a different VRID on the same interface while it backs up the other. This configuration can also help run VRRP in a High-Availability pair with a device from another vendor. Disable the VRRP monitoring of the Firewall when you use this configuration. It is enabled by default but, but not supported with this configuration. In addition, only Static Routes are supported with this configuration.
8. Enter `y` when prompted.
9. Reboot the Security Gateway.

Do this procedure for each Virtual Router member.

When you complete this procedure for each VRRP member, do these steps in the Gaia Portal:

1. In the navigation tree, click **High Availability > VRRP**.
2. Refer to the **VRRP Global Settings** section.
3. If the **Disable All Virtual Routers** option is currently selected, clear it.
4. Click **Apply Global Settings**.

When you complete these procedures, define your Virtual Routers using the Gaia Portal or the Gaia Clish.

Configuring Global Settings for VRRP

This section includes shows you how to configure the global settings. Global settings apply to all Virtual Routers.

Configure these VRRP global settings:

Step	Description
1	In the navigation tree, click one of these: • **High Availability > VRRP**. • **High Availability >Advanced VRRP**.
2	In the **VRRP Global Settings** section: • **Cold Start Delay** - Configures the delay period in seconds before a Security Gateway joins a Virtual Router. Default = 0. • **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. • **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. • **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. **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**.

Configuration Notes:

Gaia starts to monitor the firewall after the cold start delay completes. This can cause some problems:

- If all the Security Gateway (member) interfaces in a Virtual Router fail, all Security Gateways become VRRP Backups. None of the Security Gateways can become the VRRP Master and no traffic is allowed.
- If you change the time on any of the Security Gateways (member), a failover occurs automatically.
- In certain situations, installing a firewall policy causes a failover. This can happen if it takes a long time to install the policy.

Configuring Monitored Circuit/Simplified VRRP

This section includes the procedure for configuring Monitored Circuit/Simplified VRRP.

Configuring Monitored Circuit/Simplified VRRP - Gaia Clish

Description

Configure Monitored Circuit/Simplified VRRP on a single Security Gateway.

Syntax

- To add Monitored Circuit/Simplified VRRP:

  Important - The order, in which you run the `add mcvr` commands is important.

  First, configure the priority:

  ```
  add mcvr vrid VALUE priority VALUE priority-delta VALUE [authtype {none | simple VALUE} hello-interval VALUE
  ```

  Then, configure the backup address:

  ```
  add mcvr vrid VALUE backup-address VALUE vmac-mode VALUE
  ```

- To configure 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
  ```

- To show Monitored Circuit/Simplified VRRP configuration:

  ```
  show mcvr
        vrid VALUE
        all
        authtype
        backup-address VALUE
        backup-addresses
        hello-interval
        priority
        priority-delta
        vrids
  ```

- To delete 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

Parameter	Description
`vrid` *VALUE*	Configures the Virtual Router ID. • **Range:** `1 - 255` • **Default:** No default value

`authtype {none | simple` *VALUE*`}`	Configures authentication for the given Virtual Router.
	You must use the same authentication method for all Security Gateways in a Virtual Router.
	• **Range:**
	  • `none` - Disables authentication
	  • `simple <plain-text password>` - Authenticates VRRP packets using a plain-text password
	• **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. 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. 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. • **Range:** `on`, or `off` • **Default:** `off`

Parameter	Description
`backup-address` *VALUE*	Configures the IPv4 address of the VRRP Backup Security Gateway. You can define more than one address for a Virtual Router. 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.

`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.
	Each Virtual IP Address for a Virtual Router implies the existence of a virtual network interface.
	• **Range:**
	  • `default-vmac` - Generates the VMAC using the standard method described in Section 7.3 of RFC 3768.
	  • `extended-vmac` - Generates the VMAC using an extended range of uniqueness by dynamically calculating 3 bytes of the VMAC instead of only 1.
	  • `interface-vmac` - Configures the VMAC to use the interface hardware MAC address.
	  • `static-vmac <VALUE>`- Configures the Virtual Router to use a specified static VMAC address.
	• **Default:** `default-vmac`
	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. • **Range:** `default`, or `1 - 255` • **Default:** `1`

Parameter	Description
`preempt-mode {on | off}`	Configures Preempt Mode for the given Virtual Router. When Preempt Mode is enabled, if the Virtual Router has a higher Priority than the current VRRP Master, it preempts the VRRP Master. In Preempt Mode is disabled, all Virtual Routers that have monitored interfaces, are participating to avoid potential split-brain network topology. For more information on the implications of disabling Preempt Mode, see the help text for the `set mcvr vrid <VALUE> monitor-vrrp` command. • **Range:** on, or `off` • **Default:** `off`
`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. 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. • **Range:** `default`, or `1 - 254` • **Default:** `100`
`priority-delta` *VALUE*	Updates the Priority Delta of the given Virtual Router. 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. 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. • **Range:** `default`, or `1 - 254` • **Default:** No default value

Configuring Monitored Circuit/S

implified VRRP - Gaia Portal

This section includes the basic procedure for configuring a Virtual Router using the Gaia Portal.

To add a new Virtual Router:

Step	Description
1	In the navigation tree, click **High Availability > VRRP**.
2	Configure the **VRRP Global Settings** (on page 281).
3	In the **Virtual Routers** section, click **Add**.

Step	Description

4	In the **Add Virtual Router** window, configure these parameters:
	• **Virtual Router ID** - Enter a unique ID number for this virtual router. The range of valid values is 1 to 255.
	• **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.
	• **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.
	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.
	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).
	• **Authentication:**
	  • **None** - To disable authentication of VRRP packets
	  • **Simple** - To authenticate VRRP packets using a plain-text password
	  You must use the same authentication method for all Security Gateways in a Virtual Router.
	• **Priority Delta -** Enter the value to subtract from the **Priority** to create an effective priority when an interface fails. The range is 1-254.
	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.
	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.
	• **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.
	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.
	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, Priority Delta should be set equal to the Priority value, so that Priority will become zero, if an interface goes down.

Step	Description
5	In the **Backup Addresses** section, click **Add**. Configure these parameters in the **Add Backup Address** window: • **IPv4 address** - Enter the interface IPv4 address. • **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. Select one of these Virtual MAC modes: • **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. • **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. **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. • **Static** - Manually set the VMAC address. Enter the VMAC address in the applicable field. • **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. **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. Click **OK**. The new VMAC mode shows in the in the **Backup Address** table.
6	To remove a Backup Address, select an address and click **Delete**. The address is removed from the **Backup Address** table.
7	Click **Save**.

Configuring the VRRP Security Gateway Cluster in SmartConsole

Step	Description
1	In SmartConsole, click **Objects** menu **> More object types > Network Object > Gateways and Servers > Cluster > New Cluster**. The **Check Point Security Gateway Cluster Creation** window opens.
2	Click **Wizard Mode**.
3	Define these: • **Cluster Name** • **Cluster IPv4 Address** • For an IPv6 cluster: **Cluster IPv6 Address**
4	In the **Choose the Cluster's Solution** field, select **Gaia VRRP**.
5	Click **Next**.
6	On the **Cluster members' properties** page, add the cluster members.
7	Click **Finish**.

Configuring VRRP Rules for the Security Gateway

1. Define this rule above the Stealth Rule in the Rule Base:

Source	Destination	VPN	Services & Applications	Action
Firewalls (Group) fwcluster-object	mcast-224.0.0.1	Any	vrrp igmp	accept

   Where:

   - **Firewalls** -Simple Group object containing the firewall objects.
   - **fwcluster-object** - the VRRP cluster object.
   - **mcast-224.0.0.18** - Node Host object with the IP address 224.0.0.18.

2. If your Security Gateways use dynamic routing protocols (such as OSPF or RIP), create new rules for each multicast destination IP address.

   Alternatively, you can create a Network object to show all multicast network IP destinations with these values:

   - Name: MCAST.NET
   - IP: 224.0.0.0
   - Net mask: 240.0.0.0

   You can use one rule for all multicast protocols you agree to accept, as shown in this example:

Source	Destination	VPN	Services & Applications	Action
All Cluster IP addresses	fwcluster-object MCAST.NET	Any	vrrp igmp ospf rip	accept

Configuring Advanced VRRP

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 included in the VRRP sections (on page 283).

With Advanced VRRP, you must configure every Virtual Router to monitor every configured VRRP interface.

To change from Advanced VRRP to Monitored Circuit/Simplified VRRP:

Step	Description
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. Do these steps to delete and add new interfaces with the necessary IP addresses:

Step	Description
1	Cause a failover to the VRRP Backup.
2	Reduce the priority, or disconnect an interface.
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 - Gaia P

ortal

To add a Virtual Router:

Step	Description
1	In the navigation tree, click **High Availability >Advanced VRRP**.
2	Configure the *VRRP Global Settings* (on page 281).
3	In the **Virtual Routers** section, click **Add**.
4	In the **Add New Virtual Router** window, configure these parameters:
4A	**Interface** - Select the interface for the Virtual Router.
4B	**Virtual Router ID** - Enter or select the ID number of the Virtual Router.
4C	**Priority** - Enter or select the priority value. 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.
4D	**Hello Interval** - Enter or select the number of seconds, at which the VRRP Master sends VRRP advertisements. The range is 1 to 255 seconds. The default value is 1. 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. 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 minimal VRRP Hello interval is 1 second. Therefore, the minimal failover time is 3 seconds (3 * Hello Interval).
4E	**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. 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.
4F	**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. If you select 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. 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	Description
4G	**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. Select the mode: • **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. • **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. **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. • **Static** - Manually set the VMAC address. Enter the VMAC address in the applicable field. • **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. **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.
4H	**Authentication**: • **None** - To disable authentication of VRRP packets. • **Simple** - To authenticate VRRP packets using a plain-text password. You must use the same authentication method for all Security Gateways in a Virtual Router.
5	In the **Backup Addresses** section: a) Click **Add**. b) In the **IPv4 address** field, enter the IPv4 address. c) Click **Ok**. To change a Backup Address, select a Backup IP address and click **Edit**. To remove a Backup Address, select a Backup IP address and click **Delete**.

Step	Description
6	In the **Monitored Interfaces** section: a) Click **Add**. Gaia shows a warning that adding a Monitored Interface will lock the Interface for this Virtual Router. b) Click **OK** to confirm. c) In the **Interface** field, select the interface. d) In **Priority Delta** field, enter or select the number to subtract from the priority. This creates an effective priority when an interface related to the VRRP Backup fails. The range is 1-254. e) Click **Ok**. To change a Monitored Interface, select a Monitored Interface and click **Edit**. To remove a Monitored Interface, select a Monitored Interface and click **Delete**.
7	Click **Save**.

Configuring Advanced VRRP - Gaia Clish

Description

Configure Global and Advanced VRRP settings.

Syntax

- To configure Advanced VRRP:

