QUANTUM

28 October 2024

GAIA

R80.40

Administration Guide

CHECK POINT™

Check Point Copyright Notice

© 2020 - 2024 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 for a list of our trademarks.

Refer to the Third Party copyright notices 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.

Certifications

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

Check Point R80.40

For more about this release, see the R80.40 home page.

Latest Version of this Document in English

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

Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
28 October 2024	Updated: ■ *"Hardware Diagnostics" on page 461* - removed the Expert mode command "`diagMain`" because it is not supported.
30 April 2024	Updated: ■ *"Introduction to the Gaia Portal" on page 19*
17 April 2024	Updated: ■ *"Configuring Cloning Groups in Gaia Portal" on page 216*
13 March 2024	Updated: ■ *"Configuring SNMP in Gaia Clish" on page 246* ■ *"Configuring SNMP in Gaia Portal" on page 236*
17 August 2023	Added a new section: ■ *"Hardware Diagnostics" on page 461*
16 August 2023	Added a new section: ■ *"Appendix" on page 504*
12 July 2023	Added a new section: ■ *"Configuring SSH Authentication with RSA Key Files" on page 370*
05 July 2023	Added a new topic: ■ *"Getting Started" on page 31*
20 June 2023	Updated: ■ *"Authentication Servers" on page 374*
16 April 2023	Updated: ■ *"Configuring System Logging in Gaia Clish" on page 290* ■ *"Configuring System Logging in Gaia Portal" on page 286*
10 April 2023	Updated: ■ *"Advanced Gaia Configuration" on page 485*

Date	Description
03 April 2023	Updated: ■ *"Restoring a Factory Default Image on Check Point Appliance" on page 453*
27 March 2023	Updated: ■ *"Configuring Cloning Groups in Gaia Portal" on page 216*
30 January 2023	Updated: ■ *"Backing Up and Restoring the System" on page 467* ■ *"Configuring Scheduled Backups" on page 477* ■ *"Proxy" on page 204*
18 January 2023	Updated: ■ *"Backing Up and Restoring the System" on page 467* ■ *"Configuring Scheduled Backups" on page 477*
12 January 2023	Updated: ■ *"Working with Snapshot Management in Gaia Portal" on page 447* ■ *"Working with Snapshot Management in Gaia Clish" on page 450* ■ *"System Backup" on page 466* ■ *"Backing Up and Restoring the System" on page 467*
08 January 2023	Updated: ■ *"Configuring Gaia as a TACACS+ Client" on page 391*
14 November 2022	Updated: ■ *"Download SmartConsole" on page 454*

Date	Description
11 August 2022	Updated: ■ *"Expert Mode" on page 49* ■ *"Configuring Bond Interfaces in Gaia Clish" on page 113* ■ *"Configuring Job Scheduler in Gaia Portal" on page 259* ■ *"Configuring Job Scheduler in Gaia Clish" on page 262* ■ *"Snapshot Prerequisites" on page 446* ■ *"Working with Snapshot Management in Gaia Portal" on page 447* ■ *"Working with Snapshot Management in Gaia Clish" on page 450* ■ Improved the term from "slave interface(s)" to "subordinate interface (s)" Added: ■ *"Running Check Point Commands in Shell Scripts" on page 491*
16 June 2022	In the HTML version, added glossary terms in the text.
24 May 2022	Updated: ■ *"Expert Mode" on page 49* ■ *"Managing User Accounts in Gaia Clish" on page 311* ■ *"Configuring Password Policy in Gaia Portal" on page 353* ■ *"Configuring Password Policy in Gaia Clish" on page 360* ■ *"Monitoring Password Policy in Gaia Clish" on page 369*
28 December 2021	Updated: ■ *"Running the First Time Configuration Wizard in CLI Expert mode" on page 69* ■ *"Configuring SNMP in Gaia Portal" on page 236*
21 November 2021	Updated: ■ *"Managing User Accounts in Gaia Clish" on page 311*
17 October 2021	Updated ■ *"Configuring ARP in Gaia Clish" on page 156* ■ *"Configuring ARP in Gaia Portal" on page 153*
23 June 2021	Updated: ■ *"Working with System Configuration in Gaia Clish" on page 483*

Date	Description
11 May 2021	Added: ■ *"Proxy" on page 204* Updated: ■ *"ARP" on page 152*
20 October 2020	Updated: ■ *"Configuring Bond Interfaces in Gaia Portal" on page 110* ■ *"Configuring Bond Interfaces in Gaia Clish" on page 113* ■ *"NetFlow Export" on page 196*
21 August 2020	Updated: ■ *"Redirecting RouteD System Logging Messages" on page 295*
01 July 2020	Updated: ■ *"Introduction to the Gaia Portal" on page 19* ■ *"Physical Interfaces" on page 90* ■ *"Configuring Bond Interfaces in Gaia Clish" on page 113* ■ *"List of Available Features in Roles" on page 326* ■ *"License Status" on page 440*
15 January 2020	First release of this document

Table of Contents

Gaia Overview ... *18*
Introduction to the Gaia Portal ... *19*
Gaia Portal Overview ... *19*
Working with the Configuration Lock ... *23*
Using the Gaia Portal Interface Elements ... *24*
Toolbar Accessories ... *24*
Search Tool ... *24*
Navigation Tree ... *24*
Status Bar ... *25*
Configuration Tab ... *25*
Monitoring Tab ... *25*
Unsupported Characters and Words ... *26*
System Information Overview ... *27*
Showing System Overview Information in Gaia Portal ... *27*
Showing System Overview Information in Gaia Clish ... *29*
Getting Started ... *31*
Introduction to the Command Line Interface ... *32*
Syntax Legend ... *33*
Command Completion ... *35*
Commands and Features ... *37*
Command History ... *39*
Command Line Movement and Editing ... *41*
Configuration Locks ... *42*
Environment Commands ... *44*
Client Environment Output Format ... *47*
Expert Mode ... *49*
User Defined (Extended) Commands ... *52*

Summary of Gaia Clish Commands ... 54
Configuring Gaia for the First Time ... 56
Running the First Time Configuration Wizard in Gaia Portal ... 57
Running the First Time Configuration Wizard in CLI Expert mode ... 69
Centrally Managing Gaia Device Settings ... 78
Introduction of Gaia Central Management ... 78
Managing Gaia in SmartConsole ... 80
Running Command Scripts ... 80
Understanding One-Time Scripts ... 83
Running Repository Scripts ... 83
Backup and Restore ... 84
Backing up the System ... 85
Restoring the System ... 86
Opening Gaia Portal and Gaia Clish ... 87
Network Management ... 88
Network Interfaces ... 89
Physical Interfaces ... 90
Configuring Physical Interfaces in Gaia Portal ... 91
Configuring Physical Interfaces in Gaia Clish ... 93
Aliases ... 97
Configuring Aliases in Gaia Portal ... 97
Configuring Aliases in Gaia Clish ... 98
VLAN Interfaces ... 100
Configuring VLAN Interfaces in Gaia Portal ... 101
Configuring VLAN Interfaces in Gaia Clish ... 103
Access Mode VLAN and Trunk Mode VLAN ... 106
Bond Interfaces (Link Aggregation) ... 108
Configuring Bond Interfaces in Gaia Portal ... 110
Configuring Bond Interfaces in Gaia Clish ... 113
Making Sure that Bond Interface is Working ... 122

Configuring Bond High Availability in VRRP Cluster ... 125
Bridge Interfaces ... 127
Configuring Bridge Interfaces in Gaia Portal ... 128
Configuring Bridge Interfaces in Gaia Clish ... 129
Accept, or Drop Ethernet Frames with Specific Protocols ... 135
Loopback Interfaces ... 136
Configuring Loopback Interfaces in Gaia Portal ... 137
Configuring Loopback Interfaces in Gaia Clish ... 139
VPN Tunnel Interfaces ... 141
Gaia Management Interface ... 149
Selecting Management Interface in Gaia Portal ... 149
Selecting Management Interface in Gaia Clish ... 150
CLI Reference (interface) ... 151
ARP ... 152
Configuring ARP in Gaia Portal ... 153
Configuring ARP in Gaia Clish ... 156
DHCP Server ... 158
Configuring a DHCP Server in Gaia Portal ... 159
Configuring a DHCP Server in Gaia Clish ... 162
Hosts and DNS ... 168
System Name ... 169
Configuring Host Name and Domain Name in Gaia Portal ... 169
Configuring Host Name and Domain Name in Gaia Clish ... 169
Hosts ... 170
Configuring Hosts in Gaia Portal ... 170
Configuring Hosts in Gaia Clish ... 171
DNS ... 173
Configuring DNS in Gaia Portal ... 173
Configuring DNS in Gaia Clish ... 175
IPv4 Static Routes ... 177

Configuring IPv4 Static Routes in Gaia Portal ... 178
Configuring IPv4 Static Routes in Gaia Clish ... 183
IPv6 Static Routes ... 188
Configuring IPv6 Static Routes in Gaia Portal ... 188
Configuring IPv6 Static Routes in Gaia Clish ... 190
Troubleshooting ... 194
Configuring IPv6 Neighbor Entries ... 195
NetFlow Export ... 196
Introduction ... 196
Configuration Options in Gaia Portal ... 198
Configuration Options in Gaia Clish ... 198
Configuration Procedure ... 201
System Management ... **203**
Proxy ... 204
Proxy for Gaia Operating System ... 204
Proxy for Check Point Servers ... 204
Security Gateway as an HTTP/HTTPS Proxy ... 204
Configuring Proxy in Gaia Portal ... 205
Configuring Proxy in Gaia Clish ... 207
Time ... 208
Configuring the Time and Date in Gaia Portal ... 209
Configuring the Time and Date in Gaia Clish ... 210
Cloning Group ... 215
Configuring Cloning Groups in Gaia Portal ... 216
Configuring Cloning Groups in Gaia Clish ... 223
Cloning Group Modes ... 223
CLI Syntax ... 224
SNMP ... 231
Introduction ... 231
SNMP v3 - User-Based Security Model (USM) ... 233

Enabling SNMP ... 233
SNMP Agent Address ... 233
SNMP Traps ... 234
Configuring SNMP in Gaia Portal ... 236
Configuring SNMP in Gaia Clish ... 246
Interpreting SNMP Error Messages ... 254
SNMP PDU ... 254
GetRequest ... 256
GetNextRequest ... 256
GetBulkRequest ... 257
Job Scheduler ... 258
Configuring Job Scheduler in Gaia Portal ... 259
Configuring Job Scheduler in Gaia Clish ... 262
Mail Notification ... 267
Introduction ... 267
Configuring Mail Notification in Gaia Portal ... 268
Configuring Mail Notification in Gaia Clish ... 269
Messages ... 270
Comparison ... 270
Configuring Messages in Gaia Portal ... 270
Configuring Messages in Gaia Clish ... 271
Limits ... 274
Display Format ... 275
Configuring Display Format in Gaia Portal ... 275
Configuring Display Format in Gaia Clish ... 276
Session ... 277
Configuring the Session in Gaia Portal ... 277
Configuring the Session in Gaia Clish ... 277
Core Dumps ... 278
Introduction ... 278

Configuring Core Dumps in Gaia Portal ... 278
Configuring Core Dumps in Gaia Clish ... 280
System Configuration ... 282
Configuring IPv6 Support in Gaia Portal ... 283
Configuring IPv6 Support in Gaia Clish ... 283
System Logging ... 285
Configuring System Logging in Gaia Portal ... 286
Configuring System Logging in Gaia Clish ... 290
Redirecting RouteD System Logging Messages ... 295
Configuring Log Volume ... 299
Network Access ... 300
Introduction ... 300
Configuring Telnet Access in Gaia Portal ... 300
Configuring Telnet Access in Gaia Clish ... 300
Host Access ... 301
Configuring Allowed Gaia Clients in Gaia Portal ... 301
Configuring Allowed Gaia Clients in Gaia Clish ... 302
Advanced Routing ... **303**
User Management ... **304**
Change My Password ... 305
Changing My Password in Gaia Portal ... 305
Changing My Password in Gaia Clish ... 305
Users ... 306
Managing User Accounts in Gaia Portal ... 307
Managing User Accounts in Gaia Clish ... 311
Roles ... 316
Configuring Roles in Gaia Portal ... 317
Configuring Roles in Gaia Clish ... 321
List of Available Features in Roles ... 326
List of Available Extended Commands in Roles ... 346

Password Policy ... 350
Configuring Password Policy in Gaia Portal ... 353
Procedure ... 353
Password Strength ... 354
Password History ... 355
Mandatory Password Change ... 356
Denying Access to Unused Accounts ... 357
Denying Access After Failed Login Attempts ... 358
Password Hashing Algorithm ... 359
Configuring Password Policy in Gaia Clish ... 360
Password Strength ... 360
Password History ... 362
Mandatory Password Change ... 363
Denying Access to Unused Accounts ... 365
Denying Access After Failed Login Attempts ... 366
Configuring Hashing Algorithm ... 368
Monitoring Password Policy in Gaia Clish ... 369
Configuring SSH Authentication with RSA Key Files ... 370
Prerequisites ... 370
Procedure ... 370
Authentication Servers ... 374
Configuring RADIUS Servers ... 376
Configuring RADIUS Servers in Gaia Portal ... 376
Configuring RADIUS Servers in Gaia Clish ... 378
Configuring Gaia as a RADIUS Client ... 381
Configuring RADIUS Servers for Non-Local Gaia Users ... 382
Configuring TACACS+ Servers ... 385
Configuring TACACS+ Servers in Gaia Portal ... 385
Configuring TACACS+ Servers in Gaia Clish ... 388
Checking if the Logged In User is Enabled for TACACS+ ... 390

Configuring Gaia as a TACACS+ Client ... 391
Configuring TACACS+ Servers for Non-Local Gaia Users ... 394
System Groups ... 395
Introduction ... 395
Configuring System Groups in Gaia Portal ... 396
Configuring System Groups in Gaia Clish ... 398
GUI Clients ... 400
Configuring GUI Clients in Gaia Portal ... 400
Configuring GUI Clients in Command Line ... 401
High Availability ... **402**
Understanding VRRP ... 402
VRRP Terminology ... 403
VRRP on Gaia OS ... 404
VRRP Configuration Methods ... 405
Monitoring of VRRP Interfaces ... 406
How VRRP Failover Works ... 406
Typical VRRP Use Cases ... 408
Preparing a VRRP Cluster ... 411
Configuring Network Switches ... 411
Preparing VRRP Cluster Members ... 411
Configuring Global Settings for VRRP ... 412
Configuring Monitored Circuit/Simplified VRRP ... 414
Configuring Monitored Circuit/Simplified VRRP in Gaia Portal ... 414
Configuring Monitored Circuit/Simplified VRRP in Gaia Clish ... 418
Configuring the VRRP Cluster for Simplified VRRP in SmartConsole ... 422
Configuring Advanced VRRP ... 423
Changing from Advanced VRRP to Monitored Circuit/Simplified VRRP ... 423
Configuring Advanced VRRP in Gaia Portal ... 424
Configuring Advanced VRRP in Gaia Clish ... 428
Configuring the VRRP Cluster for Advanced VRRP in SmartConsole ... 434

Troubleshooting VRRP ... 435
Traces (Debug) for VRRP ... 435
General Configuration Considerations ... 437
Firewall Policies ... 437
Monitored-Circuit VRRP in Switched Environments ... 437
Maintenance ... **439**
License Status ... 440
On Check Point Appliances ... 440
On Open Servers and Virtual Machines ... 440
Activating a License in Gaia Portal ... 441
Snapshot Management ... 444
Snapshot Options ... 445
Snapshot Prerequisites ... 446
Working with Snapshot Management in Gaia Portal ... 447
Working with Snapshot Management in Gaia Clish ... 450
Restoring a Factory Default Image on Check Point Appliance ... 453
Download SmartConsole ... 454
Hardware Health Monitoring ... 455
Showing Hardware Health Information in Gaia Portal ... 455
Showing Hardware Health Information in Gaia Clish ... 456
Showing Hardware Information ... 458
Hardware Diagnostics ... 461
Introduction ... 461
Requirement ... 461
Running the tool through the LCD (recommended) ... 461
Running the tool over the Console connection (recommended) ... 461
Limitations ... 462
Monitoring RAID Synchronization ... 463
Showing RAID Information in Gaia Portal ... 463
Showing RAID Information in Command Line ... 463

Shut Down ... 465
Rebooting and Shutting Down in Gaia Portal ... 465
Rebooting and Shutting Down in Gaia Clish ... 465
System Backup ... 466
Backing Up and Restoring the System ... 467
Excluding Files from the Gaia Backup ... 468
Backing Up and Restoring the System in Gaia Portal ... 471
Backing Up the System in Gaia Clish ... 474
Restoring the System in Gaia Clish ... 476
Configuring Scheduled Backups ... 477
Configuring Scheduled Backups in Gaia Portal ... 478
Configuring Scheduled Backups in Gaia Clish ... 480
Working with System Configuration in Gaia Clish ... 483
Advanced Gaia Configuration ... ***485***
Configuring the Gaia Portal Web Server ... 485
Resetting the Expert Mode Password on a Security Gateway ... 487
Configuring Supported SSH Ciphers, MACs, and KexAlgorithms ... 487
CPUSE - Software Updates ... ***490***
Running Check Point Commands in Shell Scripts ... ***491***
On a Security Management Server / Log Server / SmartEvent Server ... 491
On a Multi-Domain Server / Multi-Domain Log Server ... 492
On a Security Gateway / Cluster Members (non-VSX) ... 492
On a VSX Gateway / VSX Cluster Members ... 493
Glossary ... ***494***
Appendix ... ***504***

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.

Gaia API:

See sk143612 and *Check Point Gaia API Reference*.