```
set vrrp
      accept-connections {on | off}
      coldstart-delay VALUE
      disable-all-virtual-routers {on | off}
      monitor-firewall {on | off}
      interface-delay VALUE
```

- To configure 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
```

- To show 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

Parameter	Description
`accept-connections {on | off}`	Controls the Accept Connections option. This option causes packets destined to VRRP Virtual IP Address(es) to be accepted, and any required responses be generated. Enabling this option enhances VRRP's interaction with network management tools, which in turn allows for faster failure detection. This option is required for High Availability applications (for example, routing protocols), whose service is tied to a Virtual IP Address. • **Range:** on, or `off` • **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. • **Range:** `0 - 3600` • **Default:** `0`
`disable-all-virtual-routers {on | off}`	Enables or disables all IPv4 VRRP Virtual Routers. If disabled, the VRRP configuration is preserved and can be enabled again. • **Range:** on, or `off` • **Default:** `off`
`monitor-firewall {on | off}`	Enables or disables VRRP monitoring of the Security Gateway state. If this option is enabled, and the Firewall is not ready, the cluster member will refuse to be the VRRP Master. • **Range:** on, or `off` • **Default:** on
`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. Note - Same value should be configured for both VRRPv2 and VRRPv3 if both protocols are configured. • **Range:** `0 - 3600` • **Default:** `0`

Parameter	Description
`interface VALUE`	The name of the interface, on which to enable the VRRP.

`authtype {none | simple` *VALUE*`}`	Configures authentication for the given Virtual Router.
	You must use the same authentication method for all Security Gateways in a Virtual Router.
	• **Range:**
	  • `none` - Disables authentication
	  • `simple <plain-text password>` - Authenticates VRRP packets using a plain-text password
	• **Default:** No default value

`monitored-circuit vrid` *VALUE*	Configures the Virtual Router ID. • **Range:** `1 - 255` • **Default:** No default value
`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. 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. 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. • **Range:** on, or `off` • **Default:** `off`

Parameter	Description
`monitored-circuit vrid` *VALUE* `backup-address` *VALUE* `{on | off}`	Configures the IPv4 address of the VRRP Backup Security Gateway. You can define more than one address for a Virtual Router. 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. • **Range:** `default`, or `1 - 255` • **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. • `on` - Creates a VRRP Virtual Router • `off` - Removes a VRRP Virtual Router • `priority-delta` - Configures the Priority Delta value 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). Otherwise, network destinations will become unreachable, etc. This coordinated failover is achieved by adding all dependent interfaces to the list of monitored interfaces. 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. Refer to the following commands for additional details: • `set vrrp interface <VALUE> monitored-circuit vrid <VALUE> priority` • `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. When Preempt Mode is enabled, if the Virtual Router has a higher Priority than the current VRRP Master, it preempts the VRRP Master. In Preempt Mode is disabled, all Virtual Routers that have monitored interfaces, are participating to avoid potential split-brain network topology. For more information on the implications of disabling Preempt Mode, see the help text for the `set mcvr vrid <VALUE> monitor-vrrp` command. • **Range:** `on`, or `off` • **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. 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. • **Range:** `default`, or `1 - 254` • **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.
	Each Virtual IP Address for a Virtual Router implies the existence of a virtual network interface.
	• **Range:**
	  • `default-vmac` - Generates the VMAC using the standard method described in Section 7.3 of RFC 3768.
	  • `extended-vmac` - Generates the VMAC using an extended range of uniqueness by dynamically calculating 3 bytes of the VMAC instead of only 1.
	  • `interface-vmac` - Configures the VMAC to use the interface hardware MAC address.
	  • `static-vmac` <VALUE>- Configures the Virtual Router to use a specified static VMAC address.
	• **Default:** `default-vmac`

`set vrrp interface` *VALUE* `off`	Deletes all Virtual Routers from the interface.
`set virtual-router legacy off`	Disables legacy VRRPv2 configuration. 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. Hence, you must replace all legacy `virtual-router` configuration commands using the equivalent `monitored-circuit` configuration commands.

Configuring VRRP Clusters in SmartConsole

This section includes the procedure for configuring a VRRP cluster object in SmartConsole. Only those procedures that are related to VRRP are shown here.:

Step	Description
1	In SmartConsole, create a new cluster object using the **Classic** mode.
2	Enter the Virtual IP address as the main IP address.
3	On the **Cluster Members** page, add the physical Security Gateways included in the Virtual Router.
4	On the **ClusterXL and VRRP** page, select **High Availability** and then select **VRRP** from the list.
5	Select all of the options in the **Advanced** settings section, including **Use State Synchronization**.
6	On the **Topology** page, configure the cluster and member Security Gateway interfaces as required. Make sure that you configure the synchronization interfaces.
7	Configure other cluster parameters as necessary.
8	Click **OK**.
9	Install the Access Control Policy.

Troubleshooting VRRP

This section shows known issues with VRRP configurations and fixes. Read this section before contacting Check Point Support (https://supportcenter.checkpoint.com).

Traces for VRRP

You can log information about errors and events for troubleshooting VRRP. Enable traces (debug) for VRRP.

To enable traces for VRRP:

Step	Description
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. We recommend you select **All**. To select several specific options: a) Press and hold the **Ctrl** key on the keyboard. b) Left-click on the applicable options. The selected options become highlighted. To select several consecutive options: a) Left-click on the first consecutive applicable option. b) Press and hold the **Shift** key on the keyboard. c) Left-click on the last consecutive applicable option. The selected options become highlighted.
4	Click **Add**. The selected options show **Enabled**.
5	Scroll to the top of this page.
6	In the **Routing Options** section, click **Apply**. The Gaia restarts the routing subsystem and signals it to reread its configuration. The debug information is saved in **/var/log/routed.log*** files and **/var/log/routed_messages*** files. Note - As an *example*, see sk84520 - How to debug OSPF and RouteD daemon on Gaia http://supportcontent.checkpoint.com/solutions?id=sk84520.

To disable traces for VRRP:

Step	Description
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**. In the **VRRP** table, select **All**.
3	Click **Remove**. The options do not show **Enabled** anymore.
4	Scroll to the top of this page.
5	In the **Routing Options** section, click **Apply**. 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 page 142) 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 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 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

In This Section:

Licenses 306
License Activation - Gaia Portal 323
Snapshot Management 325
Download SmartConsole 332
Hardware Health Monitoring 333
Monitoring RAID Synchronization 338
Shutdown 339
System Backup 340

This chapter includes procedures and reference information for maintaining your Gaia computer.

Licenses

You can add or delete licenses using one of these:

- Gaia Portal > **Maintenance** section > **Licenses** page.
- The `cplic db_add` and `cplic del` commands.

Note - While all the `cplic` commands are available in Gaia, they are not grouped into a Gaia feature.

Configuring Licenses - Gaia Portal

If you need to get a license, visit the User Center https://usercenter.checkpoint.com.

See the *R80.10 Gaia Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=54824.

To add a license:

Step	Description
1	In the left navigation tree, click **Maintenance > Licenses**.
2	Click **New**. The **Add License** window opens.
3	Enter the license data manually, or click **Paste License** to enter the data automatically. The **Paste License** button only shows in Internet Explorer. For other web browsers, paste the license strings into the empty text field.
4	Click **OK**.

To delete a license:

Step	Description
1	In the left navigation tree, click **Maintenance > Licenses**.
2	Select a license in the table.
3	Click **Delete**.

cplic

The `cplic` command lets you manage Check Point licenses. The `cplic` command can be run in Gaia Clish or in Expert Mode.

Best Practice - Manage licenses in the SmartUpdate GUI.

License Management is divided into three types of commands:

- *Local licensing commands* are executed on the Check Point computers.
- *Remote licensing commands* are executed on the Security Management Server, and affect the managed Security Gateways.
- *License Repository commands* are executed on the Security Management Server, and affect the licenses stored in the local license repository.

For more about managing licenses, see the *R80.10 Security Management Administration Guide* https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_SecurityManagement_AdminGuide/html_frameset.htm.

Syntax for Local Licensing

```
cplic
      -h
      put <options>
      del <options>
      print <options>
      check  <options>
      contract  <options>
```

Syntax for Remote Licensing

```
cplic
      -h
      put <Object Name> ...
      del <Object Name> <options>
      get {<IP Address> | <Host Name> | -all}
      upgrade -l <Input File>
```

Syntax for License Database Operations

```
cplic
      -h
      db_add <options>
      db_rm <options>
      db_print <options>
```

Note - For help on commands, add the `-h` option.

cplic check

Description

Confirms that the license includes the feature on the local Security Gateway or Security Management Server.

Syntax

```
cplic check [-p <Product>] [-v <Version>] [-c | -count] [-t <Date>] [-r |
-routers] [-S | -SRusers] <Feature>
```

Parameters

Parameter	Description
`-p` <*Product*>	Product, for which license information is requested. Example: `fw1, netso`
`-v` <*Version*>	Product version, for which license information is requested.
`-c | -count`	Outputs the number of licenses connected to this feature.
`-t` <*Date*>	Checks license status on future date. Use the format **ddmmyyyy**. A feature can be valid on a given date on one license, but invalid on another.
`-r | -routers`	Checks how many routers are allowed. The <*Feature*> option is not needed.
`-S | -SRusers`	Checks how many SecuRemote users are allowed.
<*Feature*>	Feature, for which license information is requested.

cplic db_add

Description

Adds one or more licenses to the license repository on the Security Management Server.