Introduction to the Gaia Portal

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

Gaia Portal Overview

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

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

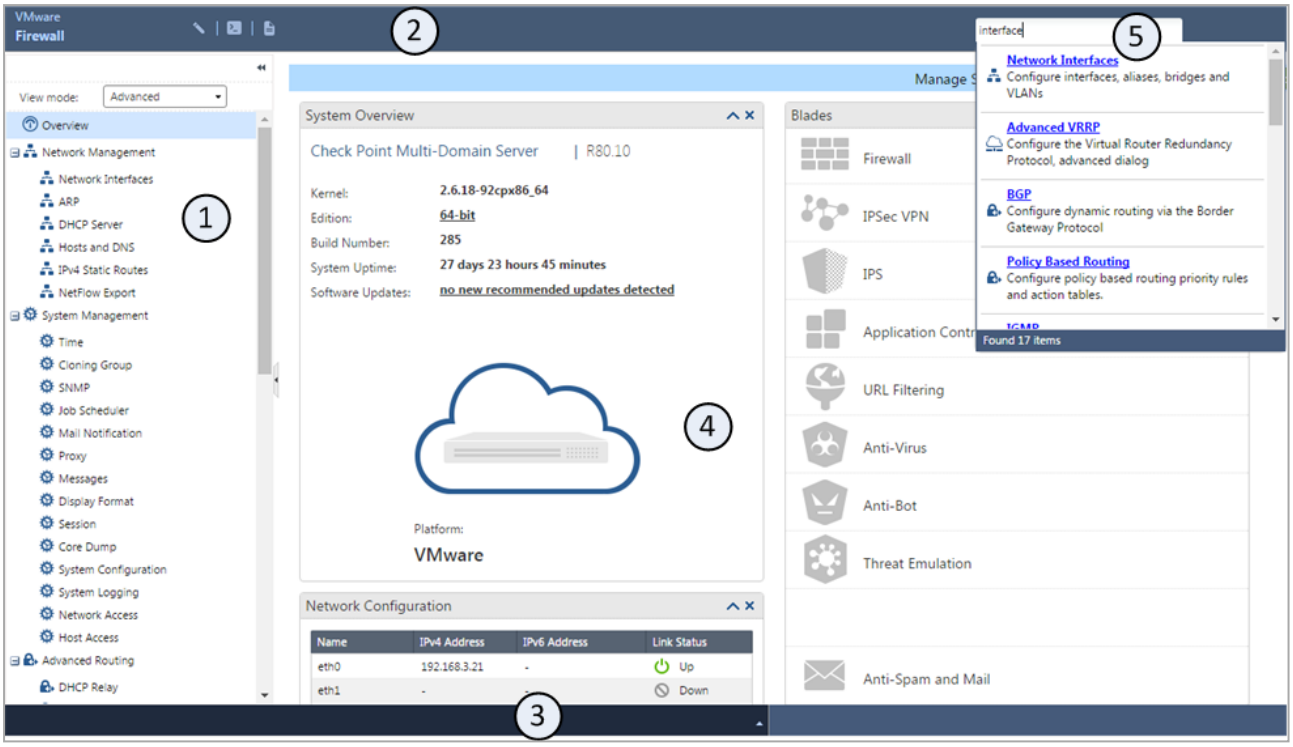
- Easy Access - Simply connect with a web browser to:

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

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

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

The Gaia Portal interface



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

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

Logging in to the Gaia Portal

To log in to the Gaia Portal:

Step	Instructions
1	Enter this URL in your browser: `https://<IP Address of Gaia Management Interface>`
2	Enter your user name and password.

Important:

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

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

  - **SmartView Web Application**

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

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

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

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

Logging out from the Gaia Portal

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

Working with the Configuration Lock

Only one user can have Read/Write access to Gaia configuration settings at a time. All other users can log in with Read-Only access to see configuration settings, as specified by their assigned roles (see *"Roles" on page 316*).

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

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

Overriding a configuration lock in the Gaia Portal

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

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

Using the Gaia Portal Interface Elements

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

Toolbar Accessories

You can use these toolbar icons to do these tasks

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

Unsupported Characters and Words

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

Unsupported Characters

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

Unsupported Words

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

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

System Information Overview

In This Section:

Showing System Overview Information in Gaia Portal 27
Showing System Overview Information in Gaia Clish 29

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

Showing System Overview Information in Gaia Portal

The **Overview** page shows status widgets.

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

Widgets

Widget	Description
System Overview	System information, including: ■ Installed product (for example: Check Point Security Management Server, Check Point Security Gateway) ■ Product version number (for example: R80.40) ■ 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.

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

Showing System Overview Information in Gaia Clish

You can use these commands to show system status:

The "show uptime" command

Description

Shows how long the Gaia system is up and running.

Syntax

```
show uptime
```

The "show version" command

Description

Shows the name and versions of the Gaia OS components.

Syntax

- To show the full system version information:

```
show version all
```

- To show version information for OS components:

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

- To show name of the installed product:

```
show version product
```

Parameters

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

Getting Started

1. Install the Gaia OS.

   See the *R80.40 Installation and Upgrade Guide*.

2. Run the Gaia First Time Configuration Wizard.

   See *"Configuring Gaia for the First Time" on page 56*.

3. Configure the required interfaces:

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

      See *"Physical Interfaces" on page 90*.

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

      See *"Network Interfaces" on page 89*.

4. Configure the required DNS settings.

   See *"Hosts and DNS" on page 168*.

5. Configure the required IPv4 and IPv6 static routes.

   See:

   - *"IPv4 Static Routes" on page 177*
   - *"IPv6 Static Routes" on page 188*

6. Configure the required Proxy Server.

   See *"Proxy" on page 204*.

7. Configure the required Roles.

   See *"Roles" on page 316*.

8. Configure the required Users.

   See *"Users" on page 306*.

9. Configure the required Password Policy.

   See *"Password Policy" on page 350*.

10. Install the required license.

    See *"License Status" on page 440*.

11. Install the applicable software updates.

    See *"CPUSE - Software Updates" on page 490*.

Introduction to the Command Line Interface

This chapter introduces the Gaia command line interface.

The default Gaia shell is called `clish`.

Using the Gaia Clish

Step	Instructions
1	Connect to the Gaia platform using one of these options: ■ In SmartConsole (see *"Centrally Managing Gaia Device Settings" on page 78*). ■ 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 the configuration changes

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

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

```
save config
```

Syntax Legend

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

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

Character	Description

TAB	Shows the available nested subcommands:
	`main command`
	`→ nested subcommand 1`
	`→ → nested subsubcommand 1-1`
	`→ → nested subsubcommand 1-2`
	`→ nested subcommand 2`
	Example:
	`cpwd_admin`
	`config`
	`-a <options>`
	`-d <options>`
	`-p`
	`-r`
	`del <options>`
	Meaning, you can run only **one** of these commands:
	■ This command: `cpwd_admin config -a <options>`
	■ Or this command: `cpwd_admin config -d <options>`
	■ Or this command: `cpwd_admin config -p`
	■ Or this command: `cpwd_admin config -r`
	■ Or this command: `cpwd_admin del <options>`

Curly brackets or braces **{ }**	Enclose a list of available commands or parameters, separated by the vertical bar **|**. User can enter only one of the available commands or parameters.

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

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`

Press ...	To do this ...

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

UP arrow DOWN arrow	Browse the command history.
LEFT arrow RIGHT arrow	Edit the command.
Enter	Run the command. 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 Clish commands are organized into groups of related features, with a basic syntax:

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

See *"Summary of Gaia Clish Commands" on page 54*.

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.

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

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

  ```
  show commands
  ```

- To see a list of all features, run:

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

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

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

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

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

- To see all operations, run:

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

At the *More* prompt:

To see the next page, press <SPACE>.

To see the next line, press <ENTER>.

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

Command History

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.

Word Designator	Meaning
`^`	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 (see *"Roles" on page 316*).

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.

The "lock database" and "lock database" commands

Description

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

Syntax

```
lock database override
unlock database
```

Comments

- Use these commands with caution.

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

The "config-lock" commands

Description

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

Syntax

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

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

Parameters

Parameter	Description
`off`	Turns off the configuration lock.
`on`	Turns on the configuration lock. 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.

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 <Number of Rows>
      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 locks the configuration when invoked. Otherwise, it continues without a configuration lock. When the configuration is locked by Gaia Clish, no configuration changes are possible in Gaia Portal, until the lock is released.
`debug {0-6}`	Debug level. 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`.
`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. The default is `pretty`. See *"Client Environment Output Format" on page 47*.
`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 <Number of Rows>`	Number of rows to show in your terminal window. If the window size is changed, the number of rows also changes, unless the value is set to 0 (zero).

Parameter	Description
`syntax-check {on | off}`	Put the shell into syntax-check mode. 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. In addition, see sk144112.

- 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** supported to run the corresponding command in Expert mode.
For example, to work with interfaces, Gaia Clish provides the commands "`show interface`" and "`set interface`".
Therefore, it is **not** supported to run the `ifconfig` command in the Expert mode.

Note - There is **no** default password for the Expert mode. You must configure a password for the Expert mode before you can use it.

Description

The Expert mode password protects the Expert shell against unapproved 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 to configure an Expert mode password in plain text

```
set expert-password
```

The password must contain at least 6 characters and a maximum of 30 characters.

Syntax to configure an Expert mode password as a salted hash

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

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

Parameters

Parameter	Description
`hash <Hash String>`	The password as an MD5, SHA256, or SHA512 salted hash instead of plain text (the password string must contain at least 6 characters). Use this option when you upgrade or restore using backup scripts. You can generate the hash of the password with the "`cpopenssl`" command (run: `cpopenssl passwd -help`). To configure the default hash algorithm, see: ■ *"Password Hashing Algorithm" on page 359* (in Gaia Portal) ■ *"Configuring Hashing Algorithm" on page 368* (in Gaia Clish) **Best Practice** - Do **not** use MD5 hash because it is not secure. **Notes:** ■ Format: `$<Hash Standard>$<Salt>$<Encrypted>` ■ The length of this hash string must be less than 128 characters. ■ *<Hash Standard>* One of these digits: • `1` = MD5 • `5` = SHA256 • `6` = SHA512 ■ *<Salt>* A string of these characters: `a-z A-Z 0-9 . / [ ] _ ` ^` The length of this string must be between 2 and 16 characters. ■ *<Encrypted>* A string of these characters: `a-z A-Z 0-9 . / [ ] _ ` ^` The length of this string must be: • For MD5, less than 22 characters. • For SHA256, less than 43 characters. • For SHA512, less than 86 characters.

Example

```
gaia> set expert-password
Enter current expert password: *******
Enter new expert password: *****
Enter new expert password (again): *****
Password is only 5 characters long; it must be at least 6
characters in length.
Enter new expert password: ******
Enter new expert password (again): ******
Password is not complex enough; try mixing more different kinds
of characters (upper case, lower case, digits, and punctuation).
Enter new expert password: *******
Enter new expert password (again): *******

gaia> save config
```

User Defined (Extended) Commands

Description

Manage user defined (extended) commands in Gaia Clish.

Extended commands include:

1. Built in extended commands.

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

2. User defined commands.

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

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

Syntax

- To show all extended commands:

  ```
  show extended commands
  ```

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

  ```
  show command <Command>
  ```

- To add an extended command:

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

- To delete an extended command:

  ```
  delete command <Command>
  ```

Parameters

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

See *"List of Available Extended Commands in Roles" on page 346*.

Example

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

Step	Instructions
1	To add the *free* command: `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.
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.

To show the list of all available Gaia Clish commands:

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

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

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

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

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

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

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

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

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

Configuring Gaia for the First Time

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

You can run the First Time Configuration Wizard in:

- Gaia Portal
- CLI Expert mode

Running the First Time Configuration Wizard in Gaia Portal

To start the Gaia First Time Configuration Wizard:

Step	Instructions
1	Connect a computer to the Gaia computer. 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://<IP address of Gaia Management Interface>`
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 R80.40 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 applies the initial deployment configuration that includes different OS version on the appliance. You must prepare the initial deployment configuration with the Zero Touch Cloud Service. For more information, see sk116375.

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 applicable IPv4 address.
Subnet mask	Enter the applicable IPv4 subnet mask.
Default Gateway	Enter the IPv4 address of the applicable default gateway.
Configure IPv6	Select how the Gaia Management Interface gets its IPv6 address: ■ **Manually** - You configure the IPv6 settings in the next fields. ■ **Off** - None.
IPv6 Address	Enter the applicable IPv6 address.
Mask Length	Enter the applicable IPv6 mask length.
Default Gateway	Enter the IPv6 address of the applicable default gateway.

Internet Connection window

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

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

Date and Time Settings window

In this window, you configure the date and time settings 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.
Multi-Domain Server	Select this option to install: ■ A Multi-Domain 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.

Field	Description
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.
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.

Field	Description
Multi-Domain Log Server	Select this option to install a dedicated single Multi-Domain Log Server.

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

Dynamically Assigned IP window

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

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 applicable 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.

The **Improve product experience** section:

- By default, the option **Send data to Check Point** is enabled. For information about this option, see sk111080.
- By default, the option **Send crash data to Check Point that might contain personal data** is disabled.

  If you enable this option, Gaia operating system uploads the detected core dump files to Check Point Cloud.

  Check Point R&D can analyze the crashes and issue fixes for them.

Notes:

- At the end of the First Time Configuration Wizard, the Gaia computer reboots and the initialization process is performed in the background for several minutes.
- If you installed the Gaia computer as a Security Management Server or Multi-Domain Server, only read-only access is possible with SmartConsole during this initialization time.
- To make sure the configuration is finished:
  1. Connect to the command line on the Gaia computer.
  2. Log in to the Expert mode.
  3. Check that the bottom section of the `/var/log/ftw_install.log` file contains one of these sentences:
     - `installation succeeded`
     - `FTW: Complete`

     Run:

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

Example outputs:

- From a Security Gateway or Cluster Member:

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

- From a Security Management Server or a Standalone:

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

- From a Multi-Domain Server:

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

Running the First Time Configuration Wizard in CLI Expert mode

Description

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

Notes:

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

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	Instructions

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, run the "`config_system -h`" command.

2	Reboot the system.

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

Step	Instructions
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	Instructions
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 the "`config_system --help`" command to see the available parameters.

Table: The 'config_system' parameters

Parameter	Description	Valid values
`install_security_gw`	Installs Security Gateway, if its value is set to "`true`".	■ `true` ■ `false`
`gateway_daip`	Configures the Security Gateway as Dynamic IP (DAIP) Security Gateway, if its value is 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 its value is set to "`true`".	■ `true` ■ `false`
`install_security_managment`	Installs a Security Management Server or a dedicated Log Server, if its value is set to "`true`".	■ `true` ■ `false`
`install_mgmt_primary`	Makes the installed Security Management Server the Primary one. **Notes** : ■ Can only be set to "`true`", if the value of the "`install_mgmt_secondary`" parameter is set to "`false`". ■ To install a dedicated Log Server, the value of this parameter must be set to "`false`".	■ `true` ■ `false`
`install_mgmt_secondary`	Makes the installed Security Management Server a Secondary one. **Notes**: ■ Can only be set to "`true`", if the value of the "`install_mgmt_primary`" parameter is set to "`false`". ■ To install a dedicated Log Server, the value of this parameter must be set to "`false`".	■ `true` ■ `false`

Table: The 'config_system' parameters (continued)

Parameter	Description	Valid values
`install_mds_primary`	Makes the installed Security Management Server the Primary Multi-Domain Server. **Note** - The value of the "`install_security_managment`" parameter must be set to "`true`".	■ `true` ■ `false` **Note** - Can only be set to "`true`", if the value of the "`install_mds_secondary`" parameter is set to "`false`".
`install_mds_secondary`	Makes the installed Security Management Server a Secondary Multi-Domain Server. **Note** - The value of the "`install_security_managment`" parameter must be set to "`true`".	■ `true` ■ `false` **Note** - Can only be set to "`true`", if the value of the "`install_mds_primary`" parameter is set to "`false`".
`install_mlm`	Installs Multi-Domain Log Server, if its value is 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 its value is set to "`true`". For more information, see sk94508. **Best Practice** - We highly recommended you enable this optional parameter.	■ `true` ■ `false`
`upload_info`	Uploads data that helps Check Point provide you with optimal services, if its value is set to "`true`". For more information, see sk94509. **Best Practice** - We highly recommended you enable this optional parameter.	■ `true` ■ `false`

Table: The 'config_system' parameters (continued)

Parameter	Description	Valid values
`mgmt_admin_radio`	Configures Management Server administrator. **Note** - You must specify this parameter, if you install a Management Server.	■ Set the value to "`gaia_admin`", if you wish to use the Gaia "`admin`" account. ■ Set the value to "`new_admin`", if you wish to configure a new administrator account.
`mgmt_admin_name`	Configures the management administrator's username. **Note** - You must specify this parameter, if the value of the "`install_security_managment`" parameter is set to "`true`".	A string of alphanumeric characters.
`mgmt_admin_passwd`	Configures the management administrator's password. **Note** - You must specify this parameter, if the value of the "`install_security_managment`" parameter is set to "`true`".	A string of alphanumeric characters.
`mgmt_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 the value of the "`mgmt_gui_clients_radio`" parameter is set to "`range`".	Single IPv4 address of a host. Example: `192.168.0.10`
`mgmt_gui_clients_last_ip_field`	Specifies the last address of the range, if the value of the "`mgmt_gui_clients_radio`" parameter is set to "`range`".	Single IPv4 address of a host. Example: `192.168.0.20`
`mgmt_gui_clients_ip_field`	Specifies the network address, if the value of the "`mgmt_gui_clients_radio`" parameter is set to "`network`".	IPv4 address of a network. Example: `192.168.0.0`

Table: The 'config_system' parameters (continued)

Parameter	Description	Valid values
`mgmt_gui_clients_subnet_field`	Specifies the netmask, if the value of the "`mgmt_gui_clients_radio`" parameter is set to "`network`".	A number from 1 to 32.
`mgmt_gui_clients_hostname`	Specifies the netmask, if value of the "`mgmt_gui_clients_radio`" parameter is set to "`this`".	Single IPv4 address of a host. Example: `192.168.0.15`
`ftw_sic_key`	Configures the Secure Internal Communication key, if the value of the "`install_security_managment`" parameter is set to "`false`".	A string of alphanumeric characters (between 4 and 127 characters long).
`admin_hash`	Configures the 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 its value is set to "`manually`".	■ `manually` ■ `off`
`ipaddr_v4`	Configures the IPv4 address of the management interface.	Single IPv4 address.
`masklen_v4`	Configures the IPv4 mask length for the management interface.	A number from 0 to 32.
`default_gw_v4`	Specifies IPv4 address of the default gateway.	Single IPv4 address.
`ipstat_v6`	Turns static IPv6 configuration on, if its value is set to "`manually`".	■ `manually` ■ `off`
`ipaddr_v6`	Configures the IPv6 address of the management interface.	Single IPv6 address.

Table: The 'config_system' parameters (continued)

Parameter	Description	Valid values
`masklen_v6`	Configures the 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`	Configures the name of the local host (optional).	A string of alphanumeric characters.
`domainname`	Configures the domain name (optional).	Fully qualified domain name. Example: `somedomain.com`

`timezone`	Configures 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 this command (names of Areas and Regions are case-sensitive):
		`set timezone Area` *<SPACE><TAB>*

`ntp_primary`	Configures the IP address of the primary NTP server (optional).	IPv4 address.
`ntp_primary_version`	Configures the NTP version of the primary NTP server (optional).	■ `1` ■ `2` ■ `3` ■ `4`
`ntp_secondary`	Configures the IP address of the secondary NTP server (optional).	IPv4 address.

Table: The 'config_system' parameters (continued)

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

Centrally Managing Gaia Device Settings

In This Section:

Introduction of Gaia Central Management 78
Managing Gaia in SmartConsole 80
Running Command Scripts 80
Understanding One-Time Scripts 83
Running Repository Scripts 83
Backup and Restore 84
Opening Gaia Portal and Gaia Clish 87

Introduction of Gaia Central Management

SmartConsole lets you:

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

  A compressed `.tgz` backup file captures the Gaia OS configuration and the Security Gateway database.
- Do maintenance operations:
  - By opening the Gaia Portal or command shell from SmartConsole
  - By fetching settings from the device, or by pushing settings to the device
- Examine recent tasks:

The **Recent Tasks** tab, located in the bottom section of SmartConsole, shows recent Gaia Security Gateway management tasks done using SmartConsole.

- Run command line scripts on the Security Gateway.

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

  Double-click the task to see the complete output.

- Receive notification on local device configuration change

  The **Status** column in the **Gateways** view indicates changes in the device configuration

- Implement configuration changes without a full policy install (**Push Settings to Device** action)

- Automate the configuration of Cloning Groups and synchronization between the members

Managing Gaia in SmartConsole

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

Running Command Scripts

One Time scripts

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

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

To run a one-time script

Step	Instructions
1	Right-click the Security Gateway.
2	Select **Scripts > Run One Time Script**.
3	The **Run One Time Script** window opens 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 Security Gateways are not part of a Cloning Group, you can run a script on multiple Security Gateways at the same time.

To run a Repository script

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

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

Understanding One-Time Scripts

If you specify a script:

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

Running Repository Scripts

You can run a predefined script from the script repository.

To run a script from the repository

Step	Instructions
1	In the **Gateways & Servers** view, right-click the Security Gateways or Security Management Servers, on which you want to run scripts.
2	Select **Scripts** > **Scripts Repository**. 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 SmartConsole session before you perform a system backup operation.

To back up the system

Step	Instructions
1	In the **Gateways & Servers** view, right-click the Security Gateway object you want to back up.
2	Select **Actions** > **System Backup**. 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	Instructions
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

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

To open a command line window on the Security Gateway

Step	Instructions
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	Instructions
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

This chapter includes configuration procedures for:

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

Network Interfaces

Gaia supports these network interface types:

- 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 in the Security Gateway or Cluster object, the incorrect topology is shown. If this occurs, run the "`cpstop`" and then the "`cpstart`" commands on the Security Gateway or Cluster Members.

Physical Interfaces

In This Section:

Configuring Physical Interfaces in Gaia Portal *91*

Configuring Physical Interfaces in Gaia Clish *93*

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

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

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

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

To add or remove an interface card

Step	Instructions
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 in Gaia Portal

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

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

To configure a physical interface

Step	Instructions
1	In the navigation tree, click **Network Management** > **Network Interfaces**.
2	Select an interface from the list and click **Edit**.
3	Select the **Enable** option to set the interface status to UP.
4	In the **Comment** field, enter the applicable comment text (up to 100 characters).
5	On the **IPv4** tab, do one of these: ■ 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 and reboot (see *"System Configuration" on page 282*). R80.40 does not support IPv6 Address on Gaia Management Interface (Known Limitation 01622840).

Step	Instructions
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 configuration procedure, see the *R80.40 Installation and Upgrade Guide* > Chapter *Special Scenarios for Security Gateways* > Section *Deploying a Security Gateway in Monitor Mode*.
8	Click **OK**.

Configuring Physical Interfaces in Gaia Clish

Syntax

To configure an interface

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

To show all configured settings of all interfaces

```
show interfaces all
```

To show all configured settings of a specific interface

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

To show the specific configured setting of a specific interface

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

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

Parameters

CLI Parameters

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

Parameter	Description
`auto-negotiation {on | off}`	Configures automatic negotiation of interface link speed and duplex settings: ■ `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>`	Configures the IPv4 address.
`ipv6-address <IPv6 Address>`	Configures the IPv6 address. **Important** - First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 282*). R80.40 does not support IPv6 Address on Gaia Management Interface (Known Limitation 01622840).
`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 and reboot (see *"System Configuration" on page 282*).

Parameter	Description
`link-speed {10M/half | 10M/full | 100M/half | 100M/full | 1000M/full | 1000M/full}`	Configures the interface link speed and duplex status. Available speed and duplex combinations are: ■ `10M/half` ■ `10M/full` ■ `100M/half` ■ `100M/full` ■ `1000M/full` ■ `10000M/full`
`mac-addr <MAC Address>`	Configures the hardware MAC address.
`monitor-mode {on | off}`	Configures Monitor Mode on this interface: ■ `on` - Enabled ■ `off` - Disabled **Default:** `off` For configuration procedure, see the *R80.40 Installation and Upgrade Guide* > Chapter *Special Scenarios for Security Gateways* > Section *Deploying a Security Gateway in Monitor Mode*.
`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 the receive buffer size. ■ **Range:** 0 - 4096 bytes ■ **Default:** Depends on the interface driver
`state {on | off}`	Configures the interface state: ■ `on` - Enabled ■ `off` - Disabled

Parameter	Description
`tx-ringsize <0-4096>`	Configures the transmit 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 1400
gaia> set interface eth2 state on
gaia> set interface eth2 link-speed 100M/full
```

Aliases

In This Section:

Configuring Aliases in Gaia Portal 97
Configuring Aliases in Gaia Clish 98

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

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

Notes:

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

Configuring Aliases in Gaia Portal

Adding an interface alias

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

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

Deleting an interface alias

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

Configuring Aliases in Gaia Clish

Syntax

Adding an alias

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

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

Viewing the configured aliases

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

Deleting an alias

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

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

Parameters

CLI Parameters

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

Example

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

VLAN Interfaces

In This Section:

Configuring VLAN Interfaces in Gaia Portal 101
Configuring VLAN Interfaces in Gaia Clish 103
Access Mode VLAN and Trunk Mode VLAN 106

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

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

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

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

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

Notes:

- The name of a VLAN interface in Gaia is "`<Name of Physical Interface>.<VLAN ID>`".
  For example, the name of a VLAN interface with a VLAN ID of 5 on a physical interface `eth1` is "*eth1.5*".
- The VLAN tunnel is not secure, because it is not encrypted.

Configuring VLAN Interfaces in Gaia Portal

To add a VLAN interface

Step	Instructions
1	In the navigation tree, click **Network Management** > **Network Interfaces**.
2	Make sure that the physical interface, on which you add a VLAN interface, does not have an IP address.
3	Click **Add** > **VLAN**.
4	In the **Add VLAN** window, select the **Enable** option to set the VLAN interface to UP.
5	On the **IPv4** tab, enter the IPv4 address and subnet mask. You can optionally select the **Obtain IPv4 address automatically** option.
6	**Optional:** 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 and reboot (see *"System Configuration" on page 282*).
7	On the **VLAN** tab, enter or select a **VLAN ID** (VLAN tag) between 2 and 4094.
8	In the **Member Of** field, select the applicable physical interface.
9	Click **OK**.

To edit a VLAN interface

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

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

To delete a VLAN interface

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

Configuring VLAN Interfaces in Gaia Clish

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

Syntax

To add a new VLAN interface

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

To configure a VLAN interface

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

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

To show the configuration of a specific VLAN interface

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

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

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

CLI Parameters

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

Parameter	Description
`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.
`<VLAN ID>`	Configures the ID of the VLAN interface (integer between 2 and 4094).
`<IPv4 Address>`	Assigns the IPv4 address.
`<IPv6 Address>`	Assigns the IPv6 address. **Important** - First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 282*).
`subnet-mask <Mask>`	Configures the IPv4 subnet mask using the dotted decimal notation (X.X.X.X) - integer between 2 and 32..
`mask-length <Mask Length>`	Configures the IPv6 subnet mask length using CIDR notation (/xx) - integer between 1 and 128.
`ipv6-autoconfig {on | off}`	Configures if this interface gets an IPv6 address from a DHCPv6 Server: ■ `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 and reboot (see *"System Configuration" on page 282*).
`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
`state {on | off}`	Configures interface's state: ■ `on` - Enabled ■ `off` - Disabled

Example

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

Access Mode VLAN and Trunk Mode VLAN

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

Access Mode VLAN

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

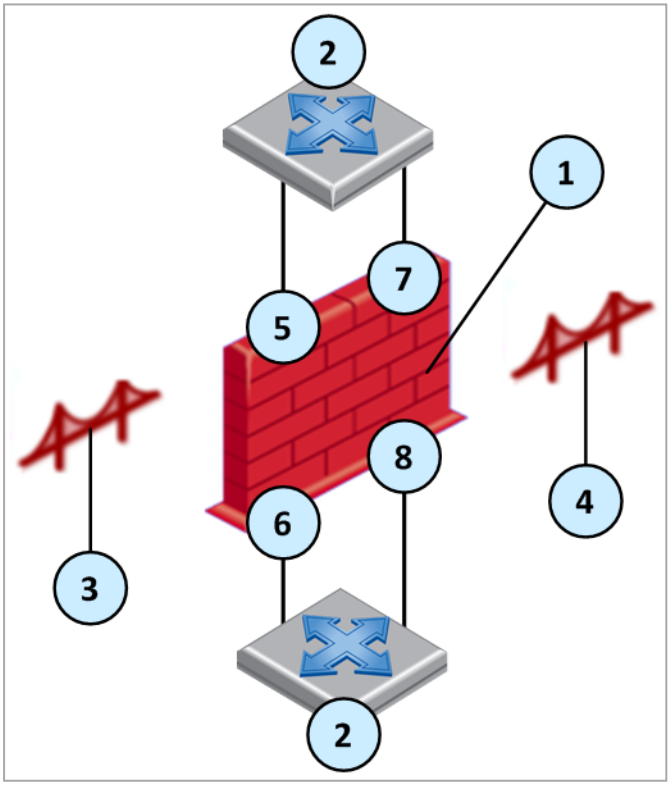
For **VLAN translation**, use different numbered VLAN interfaces to create the Bridge interface.

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

1. Configure two VLAN interfaces.
2. Create a Bridge interface and select the VLAN interfaces as its subordinate interfaces (see *"Bridge Interfaces" on page 127*).

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

Example topology:



Item	Description
1	Security Gateway

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

Trunk Mode VLAN

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

To configure a Bridge interface with VLAN trunk, create the Bridge interface with two physical (non-VLAN) interfaces as its subordinate interfaces (see *"Bridge Interfaces" on page 127*).

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

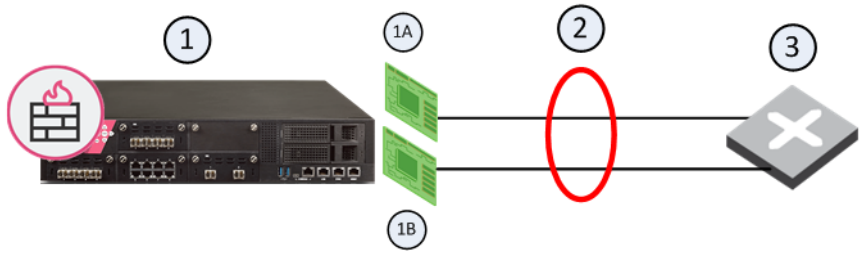
The traffic passes with the original VLAN tag to its destination.

Note - VLAN translation is not supported in Trunk mode.

Bond Interfaces (Link Aggregation)

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

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



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

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

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

- **High Availability (Active/Backup)**: Gives redundancy when there is an interface or a link failure. This strategy also supports switch redundancy. Bond High Availability works in **Active/Backup** mode - interface Active/Standby mode. When an Active subordinate interface is down, the connection automatically fails over to the primary subordinate interface. If the primary subordinate interface is not available, the connection fails over to a different subordinate interface.
- **Load Sharing (Active/Active)**: All subordinate interfaces in the UP state are used simultaneously. Traffic is distributed among the subordinate interfaces to maximize throughput. Bond Load Sharing does not support switch redundancy.

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

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

  - **Round Robin** - Selects the Active subordinate interfaces sequentially.
  - **802.3ad** (LACP) - Dynamically uses Active subordinate interfaces to share the traffic load. This mode uses the LACP protocol, which fully monitors the interface link between the Check Point Security Gateway and a switch.
  - **XOR** - All subordinate interfaces in the UP state are Active for Load Sharing. Traffic is assigned to Active subordinate interfaces based on the transmit hash policy: Layer 2 information (XOR of hardware MAC addresses), or Layer 3+4 information (IP addresses and Ports).

For Bonding High Availability mode and for Bonding 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 *R80.40 Release Notes*.
- Up to 8 physical subordinate interfaces can be configured in a single bond interface.

Configuring Bond Interfaces in Gaia Portal

Step	Instructions
1	In the navigation tree, click **Network Management** > **Network Interfaces**.
2	Make sure that the subordinate interfaces, which you wish to add to the Bond interface, do not have IP addresses.
3	For a new bond interface, select **Add** > **Bond**. 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 and reboot (see *"System Configuration" on page 282*).
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 subordinate interfaces from the **Available Interfaces** list and then click **Add**. **Note** - Make sure that the subordinate interfaces do not have any IP addresses or aliases configured. c. Select an **Operation Mode**: ■ **Round Robin** (default) - Bond uses all subordinate interfaces sequentially (High Availability + Load Sharing). ■ **Active-Backup** - Bond uses one subordinate interface at a time (High Availability). ■ **XOR** - Bond uses subordinate interfaces based on a hash function (High Availability + Load Sharing). ■ **802.3ad** - Dynamic bonding according to IEEE 802.3ad (Load Sharing).

Step	Instructions
7	On the **Advanced** tab: a. Configure the required **MTU** for your network (if not sure, leave the default value). b. Configure the **Monitor Interval** - How much time to wait between checking each subordinate interface for link-failure. The valid range is 1-5000 ms. The default is 100 ms. c. Configure the **Down Delay** - How much time to wait, after sending a monitor request to a subordinate interface, before bringing down the subordinate interface. The valid range is 1-5000 ms. The default is 200 ms. d. Configure the **Up Delay** - How much time to wait, after sending a monitor request to a subordinate interface, before bringing up the subordinate interface. The valid range is 1-5000 ms. The default is 200 ms.
8	Additional configuration settings are available depending on the selected Bond Operation Mode: ■ If you selected the **Round Robin** bond operation mode, then there are no additional configuration settings. ■ If you selected the **Active-Backup** bond operation mode, then select the **Primary Interface**. By default, the first subordinate interface added to the bond group, becomes the primary. **Important** - You must **not** configure the primary subordinate interface explicitly in ClusterXL when you configure the Sync interface on a bonding group for redundancy. For more information, see the *R80.40 ClusterXL Administration Guide* > Chapter *ClusterXL Requirements and Compatibility* > Section *Supported Topologies for Synchronization Network*. ■ If you selected the **XOR** bond operation mode, then select the **Transmit Hash Policy** - the algorithm for subordinate interface selection according to the specified TCP/IP Layer. 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 you selected the **802.3ad** bond operation mode, then perform these two steps: a. Select the **Transmit Hash Policy** - the algorithm for subordinate 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). b. 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**.

Note - The name of a Bond interface in Gaia is "`bond<`*`Bond Group ID`*`>`". For example, the name of a bond interface with a Bond Group ID of 5 is "*bond5*".

Configuring Bond Interfaces in Gaia Clish

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

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

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

Note - You configure an IP address on a Bonding Group in the same way as you do on a physical interface (see *"Physical Interfaces" on page 90*).

Syntax

Adding a new Bonding Group

Syntax

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

Example

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

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

Adding a new subordinate interface to an existing Bonding Group

Syntax

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

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

Example

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

Notes:

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

Configuring an existing Bonding Group

Syntax

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

Configuring the Bond Operating Mode

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

Syntax

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

Example

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

Notes:

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

Configuring the Up Delay Time

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

Syntax

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

Example

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

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

Configuring the Down Delay Time

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

Syntax

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

Example

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

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

Configuring the Media Monitoring Interval

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

Syntax

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

Example

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

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

Configuring an IP address on the existing Bonding Group

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

For more information, see *"Configuring Physical Interfaces in Gaia Clish" on page 93*.

Deleting a subordinate interface from an existing Bonding Group

Syntax

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

Example

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

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

Deleting the bonding group

Syntax

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

Example

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

Notes:

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

Viewing the Bonding Group configuration

Syntax

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

Parameters

CLI Parameters

Parameter	Description
<Bond Group ID>	Configures the Bond Group ID. ■ **Range:** 0 - 1024 ■ **Default:** No default value
<Name of Subordinate Interface>	Specifies the name of the subordinate physical interface, which you add to (or remove from) the bond group. Make sure that the subordinate interfaces do not have any IP addresses or aliases configured.
`mode` *<Mode>*	Configures the Bond operating mode (see *"Bond Interfaces (Link Aggregation)" on page 108*): ■ `round-robin` Bond uses all subordinate interfaces sequentially (High Availability + Load Sharing). This is the default mode. ■ `active-backup` Bond uses one subordinate interface at a time (High Availability) ■ `xor` Bond uses subordinate interfaces based on a hash function (High Availability + Load Sharing) ■ `8023AD` Dynamic bonding according to IEEE 802.3ad - LACP (Load Sharing)

Parameter	Description
`primary <Name of Subordinate Interface>`	Specifies the name of the *primary* subordinate interface in the bond. By default, the first subordinate interface added to the bond group, becomes the primary. **Important** - You must **not** configure the primary subordinate interface explicitly in ClusterXL when you configure the Sync interface on a bonding group for redundancy. For more information, see the *R80.40 ClusterXL Administration Guide* > Chapter *ClusterXL Requirements and Compatibility* > Section *Supported Topologies for Synchronization Network*. **Note** - Applies only to the Active-Backup bond mode.
`up-delay <0-5000>`	Specifies the time in milliseconds to wait before enabling a subordinate interface after link recovery was detected. ■ **Range:** 0 - 5000 ms ■ **Default:** 200 ms
`down-delay <0-5000>`	Specifies the time in milliseconds to wait before disabling a subordinate interface after link failure was detected. ■ **Range:** 0 - 5000 ms ■ **Default:** 200 ms
`lacp-rate {fast | slow}`	Specifies the Link Aggregation Control Protocol (LACP) packet transmission rate: ■ `slow`- LACPDU packets are sent every 30 seconds ■ `fast`- LACPDU packets are sent every second **Note** - Applies only to the 802.3AD bond mode.
`mii-interval <1-5000>`	Specifies the time in milliseconds to wait before checking the link on subordinate interfaces for a failure. ■ **Range:** 1 - 5000 ms ■ **Default:** 100 ms

Parameter	Description
`xmit-hash-policy {layer2 | layer3+4}`	Specifies the algorithm to use for assigning the traffic to Active subordinate interfaces: ▪ `layer2` - Based on the XOR of hardware MAC addresses ▪ `layer3+4` - Based on the IP addresses and Ports **Note** - Applies only to the XOR and the 802.3AD bond modes.

Examples

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

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

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

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

Making Sure that Bond Interface is Working

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

Example 1 - output for Bond Operating Mode "Round Robin"

```
[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 2 - output for Bond Operating Mode "Active-Backup"

```
[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 3 - output for Bond Operating Mode "XOR"

```
[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 4 - output for Bond Operating Mode "802.3ad"

```
[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]#
```

Configuring Bond High Availability in VRRP Cluster

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

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

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

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

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

Setting the value of the kernel parameter temporarily

Important - This change does not survive reboot.

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

Setting the value of the kernel parameter permanently

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

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

Bridge Interfaces

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

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

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

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 OS supports bridge interfaces that implement native, Layer 2 bridging.
- Gaia OS does **not** support Spanning Tree Protocol (STP) bridges.
- A subordinate interface that is a part of a bond interface cannot be a part of a bridge interface.

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

Configuring Bridge Interfaces in Gaia Portal

Note - For additional information, see the *R80.40 Installation and Upgrade Guide* > Chapter *Special Scenarios for Security Gateways* > Section *Deploying a Security Gateway or a ClusterXL in Bridge Mode*.

Step	Instructions
1	In the left navigation tree, click **Network Management** > **Network Interfaces**.
2	Make sure that the subordinate interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned.
3	Click **Add** > **Bridge**. 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 subordinate interfaces do not have any IP addresses or aliases configured. ■ Do **not** select the interface that you configured as Gaia Management Interface. ■ A Bridge interface in Gaia can contain only two subordinate interfaces.
6	On the **IPv4** tab, enter the IPv4 address and subnet mask. You can optionally select the **Obtain IPv4 Address automatically** option.
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 and reboot (see *"System Configuration" on page 282*).
8	Click **OK**.