When local licenses are added to the license repository, they are automatically attached to the intended Check Point Security Gateway. Central licenses have to undergo the attachment process. This command is a license repository command and can only be executed on the Security Management Server.

Syntax

```
cplic db_add -l <License File> [<Host>] [<Expiration Date>] [<Signature>]
[<SKU/Features>]
```

Parameters

Parameter	Description
`-l` <*License File*>	Name of the file that contains the license.
<*Host*>	Security Management Server hostname or IP address.
<*Expiration Date*>	The license expiration date.
<*Signature*>	The license signature string. For example: `aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m` The string is case sensitive and the hyphens are optional.
<*SKU/Features*>	The SKU of the license summarizes the features included in the license. For example, `CPSUITE-EVAL-3DES-vNG`

Example

If the file `192.0.2.11.lic` contains one or more licenses, the command `cplic db_add -l 192.0.2.11.lic` produces output similar to:

```
gaia> cplic db_add -l 192.0.2.11.lic
Adding license to database ...
Operation Done
```

cplic db_print

Description

Displays the details of Check Point licenses stored in the license repository on the Security Management Server.

Syntax

```
cplic db_print <Object Name | -all> [-n | -noheader] [-x] [-t | -type] [-a | -attached]
```

Parameters

Parameter	Description
<*Object Name*>	Prints only the licenses attached to <*Object Name*>. <*Object Name*> is the name of the Check Point Security Gateway object as defined in SmartConsole.
`-all`	Prints all the licenses in the license repository.
`-n` | `-noheader`	Prints licenses with no header.
`-x`	Prints licenses with their signatures.
`-t` | `-type`	Prints licenses with their type: Central or Local.
`-a` | `-attached`	Shows to which object the license is attached. Useful, if the `-all` option is specified.

Note - This command is a license repository command and can only run on the Security Management Server.

cplic db_rm

Description

Removes a license from the license repository on the Security Management Server. It can be executed ONLY after the license was detached using the `cplic del` command. Once the license is removed from the repository, it can no longer be used.

Syntax

```
cplic db_rm <Signature>
```

Parameters

Parameter	Description
<*Signature*>	The signature string within the license.

Example

```
gaia> cplic db_rm 2f540abb-d3bcb001-7e54513e-kfyigpwn
```

Note - This command is a license repository command and can only run on the Security Management Server.

cplic del

Description

Deletes a single Check Point license on a host, including unwanted evaluation, expired, and other licenses. Used for both local and remote machines

Syntax

```
cplic del [-F <Output File>] <Signature> <Object Name>
```

Parameters

Parameter	Description
`-F` <*Output File*>	Sends the output to <*output file*> instead of the screen.
<*Signature*>	The signature string within the license. To see the license signature string, run the `cplic print -x` command.
<*Object Name*>	The name of the Check Point Security Gateway object as defined in SmartConsole.

cplic del <object name>

Description

Detaches a Central license from a Check Point Security Gateway. When this command is executed, the license repository is automatically updated. The Central license remains in the repository as an unattached license. This command can only run on a Security Management Server.

Syntax

```
cplic del <Object Name> [-F <Output File>] [-ip <Dynamic IP Address>] <Signature>
```

Parameters

Parameter	Description
<*Object Name*>	The name of the Check Point Security Gateway object as defined in SmartConsole.
`-F` <*Output File*>	Diverts the output to `outputfile` rather than to the screen.
`-ip` <*Dynamic IP Address*>	Deletes the license on the Check Point Security Gateway with the specified IP address. Use this parameter to delete a license on a DAIP Check Point Security Gateway. **Note -** If this parameter is used, then object name must be a DAIP Security Gateway.
<*Signature*>	The signature string within the license.

Note - This is a Remote Licensing command, which affects remote managed machines. It is executed on the Security Management Server.

cplic get

Description

Retrieves all licenses from Security Gateways into the license repository on the Security Management Server. This command helps to synchronize the repository with the Check Point Security Gateways. When the command is run, all local changes are updated.

Syntax

```
cplic get {<IP Address> | <Host Name> | -all} [-v41]
```

Parameters

Parameter	Description
<*IP Address*>	The IP address of the Check Point Security Gateway, from which licenses are to be retrieved.
<*Host Name*>	The name of the Check Point Security Gateway object as defined in SmartConsole, from which licenses are to be retrieved.
`-all`	Retrieves licenses from all Check Point Security Gateways in the managed network.
`-v41`	Retrieves version 4.1 licenses from the NF Check Point Security Gateway. Used to upgrade version 4.1 licenses.

Example

If the Check Point Security Gateway with the object name `caruso` contains four Local licenses, and the license repository contains two other Local licenses, the command `cplic get caruso` produces output similar to this:

```
gaia> cplic get caruso
Get retrieved 4 licenses.
Get removed 2 licenses.
```

Note - This is a Remote Licensing Command, which affects remote machines. It is executed on the Security Management Server.

cplic print

Description

The `cplic print` command prints details of Check Point licenses on the local machine.

Syntax

```
cplic print [-n|-noheader][-x][-t|-type][-F <Output File>] [-p|-preatures]
```

Parameters

Parameter	Description
`-n|-noheader`	Prints licenses with no header.
`-x`	Prints licenses with their signature.
`-t|-type`	Prints licenses showing their type: Central or Local.
`-F <Output File>`	Diverts the output to <*Output File*>.
`-p|-preatures`	Prints licenses resolved to primitive features.

Note - On a Check Point Security Gateway, this command prints all licenses that are installed on the local machine, both local and central licenses.

cplic put

Description

Installs one or more local licenses on a local machine.

Syntax

```
cplic put [-o|-overwrite] [-c|-check-only] [-s|-select] [-F <Output File>]
[-P|-Pre-boot] [-k|-kernel-only] -l <License File> [<Host>] [<Expiration Date>]
[<Signature>] [<SKU/Features>]
```

Parameters

Parameter	Description
`-o | -overwrite`	On a Security Management Server, this erases all existing licenses and replaces them with the new licenses. On a Check Point Security Gateway, this erases only the local licenses, but not central licenses that are installed remotely.
`-c | -check-only`	Verifies the license. Checks if the IP of the license matches the machine and if the signature is valid.
`-s | -select`	Selects only the local license whose IP address matches the IP address of the machine.
`-F` <*Output File*>	Outputs the result of the command to the designated file rather than to the screen.
`-P | -Pre-boot`	Use this option after you have upgraded and before you reboot the machine. Use of this option will prevent certain error messages.
`-K | -kernel-only`	Pushes the current valid licenses to the kernel. For use by Check Point Support only.
`-l` <*License File*>	Name of the file that contains the license.
<*Host*>	Hostname or IP address of Security Management Server.
<*Expiration Date*>	The license expiration date.
<*Signature*>	The license signature string. For example: `aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m` (The string is case sensitive and the hyphens are optional).
<*SKU/Features*>	The SKU of the license summarizes the features included in the license. For example: `CPSUITE-EVAL-3DES-vNG`