Note - The name of a Bridge interface in Gaia is "`br<Bridge Group ID>`". For example, the name of a bridge interface with a Bridge Group ID of 5 is "*br5*".

Configuring Bridge Interfaces in Gaia Clish

Note - For additional information, see the *R80.40 Installation and Upgrade Guide* > Chapter *Special Scenarios for Security Gateways* > Section *Deploying a Security Gateway or a ClusterXL in Bridge Mode*.

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

Note - You configure an IP address on a Bridging Group in the same way as you do on a physical interface (see *"Physical Interfaces" on page 90*).

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Log in to Gaia Clish.

3	Make sure that the subordinate interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned:
	`show interface <Name of Subordinate Interface> ipv4-address`
	`show interface <Name of Subordinate Interface> ipv6-address`

4	Add a new bridging group: `add bridging group <Bridge Group ID 0 - 1024>` **Note** - Do **not** change the state of bond interface manually using the "`set interface <Bridge Group ID> state`" command. This is done automatically by the bridging driver.

5	Add subordinate interfaces to the new bridging group:
	`add bridging group <Bridge Group ID> interface <Name of First Subordinate Interface>`
	`add bridging group <Bridge Group ID> interface <Name of Second Subordinate Interface>`
	Notes:
	■ Do **not** select the interface that you configured as Gaia Management Interface.
	■ Only Ethernet, VLAN, and Bond interfaces can be added to a bridge group.
	■ A Bridge interface in Gaia can contain only two subordinate interfaces.

Step	Instructions

6	Assign an IP address to the bridging group.
	Note - You configure an IP address on a Bridging Group in the same way as you do on a physical interface (see *"Physical Interfaces" on page 90*).
	■ To assign an IPv4 address, run:
	`set interface <Name of Bridging Group> ipv4-address <IPv4 Address> {subnet-mask <Mask> | mask-length <Mask Length>}`
	You can optionally configure the bridging group to obtain an IPv4 Address automatically.
	■ To assign an IPv6 address, run:
	`set interface <Name of Bridging Group> ipv6-address <IPv6 Address> mask-length <Mask Length>`
	You can optionally configure the bridging group to obtain an IPv6 Address automatically.
	Important - First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 282*).

7	Save the configuration: `save config`

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

Syntax

To add a new bridging group

Syntax

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

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

To add a new subordinate interface to an existing bridging group

Syntax

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

Example

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

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

To add a fail-open interface to an existing bridging group

Syntax

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

To configure an existing Bridging Group

Syntax

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

Example

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

To delete a subordinate interface from an existing bridging group

Syntax

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

Example

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

To delete a fail-open interface from the bridging group

Syntax

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

To delete the bridging group

Syntax

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

Notes:

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

Example

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

To show the subordinate interfaces of an existing bridging group

Syntax

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

To show the configured bridging groups

Syntax

```
show bridging groups
```

Parameters

CLI Parameters

Parameter	Description
<Bridge Group ID>	Configures the Bridge Group ID. ■ **Range:** 0 - 1024 ■ **Default:** No default value
<Name of Bridge Interface>	Configures the name of the Bridge interface.
<Name of Subordinate Interface>	Specifies a physical subordinate 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 and reboot (see *"System Configuration" on page 282*).
subnet-mask *<Mask>*	Configures the IPv4 subnet mask using dotted decimal notation (X.X.X.X).
mask-length *<Mask Length>*	Configures the IPv4 or IPv6 subnet mask length using the CIDR notation (integer between 2 and 32).

Parameter	Description
`ipv6-autoconfig {on | off}`	Configures if this interface gets an IPv6 address from a DHCPv6 Server: ■ `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 and reboot (see *"System Configuration" on page 282*).
`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
`rx-ringsize <0-4096>`	Configures the receive buffer size. ■ **Range:** 0 - 4096 bytes ■ **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
```

Accept, or Drop Ethernet Frames with Specific Protocols

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

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

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

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

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

Step	Instructions
1	Connect to the command line on the Security Gateway (each Cluster Member).
2	Log in to the Expert mode.
3	Backup the current `/etc/rc.d/init.d/network` file: `cp -v /etc/rc.d/init.d/network{,_BKP}`
4	Edit the current `/etc/rc.d/init.d/network` file: `vi /etc/rc.d/init.d/network`

5	After the line:
	`./etc/init.d/functions`
	Add this line:
	`/sbin/sysctl -w net.bridge.bpdu_forwarding=0`

6	Save the changes in the file and exit the Vi editor.
7	Reboot the Security Gateway (each Cluster Member).

8	Make sure the new configuration is loaded:
	`sysctl net.bridge.bpdu_forwarding`
	The output must show:
	`net.bridge.bpdu_forwarding = 0`

Loopback Interfaces

In This Section:

Configuring Loopback Interfaces in Gaia Portal 137
Configuring Loopback Interfaces in Gaia Clish 139

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

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

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

Configuring Loopback Interfaces in Gaia Portal

To add a loopback interface

Step	Instructions
1	In the navigation tree, click **Interface Management** > **Network Interfaces**.
2	Click **Add** > **Loopback**.
3	In the **Add loopback** window: 1. The **Enable** option is selected by default to set the loopback interface status to UP. 2. In the **Comment** field, enter the applicable comment text (up to 100 characters). 3. 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 4. On the **IPv6** tab (optional), enter the IPv6 address and mask length. **Important** - First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 282*).
4	Click **OK**.

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

To configure a loopback interface

Step	Instructions
1	In the navigation tree, click **Interface Management** > **Network Interfaces**.
2	Select a loopback interface and click **Edit**.
3	In the **Edit loop<NN>** window: 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	Instructions
1	In the navigation tree, click **Network Management** > **Network Interfaces**.
2	Select a loopback interface and click **Delete**.
3	Click **OK**, when the confirmation message shows.

Configuring Loopback Interfaces in Gaia Clish

Syntax

To add a loopback interface

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

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

To configure a loopback interface

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

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

To show a loopback interface

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

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

To delete a loopback interface

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

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

Parameters

CLI Parameters

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

Parameter	Description
<IPv4 Address>	Specifies the IPv4 address 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
<Mask Length>	Configures the IPv4 subnet mask length using the CIDR notation (integer between 2 and 32)
<Name of Loopback Interface>	Specifies a loopback interface name

Example

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

VPN Tunnel Interfaces

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

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

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

To learn more about Route Based VPN, see the *R80.40 Site to Site VPN Administration Guide* > Chapter *Route Based VPN*.

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

Procedure:

1. Make sure that the IPsec VPN Software Blade is enabled on the applicable Security Gateways.
2. Create and configure the Security Gateways.
3. Configure the VPN community in SmartConsole that includes the two peer Security Gateways.

   Configuring VPN community

   You must configure the VPN Community and add the member Security Gateways to it before you configure a VPN Tunnel Interface. This section includes the basic procedure for defining a Site-to-Site VPN Community. To learn more about VPN communities and their definition procedures, see the *R80.40 Site to Site VPN Administration Guide*.

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

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

4. Make Route Based VPN the default option.

   Do this procedure one time for each.

   Configuring Route Based VPN

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

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

   Configuring an empty group

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

   Configuring the Route Based VPN as the default choice

   Do these steps for each Security Gateway.

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

5. Configure the VTI.

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

   Configuring VTI in Gaia Portal

Step	Instructions
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 ID (example: `vnpt10`). ■ **Remote Peer Name** - Alphanumeric character string as configured for the Remote Peer Name in the VPN community. You must configure the two peers in the VPN community before you can configure the VTI. ■ **VPN Tunnel Type** - Select the applicable type: • **Numbered** - Uses a specified, static IPv4 addresses for local and remote connections. • **Unnumbered** - Uses the interface and the remote peer name to get IPv4 addresses. ■ **Local Address** - Configures the local peer IPv4 address. Applies to the Numbered VTI only. ■ **Remote Address** - Configures the remote peer IPv4 address. Applies to the Numbered VTI only. ■ **Physical Device** - Local peer interface name. Applies to the Unnumbered VTI only.

Configuring VTI in Gaia Clish

Syntax

- To add a VPN Tunnel Interface (VTI):

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

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

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

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

```
show vpn tunnels
```

- To delete a VPN Tunnel Interface (VTI):

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

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

CLI Parameters

Parameter	Description
`<Tunnel ID>`	Configures the unique Tunnel ID (integer from 1 to 99). Gaia automatically adds the prefix '`vpnt`' to the Tunnel ID. Example: `vnpt10`
`type numbered`	Configures a **numbered** VTI that uses static IPv4 addresses for local and remote connections.
`type unnumbered`	Configures an **unnumbered** VTI that uses the interface and the remote peer name to get IPv4 addresses.
`local <Local IP address>`	Configures the VPN Tunnel IPv4 address in dotted decimal format on this Security Gateway or Cluster Member. Applies to the Numbered VTI only.

Parameter	Description
`remote <Remote IP address>`	Configures the VPN Tunnel IPv4 address in dotted decimal format on the VPN peer. Applies to the Numbered VTI only.
`peer <Peer Name`	Specifies the name of the remote peer object as configured in the VPN community in SmartConsole.
`dev <Name of Local Interface>`	Specifies the name of the local interface on this Security Gateway or Cluster Member. The new VTI is bound to this local interface. Applies to the Unnumbered VTI only.

Example

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

6. Configure Route Based VPN Rules.

Configuring Route Based VPN Rules

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

(A) Defining Directional Matching VPN Rules

This section contains the procedure for defining directional matching rules.

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

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

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

The directional rule must contain these directional matching conditions:

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

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

Notes:

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

Enabling the VPN directional matching

Step	Instructions
1	In SmartConsole, click **Menu** > **Global properties**> expand **VPN** > click **Advanced**.
2	Select the **Enable VPN Directional Match in VPN Column** option and click **OK**.
3	From the left navigation panel, click **Gateways & Servers**.
4	For each VPN member gateway: a. Double-click the Security Gateway object. b. From the left tree, click **Network Management**. c. Click **Get Interfaces** > **Get Interfaces with Topology**. This updates the topology to include the newly configured VTIs. d. Click **Accept**. e. Click **OK**.

Configuring a VPN directional matching rule

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

(B) Defining Rules to Allow OSPF Traffic

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

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

To learn about configuring OSPF, see the *R80.40 Gaia Advanced Routing Administration Guide*.

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>1</td><td>In the Gaia Portal or Gaia Clish, add the applicable VPN Tunnel Interfaces to the OSPF configuration page.</td></tr>
<tr><td>2</td><td>In SmartConsole, add an Access Control rule that allows traffic to the VPN community (or all communities) that uses the OSPF service:
<table>
<tr><th>Name</th><th>Source</th><th>Destination</th><th>VPN</th><th>Service</th><th>Action</th></tr>
<tr><td>Allow OSPF for a VPN Community</td><td>Any</td><td>Any</td><td>MyIntranet</td><td>ospf</td><td>Accept</td></tr>
</table>
</td></tr>
</table>

7. Install the policy and test.

Instructions

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

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

Gaia Management Interface

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

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

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

Selecting Management Interface in Gaia Portal

Procedure

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

Selecting Management Interface in Gaia Clish

Syntax

To see the current interface

```
show management interface
```

To select a new interface

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

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

Parameters

CLI Parameters

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

Example

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

CLI Reference (interface)

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

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

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

Description

Add, configure, and delete interfaces and interface properties.

Syntax

To add an interface

```
add interface<ESC><ESC>
```

To configure an interface

```
set interface<ESC><ESC>
```

To show an interface

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

```
show interfaces all
```

To delete an interface, or interface configuration

```
delete interface<ESC><ESC>
```

To work with Gaia Management Interface

```
show management interface
```

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

ARP

The Address Resolution Protocol (ARP) allows a host to find the physical address of a target host on the same physical network using only the target's IP address.

ARP is a low-level protocol that hides the underlying network physical addressing and permits assignment of an arbitrary IP address to every machine.

ARP is considered part of the physical network system and not as part of the Internet protocols.

Configuring ARP in Gaia Portal

To show dynamic ARP entries

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

To show static ARP entries

Step	Instructions
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

Step	Instructions
1	In the navigation tree, click **Network Management** > **ARP**.
2	In the upper right corner, click the **Configuration** tab.
3	In the **ARP Table Settings** section: a. Enter the **Maximum Entries**. This is the maximal number of entries in the ARP cache. **Range:** 1024 - 131072 or 16384 entries ■ 131072 entries - In R80.40 Jumbo Hotfix Accumulator Take 100 and higher ■ 16384 entries - In R80.40 Clean Install, or in the R80.40 Jumbo Hotfix Accumulator Takes lower than 100 **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, resolved dynamic ARP entries are checked for validity. If the entry is not referred to and is not used by traffic before the time elapses, it is marked as STALE. Otherwise, a request is sent to verify the MAC address. **Range:** 60 - 86400 seconds (24 hours) **Default:** 60 seconds

To add a static ARP entry

Step	Instructions
1	In the navigation tree, click **Network Management** > **ARP**.
2	In the upper right corner, click the **Configuration** tab.
3	In the **Static ARP Entries** section, click **Add**.
4	Enter the **IP Address** of the static ARP entry and the **MAC Address** used when forwarding packets to the IP address.
5	Click **OK**.

To delete a static ARP entry

Step	Instructions
1	In the navigation tree, click **Network Management** > **ARP**.
2	In the upper right corner, click the **Configuration** tab.
3	In the **Static ARP Entries** section, select a Static ARP entry.
4	Click **Remove**.

To delete all dynamic ARP entries

Step	Instructions
1	In the navigation tree, click **Network Management** > **ARP**.
2	In the upper right corner, click the **Monitoring** tab.
3	Click **Flush All**.

Configuring ARP in Gaia Clish

Syntax

Adding a static ARP entry

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

Deleting static and dynamic ARP entries

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

Configuring ARP table parameters

```
set arp table
      validity-timeout <Seconds>
      cache-size <Number of Entries>
```

Viewing ARP table parameters

```
show arp
      dynamic all
      static all
      table validity-timeout
      table cache-size
```

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

Parameters

CLI Parameters

Parameter	Description
`static`	Configures static ARP entries.
`dynamic`	Configures dynamic ARP entries.
`ipv4-address <IPv4 Address>`	Configures IPv4 Address for a static ARP entry. ■ **Range:** Dotted-quad ([0-255].[0-255].[0-255].[0-255]) ■ **Default:** No default value

Parameter	Description
`macaddress`	Configures the hardware MAC address (six hexadecimal octets separated by colons) for a static ARP entry. ■ **Range:** 00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF ■ **Default:** No default value
`table validity-timeout <Seconds>`	Configures the time, in seconds, resolved dynamic ARP entries in the ARP cache table are checked for validity. If the entry is not referred to and is not used by traffic before this time elapses, the dynamic ARP entry is marked as STALE. Otherwise, an ARP Request will be sent to verify the MAC address. ■ **Range:** 60 - 86400 seconds (24 hours) ■ **Default:** 60 seconds
`table cache-size <Number of Entries>`	Configures the maximal number of entries in the ARP cache table. **Range:** 1024 - 131072 or 16384 entries ■ 131072 entries - In R80.40 Jumbo Hotfix Accumulator Take 100 and higher ■ 16384 entries - In R80.40 Clean Install, or in the R80.40 Jumbo Hotfix Accumulator Takes lower than 100 **Default:** 4096 entries **Note** - Make sure to configure a value large enough to accommodate at least 100 dynamic ARP entries, in addition to the maximum number of static ARP entries.

DHCP Server

You can configure the Gaia device to be a Dynamic Host Configuration Protocol (DHCP) server.

The DHCP server gives IP addresses and other network parameters to network hosts.

DHCP makes it unnecessary to configure each host manually, and therefore reduces configuration errors.

You configure DHCP server subnets on the Gaia device interfaces.

A DHCP subnet allocates these network parameters to *hosts* behind the Gaia interface:

- IPv4 address
- Default Gateway (optional)
- DNS parameters (optional):
  - Domain name
  - Primary, secondary and tertiary DNS servers

Allocating DHCP parameters to hosts (for the details, see the next section)

Workflow

Step	Instructions
1	To define a DHCP subnet on a Gaia interface: 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 in Gaia Portal

To allocate DHCP parameters to hosts

Step	Instructions
1	In the navigation tree, click **Network Management** > **DHCP Server**.
2	In the **DHCP Server Subnet Configuration** section, click **Add**. 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:
	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** and select the applicable interface. Click **OK**.
	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**.
	Optional: In the **Lease Configuration** section, configure the DHCP lease settings: a. 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. In the **Maximum Lease** field, enter the maximal lease time (in seconds), for host IPv4 addresses. The default is 86,400 seconds.

Step	Instructions
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**.
9	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	Instructions
1	In the navigation tree, click **Network Management** > **DHCP Server**.
2	In the **DHCP Server Subnet Configuration** section, select the Subnet and click **Edit**.
3	Change the applicable settings.
4	Click **OK**.

To disable DHCP server on all interfaces

Step	Instructions
1	In the navigation tree, click **Network Management** > **DHCP Server**.
2	In the **DHCP Server Configuration** section, clear the **Enable DHCP Server**.
3	Click **Apply**.

To delete DHCP subnet

Step	Instructions
1	In the navigation tree, click **Network Management** > **DHCP Server**.
2	In the **DHCP Server Subnet Configuration** section, select the Subnet and click **Delete**.
3	Click **OK** to confirm.

Note - Before you delete the last DHCP subnet, you must disable DHCP server on all interfaces.

Configuring a DHCP Server in Gaia Clish

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 <Default 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

CLI 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.

Parameter	Description
`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 <Default 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

This page lets you configure:

- System Name - Host Name and Domain Name (see *"System Name" on page 169*)
- Hosts (see *"Hosts" on page 170*)
- DNS settings (see *"DNS" on page 173*)

System Name

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

Configuring Host Name and Domain Name in Gaia Portal

Step	Instructions
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 and Domain Name in 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
  ```

- To configure a domain name (optional):

  ```
  set domainname <Domain>
  ```

- To show the configured domain name:

  ```
  show domainname
  ```

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

Hosts

You should add host addresses for systems that communicate frequently with the Gaia system.

You can:

- View the entries in the hosts table.
- Add an entry to the list of hosts.
- Modify the IP address of a host.
- Delete a host entry.

Configuring Hosts in Gaia Portal

To add a static host entry

Step	Instructions
1	In the navigation tree, click **Network Management > Hosts and DNS**.
2	In the **Hosts** section, click **Add**.
3	Enter: ■ **Host Name** - Must include only alphanumeric characters, dashes ('-'), and periods ('.'). Periods must be followed by a letter or a digit. The name may not end with a dash or a period. There is no default value. ■ **IPv4 address** ■ **IPv6 address**

To edit the static host entry

Step	Instructions
1	In the navigation tree, click **Network Management > Hosts and DNS**.
2	In the **Hosts** section, select a host entry and click **Edit**.
3	Edit: ■ **Host Name** ■ **IPv4 address** ■ **IPv6 address**

To delete the static host entry

Step	Instructions
1	In the navigation tree, click **Network Management > Hosts and DNS**.
2	In the **Hosts** section, select a host entry and click **Delete**.