Copy and paste the parameters from the license received from the User Center:

Parameter	Description
`host`	One of these: • **All platforms** - The IP address of the external interface (in dot notation). The last part cannot be 0 or 255. • **Solaris2** - The response to the `hostid` command (beginning with `0x`).
`expiration date`	The license expiration date. It can be `never`.
`signature`	The license signature string. For example: `aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m` (Case sensitive. The hyphens are optional.)
`SKU/features`	A string listing the SKU and the Certificate Key of the license. The SKU of the license summarizes the features included in the license. For example: `CPSB-SWB CPSB-ADNC-M CK0123456789ab`

Example

```
gaia> cplic put -l License.lic
Host             Expiration SKU
192.168.2.3  14Jan2016  CPSB-SWB CPSB-ADNC-M CK0123456789ab
gaia>
```

cplic put <object name>

Description

Attaches one or more central or local licenses remotely. When this command is executed, the license repository is also updated.

Syntax

```
cplic put <Object Name> [-ip Dynamic IP] [-F <Output File>] -l <License File>
[<Host>] [<Expiration Date>] [<Signature>] [<SKU/Feature>]
```

Parameters

Parameter	Description
<*Object Name*>	The name of the Check Point Security Gateway object, as defined in SmartConsole.
`-ip` <*Dynamic IP*>	Installs the license on the Check Point Security Gateway with the specified IP address. This parameter is used for installing a license on a DAIP Check Point Security Gateway. **Note** - If this parameter is used, then the object name must be a DAIP Check Point Security Gateway.
`-F` <*Output File*>	Diverts the output to <*outputfile*> rather than to the screen.
`-l` <*license File*>	Installs the licenses from <*license file*>.
<*Host*>	Hostname or IP address of Security Management Server.
<*Expiration Date*>	The license expiration date.
<*Signature*>	The license signature string. For example: `aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m` The string is case sensitive and the hyphens are optional.
<*SKU/Features*>	The SKU of the license summarizes the features included in the license. For example: `CPSUITE-EVAL-3DES-vNG`

Note - This is a remote licensing command, which affects remote machines. It is executed on the Security Management Server. More than one license can be attached.

Copy and paste the parameters from the license received from the User Center:

Parameter	Description
`host`	One of these: • **All platforms** - The IP address of the external interface (in dot notation). The last part cannot be 0 or 255. • **Solaris2** - The response to the `hostid` command (beginning with `0x`).
`expiration date`	The license expiration date. It can be `never`.
`signature`	The license signature string. For example: `aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m` (Case sensitive. The hyphens are optional.)
`SKU/features`	A string listing the SKU and the Certificate Key of the license. The SKU of the license summarizes the features included in the license. For example: `CPSB-SWB CPSB-ADNC-M CK0123456789ab`

cplic upgrade

Description

Upgrades licenses in the license repository with licenses in a license file from the user center.

Syntax

```
cplic upgrade -l <Input File>
```

Parameters

Parameter	Description
`-l <Input File>`	Upgrades the licenses in the license repository and Check Point Security Gateways to match the licenses in <Input File>.

Example

This example explains the procedure to upgrade the licenses in the license repository. There are two Software Blade licenses in the file. One does not match any license on a remote Security Gateway, the other matches a version NGX license on a Security Gateway that has to be upgraded.

- Upgrade the Security Management Server to the latest version.

  Ensure that there is connectivity between the Security Management Server and the Security Gateways with the previous product versions.

- Import all licenses into the license repository. This can also be done after upgrading the products on the remote Security Gateways.

- Run this command:

  ```
  cplic get -all
  ```

  Example:

  ```
  [Expert@MyMGMT]# cplic get -all
   Getting licenses from all modules ...
  MyGW:
  Retrieved 1 licenses
  ```

- To see all the licenses in the repository, run this command:

  ```
  cplic db_print -all -a
  ```

  Example:

  ```
  [Expert@MyMGMT]# cplic db_print -all -a
   Retrieving license information from database ...

  The following licenses appear in the database:
  ==================================================
  Host         Expiration Features
  192.0.2.11   Never      CPFW-FIG-25-53       CK49C3A3CC7121 golda
  192.0.2.11   26Nov2017  CPSB-SWB CPSB-ADNC-M CK0123456789ab count
  ```

- In the User Center https://usercenter.checkpoint.com, view the licenses for the products that were upgraded from version NGX to a Software Blades license. You can also create new upgraded licenses.

- Download a file containing the upgraded licenses. Only download licenses for the products that were upgraded from version NGX to Software Blades.

- If you did not import the version NGX licenses into the repository, import the version NGX licenses now. Use the command `cplic get -all`
- Run the license upgrade command: `cplic upgrade –l <inputfile>`
  - The licenses in the downloaded license file and in the license repository are compared.
  - If the certificate keys and features match, the old licenses in the repository and in the remote Security Gateways are updated with the new licenses.
  - A report of the results of the license upgrade is printed.

Note - This is a remote licensing command, which affects remote Security Gateways. It is executed on the Security Management Server.

For more about managing licenses, see the *R80.10 Security Management Administration Guide* https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_SecurityManagement_AdminGuide/html_frameset.htm.

License Activation - Gaia Portal

A license can be activated online or offline. Appliances with Internet connectivity and access to the Check Point User Center automatically fetch the license.

- A license check takes place immediately on a newly installed Security Management Server and continues until a license is attached.
- On a Security Gateway, a license check takes place before establishing SIC with the management server. If the Security Gateway has Internet connectivity, a license is fetched. If no connectivity exists, automatic activation attempts continue after SIC is established until the Security Gateway is activated.

To activate a license manually online:

Step	Description
1	In your web browser, connect to the Gaia Portal.
2	If necessary, configure a proxy. In the navigation tree, click **System Management > Proxy**.
3	In the navigation tree, click **Maintenance > License Status**.
4	Click **Activate Now**. Gaia fetches the license, the status changes to *Activated.* Available blades populate the table.

If the appliance does not have access to the Internet or User Center, you can manually activate the license if you have the license string.

To activate a license manually offline:

Step	Description
1	In your web browser, connect to the Gaia Portal.
2	In the navigation tree, click **Maintenance > License Status**.
3	Click **Offline Activation**.
4	Click **New**.
5	Paste the license string in the top field.
6	Click **OK**.

Note - The above activation procedures applies to these Gaia appliances:

- 2200
- 3000
- 4000
- 5000
- 12000
- 13000
- 15000
- 21000
- 23000
- Threat Emulation Appliances
- Smart-1 Appliances

To delete a license:

Step	Description
1	In your web browser, connect to the Gaia Portal.
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` (on page 313) command.