Configuring Hosts in Gaia Clish

Description

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

Syntax

To add a static host entry

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

To edit the static host entry

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

To delete the static host entry

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

To show the configured static host entry

```
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

CLI Parameters

Parameter	Description
`name <Name of Host>`	The name of a static host. Must include only alphanumeric characters, dashes ('-'), and periods ('.'). Periods must be followed by a letter or a digit. The name must not end in a dash or a period. There is no default value.
`ipv4-address <IPv4 Address of Host>`	The IPv4 address of the host.
`ipv6-address <IPv6 Address of Host>`	The IPv6 address of the host.

DNS

Gaia uses the Domain Name Service (DNS) to translate host names into IP addresses.

To enable DNS lookups, you must enter the primary DNS server for your system. You can also enter secondary and tertiary DNS servers.

When the system resolves host names, it consults the primary name server. If a failure or time-out occurs, the system consults the secondary name server, and if necessary, the tertiary.

You can also define a DNS Suffix, which is a search for host-name lookup.

Configuring DNS in Gaia Portal

To configure the DNS Servers

Step	Instructions
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`).

Step	Instructions
3	In the **DNS** section: a. In the **DNS Suffix** field, enter the domain name suffix. Gaia adds 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 you try to ping the host "`foo`" (with the command "`ping foo`"). If Gaia cannot resolve "`foo`", then Gaia tries to resolve "`foo.example.com`". 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 in 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

```
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

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

To delete the DNS servers and the DNS suffix

```
delete dns
      primary
      secondary
      tertiary
      suffix
```

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

Parameters

CLI Parameters

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

Parameter	Description
`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 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 you try to ping the host "`foo`" (with the command "`ping foo`"). If Gaia cannot resolve "`foo`", then Gaia tries to resolve "`foo.example.com`".

IPv4 Static Routes

A static route defines the destination and one or more paths (next hops) to get to that destination.

You define static routes manually in the Gaia Portal, or in Gaia Clish with the "`set static-route`" command.

Static routes let you add paths to destinations that are unknown by dynamic routing protocols. You can define multiple paths (next hops) to a destination and define priorities for selecting a path. Static routes are also useful for defining the default route.

Static route definitions include these parameters:

- Destination IPv4 address.
- Route type:
  - **Normal** - Accepts and forwards packets to the specified destination.
  - **Reject** - Drops packets and sends ICMP *unreachable* packet.
  - **Blackhole** - Drops packets and does not send ICMP *unreachable* packet.
- Next-hop type:
  - **Address** - Identifies the next hop gateway by its IPv4 address.
  - **Logical** - Identifies the next hop gateway by the name of the local interface that connects to it. Use this option only if the next hop gateway has an unnumbered interface.
- Gateway identifier - IPv4 address, or name of local interface.
- Priority (Optional) - Assigns a path priority when there are many different paths.
- Rank (Optional) - Selects a route when there are many routes to a destination that use different routing protocols. You must use the Gaia Clish to configure the rank.

Configuring IPv4 Static Routes in Gaia Portal

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

Configuring One IPv4 Static Route at a Time

Step	Instructions
1	In the navigation tree, click **Network Management** > **IPv4 Static Routes**.
2	In the **IPv4 Static Routes** section, click **Add**. 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, and not send ICMP *unreachable* packet to the traffic source ■ **Reject** - To drop packets, and send ICMP *unreachable* packet to the traffic source
6	In the **Rank** field, leave the default value (60), or enter the relative rank of the IPv4 static route (an integer from 1 to 255). 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.
8	In the **Comment** field, enter the applicable comment text (up to 100 characters).

Step	Instructions
9	Click **Add Gateway** and select one of these options: ■ Option 1: a. Select **IP Address** to specify the next hop by its IPv4 address. b. In the **IPv4 Address** field, enter the IPv4 address of the next hop gateway. c. In the **Priority** field, either do not enter anything, or select an integer between 1 and 8. d. Add **Monitored IPs**. e. Click **OK**. ■ Option 2: a. Select **Network Interface** to specify the next hop by the name of the local interface name that connects to it. b. In the **Local Interface** field, select an interface that connects to the next hop gateway. c. In the **Priority** field, either do not enter anything, or select an integer between 1 and 8. d. Add **Monitored IPs**. e. Click **OK**. **Notes:** ■ *Priority* defines which next hop gateway to select when multiple next hop gateways are configured. The lower the priority, the higher the preference - priority 1 means the highest preference, and priority 8 means the lowest preference. You can define two or more paths with the same priority to specify a backup path with equal priority. A next hop gateway with no priority configured is preferred over a next hop gateway with priority configured. ■ Multihop ping in Static Routes uses ICMP Echo Request to monitor reachability of an IP address multiple hops away. Multihop ping in Static Routes updates the status of an associated next hop in accordance to the reachability status. The next hop status becomes "down", if that IP address is unreachable.
10	If you configured 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 make sure the next hop gateway for a static route is working. Gaia includes in the kernel forwarding table only next hop gateways, which are verified as working. When Ping is enabled, Gaia adds an IPv4 static route to the kernel forwarding table only after at least one next hop gateway is reachable.

Step	Instructions
11	Click **Save**.
12	In the **Advanced Options** section, you can configure the Ping behavior. If you changed the default settings, click **Apply**.

Configuring Many IPv4 Static Routes at Once

You can use the batch mode to configure multiple static routes in one step.

Note - This mode does not allow the configuration of static routes that use a logical interface as the next hop.

Step	Instructions
1	In the navigation tree, click **Network Management** > **IPv4 Static Routes**.
2	In the **Batch Mode** section, click **Add Multiple Static Routes**.
3	In the **Add Multiple Routes** window, select the **Next Hop Type**: ■ **Normal** - To accept and forward packets ■ **Blackhole** - To drop packets, and not send ICMP *unreachable* packet to the traffic source ■ **Reject** - To drop packets, and send ICMP *unreachable* packet to the traffic source

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 / Mask Length).
	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.

Step	Instructions
6	Correct errors and reload the affected routes.
7	In the top right corner, click the **Monitoring** tab to make sure that the routes are configured correctly.

Configuring IPv4 Static Routes in Gaia Clish

Description

Configure, show, and delete IPv4 static routes.

Syntax

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

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}
                  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>
                        {on | off}
                        monitored-ip <Monitored IP Address> {on | off}
                        monitored-ip-option {fail-all | fail-any | force-if-symmetry {on |
off}}
                        [priority <Priority>]
                  logical <Name of Local Interface>
                        {on | off}
                        [priority <Priority>]
            blackhole
            reject
      off
      ping {on | off}
      rank <Rank>
      scopelocal {on | off}
```

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 next hop gateways are configured

```
set static-route <Destination IPv4 Address> nexthop gateway <IPv4 Address of Next Hop Gateway> off
set static-route <Destination IPv4 Address> nexthop gateway <Name of Local Interface> off
```

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

Parameters

CLI Parameters

Parameter	Description
`default`	Defines the default static IPv4 route.
`<Destination IPv4 Address>`	Specifies the IPv4 address of destination host or network using the CIDR notation (IPv4 Address / Mask Length). 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.

Parameter	Description
`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.
`monitored-ip <Monitored IP Address> {on | off}`	Remote IPv4 address to monitor for the next hop gateway. Monitors IP address(es) configured with the "`ip-reachability-detection`". The next hop gateway becomes usable with respect to reachability of IP address(es) reported from the "`ip-reachability-detection`".
`monitored-ip-option {fail-all | fail-any | force-if-symmetry {on | off}}`	Set failure condition and flavor for the configured monitored IP address(es). ■ `fail-all` Fails the next hop gateway when all monitored IP addresses become unreachable. Restores the next hop gateway when one of the monitored IP addresses becomes reachable. Default: `off` ■ `fail-any` Fails the next hop gateway when one of the monitored IP addresses becomes unreachable. Restores the next hop gateway when all monitored IP addresses become reachable. Default: `on` ■ `force-if-symmetry` Ignores IP reachability reports from IP addresses with asymmetric traffic. Default: `off`

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 with the same priority to specify a backup path with equal priority. A next hop gateway with no priority configured is preferred over a next hop gateway with priority configured
`nexthop ... on`	Adds the specified next hop gateway.
`nexthop ... off`	Deletes the specified next hop gateway. If you specify a next hop gateway, only the specified path is deleted. If you do not specify a next hop gateway, the route and all related paths are deleted.
`off`	Removes the static route.

`ping {on | off}`	Enables (`on`) or disables (`off`) the ping of specified next hop gateways for IPv4 static routes.
	The Ping feature sends ICMP Echo Requests to make sure the next hop gateway for a static route is working.
	Gaia includes in the kernel forwarding table only next hop gateways, which are verified as working.
	When Ping is enabled, Gaia adds an IPv4 static route to the kernel forwarding table only after at least one next hop gateway is reachable.
	To configure the ping behavior, run:
	`set ping count <value>`
	`set ping interval <value>`

Parameter	Description
`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>`"
`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.

Example

```
gaia> set static-route 192.0.2.0/24 nexthop gateway address 192.0.2.155 on

gaia> set static-route 192.0.2.0/24 nexthop gateway address 192.0.2.155 off

gaia> set static-route 192.0.2.0/24 nexthop gateway logical eth0 on

gaia> set static-route 192.0.2.0/24 off

gaia> set static-route 192.0.2.100/32 nexthop blackhole

gaia> set static-route 192.0.2.100/32 rank 2

gaia> show route static
  Codes: C - Connected, S - Static, R - RIP, B - BGP,
       O - OSPF IntraArea (IA - InterArea, E - External, N - NSSA)
       A - Aggregate, K - Kernel Remnant, H - Hidden, P - Suppressed

S 0.0.0.0/0 via 192.168.3.1, eth0, cost 0, age 164115
S 192.0.2.100 is a blackhole route
S 192.0.2.240 is a reject route
gaia>
```

IPv6 Static Routes

In This Section:

Configuring IPv6 Static Routes in Gaia Portal *188*

Configuring IPv6 Static Routes in Gaia Clish *190*

Troubleshooting *194*

Important - First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 282*).

Configuring IPv6 Static Routes in Gaia Portal

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

Procedure

Step	Instructions
1	In the navigation tree, click **Network Management** > **IPv6 Static Routes**.
2	In the **IPv6 Static Routes** section, click **Add**.
3	In the **Destination / Mask Length** field, enter the IPv6 address and prefix (default prefix is 64).
4	Select the **Next Hop Type** field select: ■ **Normal** - To accept and forward packets ■ **Blackhole** - To drop packets, and not send 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**.
8	In the **Gateway Address** field, enter the IPv6 address of the next hop gateway.

Step	Instructions
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 gateway when multiple next hop gateways are configured. The lower the priority, the higher the preference - priority 1 means the highest preference, and priority 8 means the lowest preference. A next hop gateway with no priority configured is preferred over a next hop gateway with priority configured. You cannot configure two next hop gateways with the same priority, because IPv6 Equal Cost Multipath Routes are not supported.
10	Click **OK**.
11	Select the **Ping6** option, if you need to monitor next hops for the IPv6 static route using `ping6`. The Ping6 feature sends ICMPv6 Echo Requests to make sure the next hop gateway for a static route is working.
12	Click **Save**.
13	In the **Advanced Options** section, you can configure the Ping6 behavior. If you changed the default settings, you must click **Apply**.

Configuring IPv6 Static Routes in Gaia Clish

Syntax

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

To add or configure the default static IPv6 route

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

To add or configure the 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}
                  interface <Name of Local Interface> [priority <Priority>] {on | off}
            blackhole
            reject
      off
      ping6 {on | off}
      rank <Rank>
```

To show all configured static IPv6 routes

```
show ipv6 route static all
```

To remove the default static IPv6 route

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

To remove the specific static IPv6 route

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

To remove the specific path only, when multiple next hop gateways are configured

```
set ipv6 static-route <Destination IPv6 Address> nexthop gateway <IPv6 Address of Next Hop Gateway> off
```

```
set ipv6 static-route <Destination IPv6 Address> nexthop gateway <Name of Local Interface> off
```

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

Parameters

CLI Parameters

Parameter	Description
`default`	Defines the default static IPv6 route.
`<Destination IPv6 Address>`	Defines the IPv6 address of destination host or network using the CIDR notation (IPv6 Address / Mask Length). 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.

Parameter	Description
`priority <Priority>`	Defines the order for selecting the next hop gateway when multiple next hop gateways are configured. The lower the priority, the higher the preference - priority 1 means the highest preference, and priority 8 means the lowest preference. A next hop gateway with no priority configured is preferred over a next hop gateway with priority configured. You cannot configure two next hop gateways with the same priority, because IPv6 Equal Cost Multipath Routes are not supported.
`nexthop ... on`	Adds the specified next hop gateway.
`nexthop ... off`	Deletes the specified next hop gateway. If you specify a next hop, only the specified path is deleted. If you do not specify a next hop, the route and all related paths are deleted.
`off`	Removes the static route.

`ping6 {on | off}`	Enables (`on`) or disables (`off`) the ping of specified next hop gateways for IPv6 static routes.
	The Ping6 feature sends ICMPv6 Echo Requests to make sure the next hop gateway for a static route is working.
	Gaia includes in the kernel forwarding table only next hop gateways, which are verified as working.
	When Ping6 is enabled, Gaia adds an IPv6 static route to the kernel forwarding table only after at least one next hop gateway is reachable.
	To configure 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>`

Example

```
gaia> set ipv6 static-route 3100:192::0/64 nexthop gateway 3900:172::1 on

gaia> set ipv6 static-route 3100:192::0/64 nexthop gateway 3900:172::1 interface eth3 on

gaia> set ipv6 static-route 3100:192::0/64 nexthop gateway 3900:172::1 priority 3 on

gaia> set ipv6 static-route 3100:192::0/64 nexthop reject

gaia> set ipv6 static-route 3100:192::0/64 nexthop blackhole

gaia> set ipv6 static-route 3100:192::0/64 off

gaia> set ipv6 static-route 3100:192::0/64 nexthop gateway 3900:172::1 off

gaia> set ipv6 static-route 3100:192::0/64 nexthop gateway 3900:172::1 interface eth3 off

gaia> show ipv6 route static
  Codes: C - Connected, S - Static, B - BGP, Rg - RIPng, A - Aggregate,
       O - OSPFv3 IntraArea (IA - InterArea, E - External),
       K - Kernel Remnant, H - Hidden, P - Suppressed

S 3100:55::1/64 is directly connected
S 3200::/64 is a blackhole route
S 3300:123::/64 is a blackhole route
S 3600:20:20:11::/64 is directly connected, eth3
```

Troubleshooting

Scenario - SmartConsole does not let you enable the VPN Software Blade in the Security Gateway object

Symptoms

You cannot enable the VPN Software Blade. SmartConsole shows this message:

```
VPN blade demands gateway's IP address corresponding to the
interface's IP addresses
```

Cause

IPv6 feature is active on the Security Gateway, but the main IPv6 address is not configured in the Security Gateway object in SmartConsole.

Next Steps

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Gateway object.
3. From the left tree, click **General Properties**.
4. Configure the main IPv6 address.
5. Click **OK**.
6. Install the Access Control Policy on the Security Gateway object.

Configuring IPv6 Neighbor Entries

Description

You can add and delete entries in the Gaia IPv6 Neighbor table.

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

Important - First, you must enable the IPv6 Support and reboot (see *"System Configuration" on page 282*).

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

In This Section:

Introduction 196
Configuration Options in Gaia Portal 198
Configuration Options in Gaia Clish 198
Configuration Procedure 201

Introduction

NetFlow is an industry standard for traffic monitoring. Cisco developed this network protocol to collect network traffic patterns and volume.

One host (the NetFlow *Exporter*) sends information about its network flows to a different host (the NetFlow *Collector)*.

A network flow is a unidirectional stream of packets that contain the same set of characteristics.

You can configure Security Gateways and Cluster Members as an Exporter of NetFlow records for all the traffic that passes through.

Note - The state of the SecureXL on a Security Gateway is irrelevant for NetFlow export.

The NetFlow Collector is a different external server, and you configure it separately.

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

- To enable NetFlow, configure at minimum one NetFlow Collector.
- To disable NetFlow, remove all NetFlow Collectors from the Gaia configuration.

You can configure a maxumum of three NetFlow Collectors. Gaia sends the NetFlow records go to all configured NetFlow Collectors. If you configure three NetFlow Collectors, Gaia sends each NetFlow record three times.

Regardless of which NetFlow export format you configure, Gaia exports values as set of fields.

The fields

- Source IP address.
- Destination IP address.
- Source port.
- Destination port.
- Ingress physical interface index (defined by SNMP).
- Egress physical interface index (defined by SNMP).
- Packet count for this flow.
- Byte count for this flow.
- Start of flow timestamp (FIRST_SWITCHED).
- End of flow timestamp (LAST_SWITCHED).
- IP protocol number.
- TCP flags from the flow (TCP only).
- VSX VSID.

Notes:

- The IP addresses and TCP/UDP ports the NetFlow reports are the ones, on which the NetFlow expects to receive traffic.
  Therefore, for NAT connections, the NetFlow reports one of the two directions of the flow with the NATed address.
- NetFlow sends the connection records after the connections terminated.
  If the connections are open for a long time, it can take time for the NetFlow to sends the records.

For more information, see sk102041.

Configuration Options in Gaia Portal

To configure and edit the NetFlow settings, navigate to the **Network Management** section > **NetFlow Export** page.

Configuration Options in Gaia Clish

Syntax

- To configure a new NetFlow collector:

```
add netflow collector ip <IPv4 Address of Collector> port
<Destination Port on Collector> [srcaddr <Source IPv4
Address>] export-format {Netflow_V5 | Netflow_V9 | IPFIX}
enable {yes | no}
```

- To change settings of an existing NetFlow collector:

```
set netflow collector
      ip <IPv4 Address of Collector> port <Destination Port
on Collector> export-format {Netflow_V5 | Netflow_V9 |
IPFIX} [srcaddr <Source IPv4 Address>] enable {yes | no}
      for-ip <IPv4 Address of Collector>
            ip <IPv4 Address of Collector> port <Destination
Port on Collector> export-format {Netflow_V5 | Netflow_V9 |
IPFIX} [srcaddr <Source IPv4 Address>] enable {yes | no}
            for-port <Destination Port on Collector> ip
<IPv4 Address of Collector> port <Destination Port on
Collector> export-format {Netflow_V5 | Netflow_V9 | IPFIX}
[srcaddr <Source IPv4 Address>] enable {yes | no}
```

- To show the configured NetFlow collectors:

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

- To delete a configured NetFlow collector:

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

CLI Parameters

Parameter	Description
`ip <IPv4 Address of Collector>`	Specifies the destination IPv4 address of the NetFlow Collector, to which Gaia sends the NetFlow packets. This parameter is mandatory.
`port <Destination Port on Collector>`	Specifies the destination UDP port number on the NetFlow Collector, on which the collector listens. This parameter is mandatory. There is no default or standard port number for NetFlow.
`srcaddr <Source IPv4 Address>`	**Optional:** Specifies the source IPv4 address of the NetFlow packets. This must be an IPv4 address of the local host. The default is an IPv4 address of the network interface, from which Gaia sends the NetFlow packets. We recommend the default.

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

Configuration Procedure

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

1. **Configure the NetFlow Export settings in Gaia**

   You can configure these settings in Gaia Portal, or in Gaia Clish.

   Configuring the NetFlow settings in Gaia Portal

   a. In the left navigation tree, click **Network Management** > **NetFlow Export**.

   b. In the **Collectors** section, click **Add**.

   c. Enter the required data for each collector:

Parameter	Description
IP Address	The destination IPv4 address, to which Gaia sends the NetFlow packets. This parameter is mandatory.
UDP Port Number	The destination UDP port number, on which the collector listens. This parameter is mandatory. There is no default or standard port number for NetFlow.
Export Format	The NetFlow protocol version to use: ■ **Netflow_V5** - Protocol NetFlow v5 ■ **Netflow_V9** - Protocol NetFlow v9 ■ **IPFIX** - Known as protocol "NetFlow v10" Each protocol version has a different packet format. The default is **Netflow_V9**.
Source IP address	**Optional:** The source IPv4 address of the NetFlow packets. This must be an IPv4 address of the local host. The default is an IPv4 address of the network interface, from which Gaia sends the NetFlow packets. We recommend the default.
Enable	Select this option to enable the configured NetFlow Collector.

   d. Click **OK**.

Configuring the NetFlow settings in Gaia Clish

Configure a new NetFlow collector:

```
add netflow collector ip <IPv4 Address of Collector> port
<Destination Port on Collector> [srcaddr <Source IPv4
Address>] export-format {Netflow_V5 | Netflow_V9 | IPFIX}
enable {yes | no}
```

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

2. **In SmartConsole, configure the explicit Access Control rule**

   a. From the left navigation panel, click **Security Policies**.

   b. Open the applicable policy.

   c. In the top left corner, click **Access Control** > **Policy**.

   d. Add an explicit rule for the traffic that you wish to export with NetFlow:

   Important - In the **Track** column, you must select **Log** and **Accounting**.

Source	Destination	VPN	Services & Applications	Content	Action	Track
Source Host or Network objects	Destination Host or Network objects	*Any	Applicable service objects	* Any	Accept	Log Accounting

   e. Publish the SmartConsole session.

   f. Install the Access Control policy on the Security Gateway or Cluster object.

System Management

This chapter includes procedures and reference information for:

- Time and Date
- Cloning Groups
- SNMP
- Job Scheduler
- Mail Notification
- Login Messages
- Session in Gaia Portal and Gaia Clish
- Core Dump Files
- System Logging
- Network Access over Telnet
- GUI Clients for Security Management Server

Proxy

Proxy for Gaia Operating System

If this Gaia server connects to a network through a proxy server, then configure the applicable proxy server.

Note - This proxy configuration applies only to the Gaia Operating System. It does not apply to Software Blades.

Proxy for Check Point Servers

If your Management Server / Security Gateway/ Cluster connects to Check Point servers to download updates and connect to ThreatCloud through a proxy server, you can configure the proxy server settings in SmartConsole:

Location in SmartConsole	Description
Menu > **Global properties** > **Proxy**	This proxy configuration applies to the Management Server and all managed Security Gateways and Clusters.
Management Server / Security Gateway / Cluster object properties > **Network Management** > **Proxy**	This proxy configuration overrides the global proxy configuration in SmartConsole.

Note - This proxy configuration applies only to Check Point Software Blades that run on top of the Gaia Operating System.

Security Gateway as an HTTP/HTTPS Proxy

You can configure a Security Gateway or Cluster as an HTTP/HTTPS Proxy. See the *R80.40 Quantum Security Gateway Guide* > Chapter "HTTP/HTTPS Proxy".

Configuring Proxy in Gaia Portal

To configure a proxy server

Step	Instructions
1	With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
2	Click **System Management > Proxy**.
3	Select **Use a Proxy server**.
4	Enter the applicable proxy server IP address or hostname.
5	Enter the applicable proxy server port.
6	Click **Apply**.

To edit an existing proxy server configuration

Step	Instructions
1	With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
2	Click **System Management > Proxy**.
3	Enter the applicable proxy server IP address or hostname.
4	Enter the applicable proxy server port.
5	Click **Apply**.

To remove an existing proxy server configuration

Step	Instructions
1	With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
2	Click **System Management > Proxy**.

Step	Instructions
3	Clear **Use a Proxy server**.
4	Click **Apply**.

Configuring Proxy in Gaia Clish

Syntax

To configure a proxy server or edit an existing proxy server configuration

```
set proxy address <IP Address or Hostname of the Proxy Server>
port <1-65535>
```

To remove an existing proxy server configuration

```
delete proxy
      address
      all
      port
```

To show an existing proxy server configuration

```
show proxy
      address
      port
```

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

Time

All Security Management Servers, Security Gateways, and Cluster Members must synchronize their system clocks.

This is important for these reasons:

- SIC trust can fail if devices are not synchronized correctly.
- Cluster synchronization requires precise clock synchronization between members.
- SmartEvent Correlation uses time stamps that must be synchronized to approximately one a second.
- To make sure that cron jobs run at the correct time.
- To do certificate validation for applications based on the correct time.

You can use these methods to set the system date and time:

- Network Time Protocol (NTP).
- Manually, in the Gaia Portal, or Gaia Clish.

Network Time Protocol (NTP)

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.

Configuring the Time and Date in Gaia Portal

Configuring the Time and Date manually

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

Configuring the Time and Date automatically with NTP

Step	Instructions
1	In the navigation tree, click **System Management** > **Time**.
2	Click **Set Time and Date**.
3	Click **Set Time and Date automatically using Network Time Protocol (NTP)**.
4	Enter the Hostname or IP address of the primary and (optionally) secondary NTP servers. **Best Practice** - Configure more than one NTP server for redundancy.
5	Select the NTP version for the applicable server.
6	Click **OK**.

Configuring the Time Zone

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

Configuring the Time and Date in Gaia Clish

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

Showing the current system Date and Time

Syntax

```
show clock
```

Example

```
gaia> show clock
Wed Jan  8 15:20:00 2020 GMT+1
gaia>
```

Configuring and showing the Time

Syntax

- To configure the time:

  ```
  set time <Time of the Day>
  ```

- To show the current time:

  ```
  show time
  ```

Parameters

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

Configuring and showing the Date

Syntax

- To configure a date:

  ```
  set date <Date>
  ```

- To configure the configured date:

  ```
  show date
  ```

Parameters

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

Example

To configure the 20th of January 2020, run:

```
gaia> set date 2020-01-20
```

Configuring and showing the Time Zone

Syntax

- To configure the time zone:

```
set timezone <Area> / <Region>
```

Important - The spaces before and after the slash character (/) are mandatory.

- To show the configured time zone:

```
show timezone
```

Parameters

Parameter	Description
<Area>	Continent or geographic area (case sensitive). To see the valid values, press <SPACE> and <TAB>:
<Region>	Region within the specified area (case sensitive). To see the valid values, press <SPACE> and <TAB>:

Examples

```
gaia> set timezone America / Detroit
gaia> set timezone Asia / Tokyo
```

Configuring and showing the NTP

Syntax

- To configure a new NTP server:

```
set ntp
      active {on | off}
      server
            primary <IPv4 address or Hostname of NTP Server>
version {1|2|3|4}
            secondary <IPv4 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 <IPv4 address or Hostname of NTP Server>
```

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.

Parameter	Description
`secondary`	Configures the IP address or Host name of the secondary NTP server. **Best Practice** - Configure more than one NTP server for redundancy.
`version {1|2|3|4}`	Configures the version number of the NTP - 1, 2, 3, or 4. **Best Practice** - 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
```

Cloning Group

A Cloning Group is a collection of Gaia Security Gateways that synchronize their OS configurations and settings for a number of shared features, for example DNS or ARP.

Configuring Cloning Groups in Gaia Portal

Important:
If you change the members of a Gaia Cloning Group with many members down, you are logged out of the Gaia Portal with an incorrect error message:
`Unable to connect to server`
The correct message is:
`An error occurred while applying configuration change to all cloning group members - the operation was successful only for online members.`
This is the normal behavior of the cloning group. This error does not indicate a critical failure.

To create a new Cloning Group

Step	Instructions
1	With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
2	Click **System Management > Cloning Group**.
3	Click **Start Cloning Group Creation Wizard**. The **Cloning Group Creation Wizard** opens.
4	Select **Create a new Cloning Group**. The **New Gaia Cloning Group** window opens. a. In the **Cloning Group Name** field, enter a name for the Cloning Group. b. In the **IP for cloning** field, select an IPv4 address (interface) for synchronizing settings between member Security Gateways. Select an interface on a secure internal network. c. In the **Password** field, 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 d. In the **Confirm Password** field, enter the password again.
5	In the **Shared Features** screen, select features to clone to other members of the Cloning 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.

Step	Instructions
6	Click **Next** for the **Wizard Summary**.
7	Click **Finish**.

List of Shared Features

The features are listed in the same order, in which they are shown in Gaia Portal.

Table: Shared Features in Gaia Portal

Shared Feature	Description
SNMP	Configure SNMP.
Banner Messages	Configure banner messages.
Job Scheduler	Schedule automated tasks that perform actions at a specific time.
DNS	Configure DNS servers.
ARP	Configure static ARP entries and proxy ARP entries, control dynamic ARP entries.
System Logging	Configure system logging settings.
Host Access Control	Configure which hosts are allowed to connect to the cluster devices.
Proxy Settings	Configure proxy settings.
Host Address Assignment	Configure known hosts.
NTP	Configure Network Time Protocol for synchronizing the system's clock over a network.
Password Policy	Configure password and account policies.
Time	Configure the time and date of the system.
Network Access	Configure network access to Gaia.
Display Format	Configure how the system displays time, date and netmask.
Mail Notification	Configure email address, to which Gaia sends mail notifications.
Inactivity timeout	Configure session parameters, such as inactivity timeout.
Users and Roles	Configure users and roles settings.

Table: Shared Features in Gaia Portal (continued)

Shared Feature	Description
Static Routes	Configure static routes.
DHCP Relay	Configure relay of DHCP and BOOTP messages between clients and servers on different IPv4 Networks.
IPv6 DHCP Relay	Configure relay of DHCPv6 messages between clients and servers on different IPv6 Networks.
BGP	Configure dynamic routing via the Border Gateway Protocol.
IGMP	Establish multicast group memberships via the Internet Group Management Protocol.
PIM	Configure Protocol-Independent Multicast.
Static Multicast Routes	Configure static multicast routes.
RIP	Configure IPv4 dynamic routing via the Routing Information Protocol.
RIPng	Configure IPv6 dynamic routing via the Routing Information Protocol.
OSPF	Configure IPv4 dynamic routing via the Open Shortest-Path First v2 protocol.
IPv6 OSPF	Configure IPv6 dynamic routing via the Open Shortest-Path First v3 protocol.
Route Aggregation	Create a supernet network from the combination of networks with a common routing prefix.
Inbound Route Filters	Configure Inbound Route Filters for RIP, OSPFv2, BGP, and OSPFv3 (supports IPv4 and IPv6).
IP Reachability Detection	Configure reachability detection of IP Addresses.
Route Redistribution	Configure advertisement of routing information from one protocol to another (supports IPv4 and IPv6).
Route Map	Configure dynamic routing route maps.

Table: Shared Features in Gaia Portal (continued)

Shared Feature	Description
Prefix Lists and Trees	Configure dynamic routing prefix lists and trees.
Routing Options	Configure protocol ranks and trace (debug) options.
Policy Based Routing	Configure policy based routing (PBR) priority rules and action tables.
Scheduled Backups	Configure Gaia scheduled backups.

To manage a Cloning Group

Step	Instructions
1	Sign out of the Gaia Portal.
2	Sign in *to the same Gaia Portal* using the *cadmin* account and password. (Alternatively, log in to the Gaia Portal on the Security Gateway using the *cadmin* credentials.) **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.

Note - A user that gets cloning group administration privileges (the RBA role `CloningGroupManagement`), can manage specific Cloning Groups features granted by the administrator and grant Cloning Group capabilities to other users, including remote users. When these privileges are assigned, the **Group Mode** button shows in Gaia Portal.

To manage a Cloning Group as an assigned administrator

Step	Instructions
1	Connect to the Gaia Portal on a Cloning Group member Security Gateway. With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
2	At the top, click **Group Mode**. The Security Gateway switches to Cloning Group management mode.

To join a Cloning Group

Step	Instructions
1	Connect to the Gaia Portal on a Security Gateway. With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
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. ■ In the **Remote Member Address** field, enter the IPv4 address of a remote member of the Cloning Group. ■ In the **IP for cloning** field, select an IP address (interface) for synchronizing the settings between Security Gateways. Select an interface on a secure internal network. Make sure there is a physical connectivity to the Gaia computer that runs the Cloning Group, to which you wish to join. ■ In the **Password** field, enter a password for the Cloning Group administration account (*cadmin*). (The same password you entered when you created the Cloning Group, to which you wish to join.) The *cadmin* password: • Lets you log in to the *cadmin* account • Is used to create authentication credentials for members during synchronization
5	Click **Finish**.

To create a Cloning Group that follows ClusterXL

Select this option, if the Security Gateway is a member of a ClusterXL.

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

Step	Instructions
1	Connect to the Gaia Portal on a Security Gateway. With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
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**.
5	Click **Finish**.
6	Repeat Steps 1-5 for all members of the cluster.

Note - For troubleshooting steps, refer to sk119496.

Configuring Cloning Groups in Gaia Clish

In This Section:

Cloning Group Modes 223
CLI Syntax 224

Note - When run from the *cadmin* account, these commands apply to all members of the Gaia group.

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

Cloning Group Modes

You can create Cloning Groups in either **Manual** mode, or **ClusterXL** mode.

To Create the first Cloning Group member in Manual mode

Step	Instructions
1	Set the cloning group mode to `manual`.
2	Set the cloning group local IP address.
3	Set the cloning group password.
4	Set the cloning group state to `on`.
5	**Optional:** Set a name for the Cloning Group.

To Add other Security Gateways to the Cloning Group in Manual mode

Perform these steps on each of the Security Gateways.

Step	Instructions
1	Set the cloning group mode to `manual`.
2	Set the cloning group local IP address.
3	Set the cloning group password.
4	Run the "`join cloning group`" command to join the Cloning Group.

To Create Cloning Group members in ClusterXL mode

Perform these steps on all member Security Gateways.

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

CLI Syntax

To Create and configure a Cloning Group

Syntax