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
- Management database (on a Security Management Server or a Multi-Domain Server)

A snapshot is very large. A snapshot includes the entire root partition and some 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 release or on this release. You must import it to the same appliance or open server hardware model.
- After importing the snapshot, you must activate the device license from the Gaia Portal or the User Center.

Snapshot options:

- **Revert** to a user created image.
- **Revert** to a factory default image, which is automatically created on Check Point appliances by the installation or upgrade procedure.
- **Delete** an image from the local system.
- **Export** an existing image. This creates a compressed version of the image. You can download the exported image to a different computer and delete the exported image from the Gaia computer. This saves disk space. You must not rename the exported image. If you rename a snapshot image, it is not possible to revert to it.
- **Import** an exported image.
- **View** a list of images that are stored locally.

Important - See sk98068: Gaia Limitations after Snapshot Recovery http://supportcontent.checkpoint.com/solutions?id=sk98068.

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.

It is not recommended to use snapshots as a way of regularly backing up your system. System Backup is the preferred method (on page 66). Schedule system backups on a regular basis, daily or weekly, to preserve the Gaia OS configuration and firewall database.

Snapshot Prerequisites

Before you create a snapshot image, make sure the appliance or storage destination meets these prerequisites:

- To create the snapshot image requires free space on the disk. 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:

  a) Connect to the command line on the Gaia computer.

  b) Log in to the Gaia Clish.

  c) Run:

  ```
  show snapshots
  ```

  The output shows the amount of space on the disk available for snapshots.

  Note - 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 minimal size of a snapshot image is 2.5GB. Therefore, the minimal necessary free disk space in the export file location is 5GB.

See sk98068: Gaia Limitations after Snapshot Recovery
http://supportcontent.checkpoint.com/solutions?id=sk98068.

Working with Snapshot Management - Gaia Portal

Before you create a snapshot image, make sure the appliance or storage destination meets the prerequisites.

To create a snapshot:

Step	Description
1	In the navigation tree, click **Maintenance > Snapshot Management**.
2	Click **New**. The **New Image** window opens.
3	In the **Name** field, enter a name for the image. **Optional:** In the **Description** field, enter a description for the image.
4	Click **OK**.

To restore a snapshot:

Step	Description
1	In the navigation tree, click **Maintenance > Image Management.**
2	Select a snapshot.
3	Click **Revert**. The **Revert** window opens. **Note** - Pay close attention to the warnings about overwriting settings, the credentials, and the reboot and the image details.
4	Click **OK**.

To delete a snapshot:

Step	Description
1	In the navigation tree, click **Maintenance > Snapshot Management**.
2	Select a snapshot.
3	Click **Delete**. The **Delete Image** window opens.
4	Click **OK**.

To export a snapshot:

Step	Description
1	In the navigation tree, click **Maintenance > Snapshot Management**.
2	Select a snapshot.
3	Check the snapshot size.
4	Make sure that there is enough free disk space in the `/var/log/` partition:
4A	Connect to the command line on Gaia.
4B	Log in to Expert mode.
4C	Run: `[Expert@HostName]# df -kh | egrep "Mounted|/var/log"` Check the value in the `Avail` column.
5	In Gaia Portal, select a snapshot.

Step	Description
6	Click **Export**. 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.

To import 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	Description
1	In the navigation tree, click **Maintenance > Snapshot Management**.
2	Click **Import**. The **Import Image** window opens.
3	Click **Browse** to select the snapshot file for upload.
4	Click **Upload**.
5	Click **OK**.

Working with Snapshot Management - Gaia Clish

Before you create a snapshot image, make sure the appliance or storage destination meets the prerequisites.

Description

Manage system images (snapshots).

Syntax

- To create a new snapshot image:

```
add snapshot <Name of Snapshot> desc "<Description of Snapshot>"
```

- To export an existing snapshot image:

```
set snapshot export<SPACE><TAB>
```

```
set snapshot export <Name of Snapshot> path <Path> name <Name of Exported Snapshot>
```

- To import a snapshot image:

```
set snapshot import <External Name of Snapshot> path <Path> name <Name of Imported Snapshot>
```

- To revert to an existing snapshot image:

```
set snapshot revert<SPACE><TAB>
```

```
set snapshot revert <Name of Snapshot>
```

  Important - Reverting to the selected snapshot will overwrite the existing running configuration and settings. Make sure you know credentials of the snapshot, to which you revert.

- To show snapshot image information:

```
show snapshot <Name of Snapshot>
      all
      date
      desc
      size
```

```
show snapshots
```

- To delete a 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
`snapshot` <*Name of Snapshot*>	Configures the name of the snapshot image. You must enter a string that does not contain spaces.
`desc "`<*Description of Snapshot*>`"`	Configures the description of the snapshot image. You must enclose the text in double quotes, or enter the string that does not contain spaces.
`export` <*Name of Snapshot*>	Selects the snapshot image you export by the specified name. You must enter a string that does not contain spaces.
`import` <*Name of Snapshot*>	Selects the snapshot image you import by the specified name. You must enter a string that does not contain spaces.
`path` <*Path*>	Configures the path to the specified snapshot image file (for example: `/var/log/`).
`name` <*Name of Exported Snapshot*>	Configures the name, under which the exported snapshot image file is stored on the hard disk. You must enter a string that does not contain spaces.
`name` <*Name of Imported Snapshot*>	Configures the name, under which the imported snapshot image is stored on Gaia. You must enter a string that does not contain spaces.

Example

```
gaia> add snapshot snap1 desc first_image_after_installation

gaia> set snapshot export snap1 path /var/log/ name
first_image_after_installation
```

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 same Gaia computer, from which it was exported.

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.

Note - This procedure overwrites all existing configuration settings. We recommend that you create a snapshot image before you restore a factory default image.

To restore a factory default image in Gaia Portal:

Step	Description
1	In the navigation tree, click **Maintenance > Snapshot Management**.
2	Use the revert option.
3	Follow the instructions on the screen.
4	In the navigation tree, click **Maintenance > Shut Down**.
5	Click **Reboot**.

To restore a factory default image in Gaia Clish:

Step	Description
1	Connect to the command line on your appliance.
2	Log in to Gaia Clish.

3	Run:
	`gaia> set fcd revert<SPACE><TAB>`
	`gaia> set fcd revert <Name of Default Image>`

4	Follow the instructions on the screen.
5	Reboot: `gaia> reboot`

Download SmartConsole

You can download the SmartConsole application package from the Gaia Portal of your Security Management Server or Multi-Domain Security Management Server. After downloading the SmartConsole package, you can install it and use it to connect to the Security Management Server or Multi-Domain Security Management Server.