```
set cloning-group
      local-ip <IPv4 address>
      mode {manual | cluster-xl}
      name <Name of Cloning Group>
      password <Password>
      state {on | off}
```

Parameters

Parameter	Description
`local-ip <IPv4 address>`	The IPv4 address used to synchronize shared features between members of the Cloning Group.
`mode {manual | cluster-xl}`	The mode determines whether the Cloning Group is defined manually, or through ClusterXL.
`name <Name of Cloning Group>`	Name of the Cloning Group.
`password <Password>`	Password for the administrator's (cadmin) account, used to access the Cloning Group configuration in the Gaia Portal, or Gaia Clish. When prompted, enter and confirm the password.
`state {on | off}`	Enables (`on`) or disables (`off`) the Cloning Group feature. **Important** - When you configure the state "`off`", the Security Gateway is removed from the Cloning Group.

To add Shared Features

Syntax

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

Parameters

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

List of Shared Features

The features are listed in the same order, in which they are shown in Gaia Clish when you run the "`show cloning-group shared-feature`" command.

Table: Shared Features in Gaia Clish

Name of Shared Feature	Description
`aggregate`	Configure route aggregation - create a supernet network from the combination of networks with a common routing prefix.
`bgp`	Configure dynamic routing via the Border Gateway Protocol.
`bootp`	Configure IPv4 DHCP Relay - relay of DHCP and BOOTP messages between clients and servers on different IPv4 Networks.
`cron`	Configure job scheduler - schedule automated tasks that perform actions at a specific time.
`dhcp6relay`	Configure IPv6 DHCP Relay - relay of DHCPv6 messages between clients and servers on different IPv6 Networks.
`dns`	Configure DNS servers.
`hosts`	Configure known hosts.
`igmp`	Establish multicast group memberships via the Internet Group Management Protocol.
`inboundfilters`	Configure Inbound Route Filters for RIP, OSPFv2, BGP, and OSPFv3 (supports IPv4 and IPv6).
`ipreachdetect`	Configure reachability detection of IP Addresses.
`time`	Configure the time and date of the system.
`ntp`	Configure Network Time Protocol (NTP) for synchronizing the system's clock over a network.
`message`	Configure banner messages.
`ospf`	Configure IPv4 dynamic routing via the Open Shortest-Path First v2 protocol.
`ospf3`	Configure IPv6 dynamic routing via the Open Shortest-Path First v3 protocol.
`password-controls`	Configure password and account policies.

Table: Shared Features in Gaia Clish (continued)

Name of Shared Feature	Description
`mailrelay`	Configure email address, to which Gaia sends mail notifications.
`display-format`	Configure how the system displays time, date and netmask.
`http`	Configure session parameters, such as inactivity timeout.
`net-access`	Configure network access to Gaia.
`users-and-roles`	Configure users and roles settings.
`arp`	Configure static ARP entries and proxy ARP entries, control dynamic ARP entries.
`syslog`	Configure system logging settings.
`proxy`	Configure proxy settings.
`host-access`	Configure which hosts are allowed to connect to the cluster devices.
`pbr`	Configure policy based routing (PBR) priority rules and action tables.
`pim`	Configure Protocol-Independent Multicast.
`prefix`	Configure dynamic routing prefix lists and trees.
`redistribution`	Configure route redistribution - advertisement of routing information from one protocol to another (supports IPv4 and IPv6).
`rip`	Configure IPv4 dynamic routing via the Routing Information Protocol.
`ripng`	Configure IPv6 dynamic routing via the Routing Information Protocol.
`routemap`	Configure dynamic routing route maps.
`routingoptions`	Configure protocol ranks and trace (debug) options.
`static`	Configure static routes.

Table: Shared Features in Gaia Clish (continued)

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

To delete Shared Features

Syntax

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

Parameters

Parameter	Description
<Feature>	The name of the feature to be deleted from the list of shared features. To see the list of the enabled Shared Features: a. Enter: `delete cloning-group shared-feature` b. Press <SPACE> and <TAB>.

To join a Cloning Group

Syntax

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

Parameters

Parameter	Description
<IPv4 address of Cloning Group>	The IPv4 address of the Cloning Group member, to which you join. **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

Syntax

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

Parameters

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

Important - Use this command only for troubleshooting purposes, when the remote Cloning Group member is not accessible. A normal way to remove a member from a Cloning Group is to run the "`leave cloning-group`" command on that member.

Notes:

- The Cloning Group configuration on the remote member itself does not change, and as soon as the device regains connectivity, it joins the Cloning Group again.
- This command can only be run if the Cloning Group is in Manual mode.

To view the Cloning Group configuration

Syntax

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

Parameters

Parameter	Description
`local-ip`	The IPv4 address used to synchronize shared features between the members of the Cloning Group.
`members`	Shows the members of the Cloning Group.
`mode`	Shows the Cloning Group mode - `Manual`, or `Cluster XL`
`name`	Shows the name of the Cloning Group
`shared-feature`	Lists the shared features that are enabled to be used by all members of the Cloning Group.
`state`	Shows the Cloning Group state - enabled, or disabled.
`status`	Shows the status of the Cloning Group member. **Note** - This option is not available, if you are logged into the *cadmin* account.

To synchronize a member in the Cloning Group

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

To Enable or disable the Cloning Group management mode

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

Syntax

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

Parameters

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

SNMP

In This Section:

Introduction 231
SNMP v3 - User-Based Security Model (USM) 233
Enabling SNMP 233
SNMP Agent Address 233
SNMP Traps 234

Introduction

Simple Network Management Protocol (SNMP) is an Internet standard protocol. SNMP is used to send and receive management information to other network devices. SNMP sends messages, called protocol data units (PDUs), to different network parts. SNMP-compliant devices, called agents, keep data about themselves in Management Information Bases (MIBs) and resend this data to the SNMP requesters.

Through the SNMP protocol, network management applications can query a management agent using a supported MIB. The Check Point SNMP implementation lets an SNMP manager monitor the system and modify selected objects only. You can define and change one read-only community string and one read-write community string. You can set, add, and delete trap receivers and enable or disable various traps. You can also enter the location and contact strings for the system.

Check Point Gaia supports SNMP v1, v2, and v3.

To view detailed information about each MIB that the Check Point implementation supports (also, see sk90470):

MIB	Location
Standard MIBs	`/usr/share/snmp/mibs/*.txt`
Check Point MIBs	`$CPDIR/lib/snmp/chkpnt.mib` `$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 were made to the first version to address security and other fixes. For more information, see *Net-SNMP*.

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.

Use Gaia to run these tasks:

- Define and change one read-only community string.
- Define and change one read-write community string.
- Enable and disable the SNMP daemon.
- Create SNMP users.
- Change SNMP user accounts.
- Add or delete trap receivers.
- Enable or disable the various traps.
- Enter the location and contact strings for the device.

SNMP v3 - User-Based Security Model (USM)

Gaia supports the user-based security model (USM) component of SNMPv3 to supply message-level security. With USM (described in RFC 3414), access to the SNMP service is controlled based on user identities. Each user has a name, an authentication pass phrase (used for identifying the user), and an optional privacy pass phrase (used for protection against disclosure of SNMP message payloads).

The system uses the MD5 hashing algorithm to supply authentication and integrity protection and DES to supply encryption (privacy).

Best Practice - Use authentication and encryption. You can use them independently by specifying one or the other with your SNMP manager requests. The Gaia responds accordingly.

SNMP users are maintained separately from system users. You can create SNMP user accounts with the same names as existing user accounts or different. You can create SNMP user accounts that have no corresponding system account. When you delete a system user account, you must separately delete the SNMP user account.

Enabling SNMP

The SNMP daemon is disabled by default.

If you choose to use SNMP, enable and configure it according to your security requirements.

At minimum, you must change the default community string to something other than public.

You can choose to use all versions of SNMP (v1, v2, and v3) on your system, or to grant SNMPv3 access only.

Best Practice - If your SNMP management station supports SNMP v3, select only SNMP v3 on Gaia. SNMPv3 limits community access. Only requests from users with enabled SNMPv3 access are allowed, and all other requests are rejected.

Note - If you do not plan to use SNMP to manage the network, disable it. Enabling SNMP opens potential attack vectors for surveillance activity. It lets an attacker learn about the configuration of the device and the network.

SNMP Agent Address

An SNMP Agent address is a specified IP address, on which the SNMP agent listens and reacts to requests.

The default behavior is for the SNMP agent to listen to and react to requests on all interfaces. If you specify one or more agent addresses, the system SNMP agent listens and responds only on those interfaces.

You can use the agent address as a different method to limit SNMP access. For example: you can limit SNMP access to one secure internal network that uses a specified interface. Configure that interface as the only agent address.

SNMP Traps

Managed devices use trap messages to report events to the Network Management Station (NMS).

When some types of events occur, the platform sends a trap to the management station.

The Gaia proprietary traps are configured in the `/etc/snmp/GaiaTrapsMIB.mib` file.

Gaia supports these types of SNMP traps:

Table: SNMP Traps in Gaia

Type of Trap	Description
`coldStart`	Notifies when the SNMPv2 agent is re-initialized.
`linkUpLinkDown`	Notifies when one of the links changes state to up or down.
`authorizationError`	Notifies when an SNMP operation is not properly authenticated.
`configurationChange`	Notifies when a change to the system configuration is applied.
`configurationSave`	Notifies when a permanent change to the system configuration occurs.
`lowDiskSpace`	Notifies when space on the system disk is low. 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`	Notifies if one of the voltage sensors exceeds its maximum value.
`lowVoltage`	Notifies if one of the voltage sensors falls below its minimum value.

Table: SNMP Traps in Gaia (continued)

Type of Trap	Description
`raidVolumeState`	Notifies if the raid volume state is not optimal. This trap works only if RAID is supported on the Gaia computer. To make sure that RAID monitoring is supported, run the command `raid_diagnostic` and confirm that it shows the RAID status.
`biosFailure`	Notifies when the Primary BIOS failure is detected. Sent once the event occurs. Applies to computers with Dual BIOS.
`vrrpv2AuthFailure`	Notifies when the VRRP Cluster Member has packet an authentication failure in VRRPv2 (IPv4) and VRRPv3 (IPv6). Sent each polling interval.
`vrrpv2NewMaster`	Notifies when the VRRP Cluster Member transitioned to VRRP Master state in VRRPv2 (IPv4). Sent each polling interval.
`vrrpv3NewMaster`	Notifies when the VRRP Cluster Member transitioned to VRRP Master state in VRRPv3 (IPv6). Sent each polling interval.
`vrrpv3ProtoError`	Notifies when the VRRP Cluster Member has a protocol error in VRRPv2 (IPv4) and VRRPv3 (IPv6). Sent each polling interval.

Configuring SNMP in Gaia Portal

For detailed information, see sk90860: How to configure SNMP on Gaia OS.

To enable SNMP

Step	Instructions
1	In the navigation tree, click **System Management** > **SNMP**.
2	Select **Enable SNMP Agent**.
3	In the **Version** drop down list, select the version of SNMP to run: ■ **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	Instructions
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	Instructions
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.

Configuring USM users

To add a USM user

Step	Instructions
1	In the navigation tree, click **System Management** > **SNMP**.
2	In the **V3 - User-Based Security Model (USM)** section, click **Add**. The **Add New USM User** window opens.
3	In the **User Name**, enter the applicable user name. This can be the same as a user name for system access. **Notes:** ■ This string must contain alphanumeric characters with no spaces, backslash, or colon characters. ■ The length of this string is between 1 and 31 characters on Management Server, Log Servers, and Security Gateways that run in the Gateway mode with MDPS disabled. ■ The length of this string is between 1 and 26 characters on Security Gateways that run in the VSX mode or with MDPS enabled.
4	In the **Security Level**, select one of these options from the drop-down list: ■ **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** ■ **SHA256** ■ **SHA512** 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.

Step	Instructions
8	In the **Privacy Protocol**, select: ▪ **DES** ▪ **AES** The default is **DES**.
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 edit a USM user

Step	Instructions
1	In the navigation tree, click **System Management** > **SNMP**.
2	In the **V3 - User-Based Security Model (USM)** section, select the user and click **Edit**. 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 delete a USM user

Step	Instructions
1	In the navigation tree, click **System Management** > **SNMP**.
2	In the **V3 - User-Based Security Model (USM)** section, select the user and click **Remove**. 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 enable or disable SNMP trap types

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

Configuring SNMP trap receivers

To add SNMP trap receivers

Step	Instructions
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	Instructions
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	Instructions
1	In the navigation tree, click **System Management** > **SNMP**.
2	In the **Trap Receivers Settings** section, select the SNMP trap receiver and click **Remove**. 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 custom SNMP traps

Adding a custom SNMP trap

Step	Instructions
1	In the navigation tree, click **System Management** > **SNMP**.
2	In the **Custom Traps** section, click **Add**. The **Add New Custom Trap** window opens.
3	In the **Trap Name**, enter the name of an SNMP trap. Range: 1 - 128 characters.
4	In the **OID**, enter the SNMP OID to query. ■ The OID value can contain only numbers and periods (sub-identifiers separated by periods). ■ The OID value can contain from 2 to 128 sub-identifiers: from `X.X` to `X.X.` (124 sub-identifiers more) ■ Number range of each sub-identifier: 0 - 4294967295. ■ The first sub-identifier must be one of these numbers: • `0` In this case, the second sub-identifier must be between 0-39: `0.<0-39>.` (other applicable sub-identifiers) • `1` In this case, the second sub-identifier must be between 0-39: `1.<0-39>.` (other applicable sub-identifiers) • `2` `2.X.` (other applicable sub-identifiers)
5	In the **Operator** field, select the applicable operator to examine the value the SNMP OID to query returns: ■ **Equal** - The returned value is equal to the value in the **Threshold** field. ■ **Not_Equal** - The returned value is not equal to the value in the **Threshold** field. ■ **Less_Than** - The returned value is less than the value in the **Threshold** field. ■ **Greater_Than** - The returned value is greater than the value in the **Threshold** field. ■ **Changed** - The returned value is different than the returned value in the previous SNMP OID query.
6	In the **Threshold**, enter an integer value to which Gaia operating system compares the value returned in the SNMP OID query. Range: 1 - 128 characters.

Step	Instructions
7	In the **Frequency**, enter the interval (in seconds) between the SNMP OID queries. Range: 1 - 4294967295.
8	In the **Message**, enter the applicable text. This is the message you get in the SNMP Trap packets the Gaia operating system sends. Range: 1 - 128 characters.
9	Click **Save**.

Editing a custom SNMP trap

For explanations, see the section "Adding a custom SNMP trap".

Step	Instructions
1	In the navigation tree, click **System Management** > **SNMP**.
2	In the **Custom Traps** section, select the custom SNMP trap and click **Edit**. The **Edit Custom Trap** window opens.
3	Configure the applicable settings.
6	Click **Save**.

Deleting a custom SNMP trap

Step	Instructions
1	In the navigation tree, click **System Management** > **SNMP**.
2	In the **Custom Traps** section, select the custom SNMP trap and click **Remove**.
3	The window shows this message: **Are you sure you want to delete "<Name of Custom Trap>" entry?** Click **Yes**.

Configuring SNMP in Gaia Clish

For detailed information, see sk90860: How to configure SNMP on Gaia OS.

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

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

Syntax for the '`add`' commands

Note - To see all available commands:

1. Enter:
   `add snmp`
2. Press <SPACE>
3. Press <ESC><ESC>

Syntax

`add snmp interface <Name of Interface>`
`add snmp traps receiver <IPv4 address> version {v1 | v2 | v3} community <String>` `add snmp custom-trap <Custom Trap Name> oid <Value> operator <Logical Operator> threshold <Value> frequency <Value> message "<Text>"`

`add snmp usm user <UserName> security-level authPriv auth-pass-phrase <Pass Phrase> privacy-pass-phrase <Privacy Pass Phrase> privacy-protocol {DES | AES} authentication-protocol {MD5 | SHA1}`
`add snmp usm user <UserName> security-level authPriv auth-pass-phrase-hashed <Hashed Pass Phrase> privacy-pass-phrase <Privacy Pass Phrase> privacy-protocol {DES | AES} authentication-protocol {MD5 | SHA1}`
`add snmp usm user <UserName> security-level authNoPriv auth-pass-phrase <Pass Phrase> authentication-protocol {MD5 | SHA1}`
`add snmp usm user <UserName> security-level authNoPriv auth-pass-phrase-hashed <Hashed Pass Phrase>`

Description of commands

Command	Description
`add snmp custom-trap ...`	Adds a custom SNMP trap: ■ `<Custom Trap Name>` Specifies the name of the custom trap. Range: 1 - 128 characters. ■ `oid <Value>` Specifies the SNMP OID to query. • The OID value can contain only numbers and periods (sub-identifiers separated by periods). • The OID value can contain from 2 to 128 sub-identifiers: from `X.X` to `X.X.` (124 sub-identifiers more) • Number range of each sub-identifier: 0 - 4294967295. • The first sub-identifier must be one of these numbers: ◦ `0` In this case, the second sub-identifier must be between 0-39: `0.<0-39>.` (other applicable sub-identifiers) ◦ `1` In this case, the second sub-identifier must be between 0-39: `1.<0-39>.` (other applicable sub-identifiers) ◦ `2` `2.X.` (other applicable sub-identifiers) ■ `operator <Logical Operator>` Specifies the operator to examine the value the SNMP OID to query returns: • `Equal` - The returned value is equal to the value in the "`threshold`" parameter. • `Not_Equal` - The returned value is not equal to the value in the "`threshold`" parameter. • `Less_Than` - The returned value is less than the value in the "`threshold`" parameter. • `Greater_Than` - The returned value is greater than the value in the "`threshold`" parameter. • `Changed` - The returned value is different than the returned value in the previous SNMP OID query. ■ `threshold <Value>` Specifies an integer value to which Gaia operating system compares the value returned in the SNMP OID query. Range: 1 - 128 characters. ■ `frequency <Value>`

Command	Description
	Specifies the interval (in seconds) between the SNMP OID queries. Range: 1 - 4294967295. ■ `message "<Text>"` Specifies the applicable text. This is the message you get in the SNMP Trap packets the Gaia operating system sends. Range: 1 - 128 characters.
`add snmp interface ...`	Adds a local interface to the list of local interfaces, on which the SNMP daemon listens.
`add snmp traps receiver ...`	Adds a SNMP Trap Sink.
`add snmp usm user ...`	Adds an SNMPv3 USM user. **Notes:** ■ This string must contain alphanumeric characters with no spaces, backslash, or colon characters. ■ The length of this string is between 1 and 31 characters on Management Server, Log Servers, and Security Gateways that run in the Gateway mode with MDPS disabled. ■ The length of this string is between 1 and 26 characters on Security Gateways that run in the VSX mode or with MDPS enabled.

Syntax for the 'set' commands

Note - To see all available commands:

1. Enter:
   `set snmp`
2. Press <SPACE>
3. Press <ESC><ESC>

Syntax

```
set snmp agent {on | off}
set snmp agent-version {any | v3-Only}
```

set snmp clear-trap interval <*Value*> retries <*Value*> set snmp custom-trap <*Custom Trap Name*> oid <*Value*> operator <*Logical Operator*> threshold <*Value*> frequency <*Value*> message "<*Text*>" 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*>
set snmp community <*String*> {read-only | read-write}
set snmp contact <*Contact Information*> set snmp location <*Location Information*>
set snmp mode {default | vs}
set snmp usm user <*UserName*> security-level authPriv auth-pass-phrase <*Pass Phrase*> privacy-pass-phrase <*Privacy Pass Phrase*> privacy-protocol {DES | AES} 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 vs-direct-access {on | off}

Description of commands

Command	Description
`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 agent {on | off}`	Enables (`on`) or disables (`off`) the SNMP Agent.
`set snmp clear-trap ...`	Configures the indication of a custom SNMP trap termination.
`set snmp community <String> {read-only | read-write}`	Configures the SNMP community password and if this password lets you only read the values of SNMP objects (`read-only`), or set the values as well (`read-write`).
`set snmp contact ...`	Configures the contact name for the SNMP community.
`set snmp custom-trap ...`	Configures the settings of an existing custom SNMP trap. See the explanations in the "`add snmp custom-trap`" command.
`set snmp location ...`	Configures the contact location for the SNMP community.
`set snmp mode {default | vs}`	Configures how to run the SNMP daemon: ■ `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 traps coldStart-threshold <Seconds>`	Configures the threshold for the SNMP `coldStart` trap.

Command	Description
`set snmp traps polling-frequency <Seconds>`	Configures the polling interval for the SNMP traps.
`set snmp traps receiver ...`	Configures the IPv4 address of the SNMP Trap Sink.
`set snmp traps trap-user <UserName>`	Configures the user, which will generate the SNMP traps.
`set snmp traps trap ...`	Configures the Gaia built-in SNMP traps.
`set snmp usm user <UserName> ...`	Configures the SNMPv3 USM user.
`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 *R80.40 VSX Administration Guide*.

Syntax for the 'delete' commands

Note - To see all available commands:

1. Enter:
   `delete snmp`
2. Press <SPACE>
3. Press <ESC><ESC>

Syntax

```
delete snmp clear-trap
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>
```

```
delete snmp community <String>
```

```
delete snmp contact <Contact Information>
delete snmp location <Location Information>
```