Step	Description
1	In your web browser, connect to the Gaia Portal on your Security Management Server or Multi-Domain Security Management Server.
2	In the navigation tree, select one of these options: • Click **Overview**. At the top of the page, click **Download Now!** • Click **Maintenance > Download SmartConsole > Download**.

Hardware Health Monitoring

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 http://supportcontent.checkpoint.com/solutions?id=sk119232.

Showing Hardware Health Information - Gaia Portal

Note - The **Hardware Health** page appears only on supported hardware.

In the navigation tree, click **Maintenance** > **Hardware Health**.

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 - Gaia Clish (show sysenv)

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.

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/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.

In addition, see sk119232 - Hardware sensors thresholds on Check Point appliances http://supportcontent.checkpoint.com/solutions?id=sk119232.

show asset

Description

Shows information about the hardware, on which Gaia is installed. You can run it 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>	Shows a list of asset categories, such as `system` and `disk`. The available categories depend on the type of hardware.
`all`	Shows all available hardware information. The information shown depends on the type of hardware.
<*Category Name*>	Shows available information for a specified category.

Example 1

```
gaia> show asset<SPACE><TAB>
system  all
gaia>
```

Example 2

```
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>
```

cpstat os -f sensors

Description

Shows information from supported hardware sensors. You can run it in Gaia Clish, or Expert mode.

Syntax

```
cpstat os -f sensors
```

Example

```
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|
----------------------------------------
```

Monitoring RAID Synchronization

In R80.10, 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 - 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 - Command Line

Run one of these commands in Gaia Clish or Expert mode:

- `raid_diagnostic`

  This shows data about the RAID and hard disks, with the percent synchronization done.

  Example output from a Smart-1 225 appliance:

```
Expert@cpmodule]#raid_diagnostic
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.

- `cpstat os -f raidInfo`

  This shows almost the same information as the `raid_diagnostic` command, in tabular format.

  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|
-------------------------------------------------------------------------------------------



Disk 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|
-----------------------------------------------------------------------------------------------------------------------------------------------
```

Shutdown

There are two ways to shut down:

- **Reboot:** Shut down the system and then immediately restart it.
- **Halt:** Shut down the system. You start the system, use the power switch.

Shutting Down and Rebooting - Gaia Portal

To shut down the system and then immediately restart it:

Step	Description
1	In the navigation tree, click **Maintenance > Shut Down**.
2	Click **Reboot**.

To shut down the system completely:

Step	Description
1	In the navigation tree, click **Maintenance > Shut Down**.
2	Click **Halt**.

Shutting Down and Rebooting - Gaia Clish

To shut down the system and then immediately restart it:

Run the `reboot` command.

To shut down the system completely:

Run the `halt` command.

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. The configuration is saved to a `*.tgz` file. You can store backups locally, or remotely to a TFTP, SCP or FTP server. You can run the backup manually, or on a schedule.
- Save your Gaia system configuration settings as a ready-to-run a CLI shell script. This lets you quickly restore your system configuration after a system failure or migration.

Notes:

- You can only do a migration using the same Gaia version on the source and target computers.
- When you do a backup for a Management Server, make sure to close all SmartConsole clients. Otherwise, the backup does not start.

Backing Up and Restoring the System - Gaia Portal

To add a backup:

Step	Description
1	In the navigation tree, click **Maintenance > System Backup**. Refer to the **Backup** section.
2	Click **Backup**. The **New Backup** window opens.
3	Select the location of the backup file: • **This appliance** - To store the collected backup locally • **Management** - To send the collected backup to the Security Management Server that manages this Security Gateway. • **SCP server** - To send the collected backup to an SCP server. Enter the IP address, User name, Password and Upload path. • **FTP server** - To send the collected backup to an FTP server. Enter the IP address, User name, Password and Upload path. • **TFTP server** - To send the collected backup to a TFTP server. Enter the IP address.

Important - When you create a backup on a Security Management Server, make sure to close all SmartConsole clients. Otherwise, backup does not start.

Note - Gaia Portal does not support the change of backup file names. You can change a backup file name in Expert mode. Make sure not to use special characters.

To restore from a locally saved backup:

Step	Description
1	In the navigation tree, click **Maintenance > System Backup**. Refer to the **Backup** section.
2	Select the backup file and click **Restore**.

To restore from a remotely saved backup:

Step	Description
1	In the navigation tree, click **Maintenance > System Backup**. Refer to the **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: • **Management** - To restore the backup from the Security Management Server that manages this Security Gateway • **SCP server** - To restore the backup from an SCP server. Enter the IP address, User name, Password and Upload path. • **FTP server** - To restore the backup from an FTP server. Enter the IP address, User name, Password and Upload path. • **TFTP server** - To restore the backup from a TFTP server. Enter the IP address.
5	Click **Restore**.

To export a backup:

Step	Description
1	In the navigation tree, click **Maintenance > System Backup**. Refer to the **Backup** section.
2	Select the backup file.
3	Click **Export**.
4	Click **OK** to confirm. Make sure you have enough free disk space on your computer.

To import a backup:

Step	Description
1	In the navigation tree, click **Maintenance > System Backup**. Refer to the **Backup** section.
2	Select the backup file.
3	Click **Import**.
4	Click **Browse** and select the backup file on your computer.
5	Click **Import**.

To delete a backup:

Step	Description
1	In the navigation tree, click **Maintenance > System Backup**. Refer to the **Backup** section.
2	Select the backup file.
3	Click **Delete**.
4	Click **OK** to confirm.

Backing Up an

d Restoring the System - Gaia Clish

Description

Collect a backup of the system's configuration. Restore the system's configuration.

Important - When you create a backup on a Security Management Server, make sure to close all SmartConsole clients. Otherwise, backup does not start.

Syntax

- To collect a backup and store it locally:
  ```
  add backup local [interactive]
  ```
- To collect a backup and upload it to an SCP server:
  ```
  add backup scp ip <IPv4 Address of SCP Server> path <Path on SCP Server> username
  <User Name on SCP Server> [password <Password in Plain Text>] [interactive]
  ```
- To collect a backup and upload it to an FTP server:
  ```
  add backup ftp ip <IPv4 Address of FTP Server> path <Path on FTP Server> username
  <User Name on FTP Server> [password <Password in Plain Text>] [interactive]
  ```
- To collect a backup and upload it to a TFTP server:
  ```
  add backup tftp ip <IPv4 Address of TFTP Server> [interactive]
  ```
- To show the status of the latest backup:
  ```
  show backup {last-successful | logs | status}
  ```
- To show 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.

Note - Gaia Clish does not support change of file names. You can change a file name in Expert mode. Make sure not to use special characters.

Example

```
gaia> add backup local
Creating backup package. Use the command 'show backups' to monitor creation
progress.
gaia>
gaia> show backup status
Performing local backup
gaia>
gaia> show backups
backup_gw-8b0891_22_7_2012_14_29.tgz Sun, Jul 22, 2012 109.73 MB
gaia>
```

Description

Restore the system's configuration.

Syntax

- To restore a backup from a local hard disk:
  ```
  set backup restore local<SPACE><TAB>
  ```
- To restore 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 <User Name on SCP Server> [password <Password in Plain Text>] [interactive]
  ```
- To restore 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 <User Name on FTP Server> [password <Password in Plain Text>] [interactive]
  ```
- To restore a backup from a TFTP Server:
  ```
  set backup restore tftp ip <IPv4 Address of TFTP Server> file <Name of Backup File> [interactive]
  ```

Note - To restore the Gaia OS configuration quickly after a system failure or migration, use the Gaia Clish `configuration` (on page 349) feature.

Configuring Scheduled Backups - Gaia Portal

To add a scheduled backup:

Step	Description
1	In the navigation tree, click **Maintenance > System Backup**. Refer to the **Scheduled Backup** section.
2	Click **Add Scheduled Backup**.
3	In the **Backup Name** field, enter the name of the job. • The maximal length is 15 characters. • The name can consist only of letters, numbers, or underscore "_".
4	In the **Backup Type** section, configure the location of the backup file: • **This appliance** - To store the collected backup locally • **Management** - To send the collected backup to the Security Management Server that manages this Security Gateway. • **SCP server** - To send the collected backup to an SCP server. Enter the IP address, User name, Password and Upload path. • **FTP server** - To send the collected backup to an FTP server. Enter the IP address, User name, Password and Upload path. • **TFTP server** - To send the collected backup to a TFTP server. Enter the IP address.
5	In **Backup Schedule** section, configure the frequency (**Daily**, **Weekly**, **Monthly**) for this backup.
6	Click **Add**. The scheduled backup shows in the **Scheduled Backups** table.

Important - When you create a backup on a Security Management Server, make sure to close all SmartConsole clients. Otherwise, scheduled backup does not start.

To delete a scheduled backup:

Step	Description
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 - Gaia Clish

Description

Configure a scheduled backup of the system configuration.

Important - When you create a backup on a Management Server, make sure to close all SmartConsole clients. Otherwise, scheduled backup does not start.

Syntax

- To add a backup schedule that stores the backup file locally:
```
add backup-scheduled name <Name of Schedule> local
```
- To add 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 <User Name on FTP Server> password <Password in Plain Text>
```
- To add 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 <User Name on SCP Server> password <Password in Plain Text>
```
- To add 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>
```
- To configure the backup schedule to run each day:
```
set backup-scheduled name <Name of Schedule> recurrence daily time <HH:MM>
```
- To configure the backup schedule to run each month on specified date and time:
```
set backup-scheduled name <Name of Schedule> recurrence monthly month <1-12> days <1-31> time <HH:MM>
```
- To configure the backup schedule to run each week on specified day of week and time:
```
set backup-scheduled name <Name of Schedule> recurrence weekly days <1-6> time <HH:MM>
```
- To show the scheduled backup configuration:
```
show backup-scheduled<SPACE><TAB>
```
```
show backup-scheduled <Name of Schedule>
```
- **To delete 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: • The maximal length is 15 characters. • The name can consist only of letters, numbers, or underscore "_".
`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.
`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 FTP remote server where to upload the backup file.
`path` <*Path on SCP Server*>	Specifies the path on the SCP remote server where to upload the backup file.
`username` <*User Name on FTP Server*>	Specifies the user name required to log in to the remote FTP server.
`username` <*User Name on SCP Server*>	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.
`recurrence daily time` <*HH:MM*>	Specifies that the job should run once a day - every day, at specified time. Enter the time of day in the 24-hour clock format - <Hours>:<Minutes>. Example: 14:35
`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. Months are specified by numbers from 1 to 12: January = 1, February = 2, ..., December = 12. Dates of month are specified by numbers from 1 to 31. To specify several consequent months, enter their numbers separate by commas. Example: for January through March, enter 1,2,3 To specify several consequent dates, enter their numbers separate by commas. Example: for 1st, 2nd and 3rd day of month, enter 1,2,3

`recurrence weekly days <1-31> time` *<HH:MM>*	Specifies that the job should run once a week - on specified days of week, and at specified time. Days of week are specified by numbers from 0 to 6: Sunday = 0, Monday = 1, Tuesday = 2, Wednesday = 3, Thursday = 4, Friday = 5, Saturday = 6. To specify several consequent days of a week, enter their numbers separate by commas. Example: for Sunday, Monday, and Tuesday, enter 0,1,2

Working with System Configuration - Gaia Clish

You can save your Gaia system configuration settings as a ready-to-run a 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.

To save the system configuration to a CLI script, run:

```
save configuration <Name of Script>
```

To restore configuration settings, run:

```
load configuration <Name of Script>
```

To see the latest configuration settings, run:

```
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>
```

Advanced Configuration

In This Section:

Configuring the Gaia Portal Web Server 350
Resetting the Expert Mode Password on a Security Gateway 351

Configuring the Gaia Portal Web Server

Description

Configure the server responsible for the Gaia Portal.

Syntax

- To configure Gaia Portal web server:

```
set web
      daemon-enable {on | off}
      session-timeout <Timeout>
      ssl-port <Port>
      ssl3-enabled {on | off}
      table-refresh-rate <Rate>
```

- To show the Gaia Portal web server configuration:

```
show web
      daemon-enable
      session-timeout
      ssl-port
      ssl3-enabled
      table-refresh-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. • **Range:** on, or `off` • **Default:** on
`session-timeout <Timeout>`	Configures the time (in minutes), after which the HTTPS session to the Gaia Portal terminates. • **Range:** `1 - 720` • **Default:** `15`

Parameter	Description
`ssl-port <Port>`	Configures the TCP port number, on which the Gaia Portal can be accessed over HTTPS. • **Range:** `1 - 65535` • **Default:** `443` Use this command for initial configuration only. 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. **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 will have to change the URL used to access the Gaia Portal from `https://<Hostname or IP Address>/` to `https://<Hostname or IP Address>:<PORTNUMBER>`
`ssl3-enabled {on | off}`	Enables or disables the HTTPS SSLv3 connection to Gaia Portal. • **Range:** `on`, or `off` • **Default:** `off`
`table-refresh-rate <Rate>`	Configures the refresh rate (in seconds), at which some tables in the Gaia Portal are refreshed. • **Range:** `10 - 240` • **Default:** `10`

Resetting the Expert Mode Password on a Security Gateway

If you forget your Expert mode password for a Security Gateway or Cluster Member, follow sk106490 http://supportcontent.checkpoint.com/solutions?id=sk106490.

CPUSE - Software Updates

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 relevant 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 once 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 http://supportcontent.checkpoint.com/solutions?id=sk92449.