```
delete snmp interface <Name of Interface>
delete snmp usm user <UserName>
```

Description of commands

Command	Description
`delete snmp clear-trap`	Removes the indication of a custom SNMP trap termination.
`delete snmp community <String>`	Removes the SNMP community password.
`delete snmp contact ...`	Removes the contact name for the SNMP community.
`delete snmp custom-trap <Custom Trap Name>`	Removes the custom SNMP trap.
`delete snmp interface <Name of Interface>`	Removes the local interface from the list of local interfaces, on which the SNMP daemon listens.
`delete snmp location ...`	Removes the contact location for the SNMP community.
`delete snmp traps coldStart-threshold`	Removes the threshold for the SNMP `coldStart` trap.
`delete snmp traps polling-frequency`	Removes the polling interval for the SNMP traps.
`delete snmp traps receiver <IPv4 address>`	Removes the IPv4 address of the SNMP Trap Sink.
`delete snmp traps trap-user <UserName>`	Removes the user, which will generate the SNMP traps.
`delete snmp usm user <UserName>`	Removes the SNMPv3 USM user.

Interpreting SNMP Error Messages

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

SNMP PDU

Within the SNMP PDU, the **third** field can include an error-status integer that refers to a specific problem.

The integer zero (0) means that no errors were detected.

When the error field is anything other than 0, the next field includes an error-index value that identifies the variable, or object, in the variable-bindings list that caused the error.

This table lists the error status codes and their meanings:

Error status code	Meaning		Error status code	Meaning
0	`noError`		10	`wrongValue`
1	`tooBig`		11	`noCreation`
2	`NoSuchName`		12	`inconsistentValue`
3	`BadValue`		13	`resourceUnavailable`
4	`ReadOnly`		14	`commitFailed`
5	`genError`		15	`undoFailed`
6	`noAccess`		16	`authorizationError`
7	`wrongType`		17	`notWritable`
8	`wrongLength`		18	`inconsistentName`
9	`wrongEncoding`			

Note - You might not see the codes. The SNMP manager or utility interprets the codes and then logs the appropriate message.

Within the SNMP PDU, the **fourth** field, contains the error index when the error-status field is nonzero.

That is, when the error-status field returns a value other than zero, which indicates that an error occurred. The error-index value identifies the variable, or object, in the variable-bindings list that caused the error. The first variable in the list has index 1, the second has index 2, and so on.

Within the SNMP PDU, the **fifth** field, is the variable-bindings field.

This field consists of a sequence of pairs:

- The first element in a pair is the identifier.
- The second element in a pair is one of these options: `value`, `unSpecified`, `noSuchOjbect`, `noSuchInstance`, or `EndofMibView`.

This table describes the elements:

Variable-bindings element	Description
`value`	Value that is associated with each object instance. This value is specified in a PDU request.
`unSpecified`	A NULL value is used in retrieval requests.
`noSuchObject`	Indicates that the agent does not implement the object, to which it refers by this object identifier.
`noSuchInstance`	Indicates that this object does not exist for this operation.
`endOfMIBView`	Indicates an attempt to reference an object identifier that is beyond the end of the MIB at the agent.

GetRequest

This table lists possible value field sets in the response PDU or error-status messages when performing an SNMP `GetRequest`.

Value Field Set	Description
`noSuchObject`	If a variable does not have an `OBJECT IDENTIFIER` prefix that exactly matches the prefix of any variable accessible by this request, its value field is set to `noSuchObject`.
`noSuch Instance`	If the variable's name does not exactly match the name of a variable, its value field is set to `noSuchInstance`.
`genErr`	If the processing of a variable fails for any other reason, the responding entity returns `genErr` and a value in the error-index field that is the index of the problem object in the variable-bindings field.
`tooBig`	If the size of the message that encapsulates the generated response PDU exceeds a local limitation or the maximum message size of the request's source party, then the response PDU is discarded and a new response PDU is constructed. The new response PDU has an error-status of `tooBig`, an `error-index` of zero, and an empty `variable-bindings` field.

GetNextRequest

The only values that can be returned as the second element in the variable-bindings field to a `GetNextRequest` when an error-status code occurs are `unSpecified` or `endOfMibView`.

GetBulkRequest

The `GetBulkRequest` minimizes the number of protocol exchanges and lets the SNMPv2 manager request that the response is large as possible.

The `GetBulkRequest` PDU has two fields that do not appear in the other PDUs: non-repeaters and max-repetitions. The non-repeaters field specifies the number of variables in the variable-bindings list, for which a single-lexicographic successor is to be returned. The max-repetitions field specifies the number of lexicographic successors to be returned for the remaining variables in the variable-bindings list.

If at any point in the process, a lexicographic successor does not exist, the `endofMibView` value is returned with the name of the last lexicographic successor, or, if there were no successors, the name of the variable in the request.

If the processing of a variable name fails for any reason other than `endofMibView`, no values are returned. Instead, the responding entity returns a response PDU with an error-status of `genErr` and a value in the error-index field that is the index of the problem object in the variable-bindings field.

Job Scheduler

You can schedule regular jobs.

You can configure the jobs to run at the dates and times that you specify, or at startup.

Configuring Job Scheduler in Gaia Portal

Scheduling new jobs

Step	Instructions
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.
	Important:
	■ The command must be a Linux command.
	■ If you wish to run a Check Point command or use a Check Point environment variable, then use this syntax (see *"Running Check Point Commands in Shell Scripts" on page 491*):
	• On a Security Management Server / Log Server / SmartEvent Server:
	`source /etc/profile.d/CP.sh ; <Applicable Check Point Command>`
	• On a Multi-Domain Server / Multi-Domain Log Server:
	`source /etc/profile.d/CP.sh ; source $MDSDIR/scripts/MDSprofile.sh ; source $MDS_SYSTEM/shared/mds_environment_utils.sh ; source $MDS_SYSTEM/shared/sh_utilities.sh ; <Applicable Check Point Command>`
	• On a Security Gateway / Cluster Members (non-VSX):
	`source /etc/profile.d/CP.sh ; <Applicable Check Point Command>`
	• On a VSX Gateway / VSX Cluster Members:
	`source /etc/profile.d/CP.sh ; source /etc/profile.d/vsenv.sh ; <Applicable Check Point 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.

Step	Instructions
7	In the **E-mail Notification**, enter the e-mail address, to which Gaia should send the notifications. **Note** - You must also configure a Mail Server (see *"Mail Notification" on page 267*).
8	Click **Apply**.

Editing the scheduled jobs

Step	Instructions
1	In the navigation tree, click **System Management** > **Job Scheduler**.
2	In the scheduled Jobs table, select the job that you want to edit.
3	Click **Edit**. The **Edit Scheduled Job** opens.
4	Enter the changes.
5	Click **OK**.

Deleting the scheduled jobs

Step	Instructions
1	In the navigation tree, click **System Management** > **Job Scheduler**.
2	In the **Scheduled Jobs** table, select the job to delete.
3	Click **Delete**.
4	Click **OK** to confirm. (Click **Cancel** to abort.)

Configuring Job Scheduler in Gaia Clish

Description

Use these commands to configure Gaia to schedule jobs. The jobs run on the dates and times you specify.

You can define an email address, to which Gaia sends the output of the scheduled job.

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

Syntax

Adding new scheduled jobs

```
add cron job <Job Name> command "<Command>" recurrence
      daily time <HH:MM>
      monthly month <1-12> days <1-31> time <HH:MM>
      weekly days <0-6> time <HH:MM>
      system-startup
```

Editing the existing scheduled jobs

```
set cron job <Job Name>
      command "<Command>"
      recurrence
            daily time <HH:MM>
            monthly month <1-12> days <1-31> time <HH:MM>
            weekly days <0-6> time <HH:MM>
            system-startup
```

```
set cron mailto <Email Address>
```

Viewing the existing scheduled jobs

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

Deleting the existing scheduled jobs

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

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

Parameters

CLI Parameters

Parameter	Description
<Job Name>	The name of the job to schedule.

Parameter	Description

"<*Command*>"	The command to run.
	Important:
	■ The command must be a Linux command.
	■ You must enclose the syntax in quotes:
	• If the command contains variables (`$NameOfVariable`), then use double quotes.
	• If the command does not contain variables, you can use single quotes.
	■ If you wish to run a Check Point command or use a Check Point environment variable, then use this syntax (see *"Running Check Point Commands in Shell Scripts" on page 491*):
	• On a Security Management Server / Log Server / SmartEvent Server:
	`source /etc/profile.d/CP.sh ; <Applicable Check Point Command>`
	• On a Multi-Domain Server / Multi-Domain Log Server:
	`source /etc/profile.d/CP.sh ; source $MDSDIR/scripts/MDSprofile.sh ; source $MDS_SYSTEM/shared/mds_environment_utils.sh ; source $MDS_SYSTEM/shared/sh_utilities.sh ; <Applicable Check Point Command>`
	• On a Security Gateway / Cluster Members (non-VSX):
	`source /etc/profile.d/CP.sh ; <Applicable Check Point Command>`
	• On a VSX Gateway / VSX Cluster Members:
	`source /etc/profile.d/CP.sh ; source /etc/profile.d/vsenv.sh ; <Applicable Check Point Command>`

Parameter	Description
`recurrence daily time <HH:MM>`	Specifies that the job should run once a day - every day, at specified time. 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, February, and March, enter `1,2,3` To specify several consequent dates, enter their numbers separate by commas. Example: For 1st, 2nd and 3rd day of the month, enter `1,2,3`
`recurrence weekly days <0-6> time <HH:MM>`	Specifies that the job should run once a week - on specified days of week, and at specified time. 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.

Parameter	Description
`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 (see *"Mail Notification" on page 267*).

Mail Notification

In This Section:

Introduction 267
Configuring Mail Notification in Gaia Portal 268
Configuring Mail Notification in Gaia Clish 269

Introduction

Mail notifications (also known as Mail Relay) allow you to send email from the Security Gateway.

You can send email interactively or from a script. The email is relayed to a mail hub that sends the email to the final recipient.

Mail notifications are used as an alerting mechanism when a Firewall rule is triggered. It is also used to email the results of cron jobs to the system administrator.

Gaia supports these mail notification features:

- Presence of a mail client or Mail User Agent (MUA) that can be used interactively or from a script.
- Presence of a Sendmail-like replacement that relays mail to a mail hub by using SMTP.
- Ability to specify the default recipient on the mail hub.

Gaia does not support these mail notification features:

- Incoming e-mail.
- Mail transfer protocols other than outbound SMTP.
- Telnet to port 25.
- E-mail accounts other than *admin* or *monitor*.

Configuring Mail Notification in Gaia Portal

Step	Instructions
1	In the navigation tree, click **System Management** > **Mail Notification**.
2	In the **Mail Server** field, enter the IPv4 Address or Hostname of the mail server. 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 in 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 <IPv4 Address or Hostname>
```

- To configure the user on the mail server that receives the mail notifications:

```
set mail-notification username <User Name>
```

- To show the configured mail server and user:

```
show mail-notification
      server
      username
```

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

Parameters

Parameter	Description
`server <IPv4 Address or Hostname>`	The IPv4 address or Hostname of the mail server, to which Gaia sends mail notifications. 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

In This Section:

Comparison *270*

Configuring Messages in Gaia Portal *270*

Configuring Messages in Gaia Clish *271*

Limits *274*

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

Comparison

Item	Banner Message	Message of the Day
Default Message	`This system is for authorized use only`	`You have logged into the system`
When shown in Gaia Portal	Browser login page, before logging in	After logging in to the system
When shown in Gaia Clish	When logging in, before entering the password	After logging in to the system
Default state	Enabled	Disabled

Configuring Messages in Gaia Portal

Step	Instructions
1	In the navigation tree, click **System Management** > **Messages**.
2	To enter a Banner message, select **Banner message**.
3	To enter a Message of the Day, select **Message of the day**.
4	Enter the message text. See the **Limits** section below.
5	Click **Apply**.

Configuring Messages in Gaia Clish

Syntax for Banner message

- To show if the banner message is enabled or disabled:

```
show message banner status
show message all status
```

- To show the configured banner message:

```
show message banner
show message all
```

- To define a new single-line banner message:

```
set message banner on msgvalue "<Banner Text>"
```

  See the **Limits** section below.

  Example:

```
gaia> set message banner on msgvalue "This system is private
and confidential"
```

- To define a new multi-line banner message:

```
set message banner on line msgvalue "<Banner Text for Line
#1>"
set message banner on line msgvalue "<Banner Text for Line
#2>"
```

- To enable or disable the configured banner message:

```
set message banner on
set message banner off
```

- To delete the configured banner message perform these two steps:

1. Delete the user-defined banner message:

   ```
   delete message banner
   ```

   Note - This deletes the configured banner message, and replaces it with the default banner message "`This system is for authorized use only.`"

2. Disable the default banner:

   ```
   set message banner off
   ```

Syntax for Message of the Day

- To show the configured message of the day:

```
show message motd
show message all
```

- To show if the message of the day is enabled or disabled:

```
show message motd status
show message all status
```

- To define a new single-line message of the day:

```
set message motd on msgvalue "<Message Text>"
```

  See the **Limits** section below.

  Example:

```
gaia> set message motd on msgvalue "Hi all - no changes
allowed today"
```

- To define a new multi-line message of the day:

```
set message motd on line msgvalue "<Message Text for Line
#1>"
set message motd on line msgvalue "<Message Text for Line
#2>"
```

  See the **Limits** section below.

- To enable or disable the configured message of the day:

```
set message motd on
set message motd off
```

- To delete the configured message of the day, perform these two steps:

1. Delete the user-defined message of the day:

   ```
   delete message motd
   ```

   Note - This deletes the configured message of the day, and replaces it with the default message of the day "`You have logged into the system.`"

2. Disable the default message of the day:

   ```
   set message motd off
   ```

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

Limits

Message type	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

In This Section:

Configuring Display Format in Gaia Portal 275
Configuring Display Format in Gaia Clish 276

You configure format for the Time, Date, and IPv4 netmask on Gaia.

Configuring Display Format in Gaia Portal

Step	Instructions
1	In the navigation tree, click **System Management** > **Display Format**.
2	In **Time**, select one of these options: ■ **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 in Gaia Clish

Syntax for the Time

- To show the current time format:

```
show format time
show format all
```

- To configure the time format:

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

Syntax for the Date

- To show the current date format:

```
show format date
show format all
```

- To configure the date format:

```
set format date
      dd/mm/yyyy
      mm/dd/yyyy
      yyyy/mm/dd
      dd-mmm-yyyy
```

Syntax for the IPv4 netmask

- To show the current IPv4 netmask format:

```
show format netmask
show format all
```

- To configure the IPv4 netmask format:

```
set format netmask
      dotted
      length
```

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

Session

You can manage inactivity timeout for Gaia Portal and Gaia Clish.

Configuring the Session in Gaia Portal

Step	Instructions
1	In the navigation tree, click **System Management** > **Session**.
2	In the **Command Line Shell** section, configure the inactivity timeout for the Gaia Clish.
3	In the **Web UI** section, configure the inactivity timeout for the Gaia Portal. ■ **Range:** 1 - 720 minutes ■ **Default:** 10 minutes

Configuring the Session in Gaia Clish

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

Syntax

- To configure the timeout:

```
set inactivity-timeout <Timeout>
```

- To show the configured timeout:

```
show inactivity-timeout
```

Parameters

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

Core Dumps

In This Section:

Introduction 278
Configuring Core Dumps in Gaia Portal 278
Configuring Core Dumps in Gaia Clish 280

Introduction

A process core dump file 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 dump file in the `/var/log/dump/usermode/` directory.

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

Configuring Core Dumps in Gaia Portal

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

Procedure

Step	Instructions
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 in Gaia Clish

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 status of this feature:

  ```
  show core-dump status
  ```

- 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

In This Section:

Configuring IPv6 Support in Gaia Portal 283
Configuring IPv6 Support in Gaia Clish 283

Important:

- Security Management Server R80.40 does not support IPv6 Address on Gaia Management Interface (Known Limitation 01622840).
- Multi-Domain Server R80.40 does not support IPv6 at all (Known Limitation PMTR-14989).

Before you can configure IPv6 addresses and IPv6 static routes, you must:

Step	Instructions
1	Enable the IPv6 support.
2	Reboot.
3	To configure IPv6 addresses, see *"Network Interfaces" on page 89*. To configure IPv6 static routes, see *"IPv6 Static Routes" on page 188*.

To enforce a Security Policy for IPv6 traffic:

Step	Instructions
1	Enable the IPv6 support in Gaia OS on both the Security Management Server and the Security Gateway (each Cluster Member).
2	Connect with SmartConsole to the Management Server.
3	Create the applicable IPv6 objects.
4	Create the applicable IPv6 rules in the Access Control Policy.
5	Install the Access Control Policy on the Security Gateway (the Cluster) object.

Configuring IPv6 Support in Gaia Portal

Step	Instructions
1	With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
2	From the navigation tree, click **System Management** > **System Configuration**.
3	In the **IPv6 Support** section, select **On**.
4	Click **Apply**.
5	When prompted, select **Yes** to reboot. **Important** - IPv6 support is **not** available until you reboot.

Configuring IPv6 Support in Gaia Clish

- To configure IPv6 support:

  ```
  set ipv6-state {on | off}
  ```

  Important - This change requires reboot.

- 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.

Procedure

Step	Instructions
1	Connect to the command line on Gaia.
2	Log in to Gaia Clish.
3	Enable the IPv6 support: `set ipv6-state on`

Step	Instructions
4	Save the changes: `save config`
5	Reboot: `reboot` **Important** - IPv6 support is **not** available until you reboot.

System Logging

You can configure the settings for the system logs, including sending them to a remote server.

Make sure to configure the remote server to receive the system logs.

Configuring System Logging in Gaia Portal

This section includes procedures for configuring System Logging and Remote System Logging.

System Logging configures if Gaia sends these logs:

- Gaia syslog messages to its Check Point Management Server
- Gaia audit logs upon successful configuration to its Check Point Management Server
- Gaia audit logs upon successful configuration to Gaia syslog facility

Remote System Logging configures a remote syslog server, to which Gaia sends its syslog messages.

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

To configure System Logging

Step	Instructions
1	In the navigation tree, click **System Management** > **System Logging**.
2	In the **System Logging** section, select the applicable options:
	■ **Send Syslog messages to management server** Specifies if the Gaia sends the Gaia system logs to a Check Point Management Server. **Default:** Not selected **Note** - You can configure this option in Gaia Clish with the "`set syslog cplogs {on | off}`" command.
	■ **Send audit logs to management server upon successful configuration** 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** - You can configure this option in the Gaia Clish with the "`set syslog mgmtauditlogs {on | off}`" command.

Step	Instructions
	■ **Send audit logs to syslog upon successful configuration** Specifies if the Gaia saves the logs for configuration changes that authorized users make. Otherwise, Gaia uses the default `/var/log/messages` file. **Default:** Selected To specify a Gaia configuration audit log file, run this command: `set syslog filename /<Path>/<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	Instructions
1	In the navigation tree, click **System Management** > **System Logging**.
2	In the **Remote System Logging** section, click **Add**.
3	In the **IP Address** field, enter the IPv4 address of the remote syslog server.
4	In the **Priority** field, select the severity level of the logs that are sent to the remote server. 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	Instructions
1	In the navigation tree, click **System Management** > **System Logging**.
2	In the **Remote System Logging** section, select the remote server.
3	Click **Edit**.
4	In the **IP Address** field, enter the IPv4 address of the remote syslog server.
5	In the **Priority** field, select the severity level of the logs that are sent to the remote server.
6	Click **OK**.

To delete Remote System Logging settings

Step	Instructions
1	In the navigation tree, click **System Management** > **System Logging**.
2	In the **Remote System Logging** section, select the remote syslog server.
3	Click **Delete**.
4	In the confirmation window, click **Yes**.

Syslog Configuration Files

By default, Gaia OS saves the Syslog configuration in these files:

- `/etc/syslog.conf`
- `/etc/sysconfig/syslog`

If it is necessary to add specific settings manually in these files (that Gaia OS does not have), then it is necessary to make these files immutable, so Gaia OS does not overwrite them:

1. Connect to the command line on Gaia OS.
2. Log in to the Expert mode.
3. Edit the applicable Syslog configuration file as required in your environment.
4. Examine the current attributes on the applicable configuration file you edited:

- `lsattr /etc/syslog.conf`
- `lsattr /etc/sysconfig/syslog`

5. Add the immutable attribute on the applicable configuration file you edited:
   - `chattr +i /etc/syslog.conf`
   - `chattr +i /etc/sysconfig/syslog`
6. Examine the current attributes on the applicable configuration file you edited:
   - `lsattr /etc/syslog.conf`
   - `lsattr /etc/sysconfig/syslog`
7. Restart the Syslog service:

```
service syslog restart
```

Warning - While the Syslog configuration files are immutable:

- Gaia OS cannot save the changes in the Syslog configuration you make in Gaia Portal or Gaia Clish.
- Gaia OS cannot restore a Gaia Backup.

To remove the immutable attribute from a file, use this command:

```
chattr -i <file>
```

Configuring System Logging in Gaia Clish

Description

You can configure the System Logging and Remote System Logging.

System Logging configures the Gaia to sends these logs:

- Gaia syslog messages to its Check Point Management Server
- Gaia audit logs upon successful configuration to its Check Point Management Server
- Gaia audit logs upon successful configuration to Gaia syslog facility

Remote System Logging configures a remote server, to which Gaia sends its syslog messages.

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

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

Syntax for System Logging configuration

- To send the Gaia system logs to a Check Point Management Server:

```
set syslog cplogs {on | off}
```

- To send the Gaia configuration audit logs to a Check Point Management Server:

```
set syslog mgmtauditlogs {on | off}
```

- To save the Gaia configuration audit logs:

```
set syslog auditlog {disable | permanent}
```

- To configure the file name of the Gaia configuration audit log:

```
set syslog filename /<Path>/<File>
```

- To show the Gaia system logging configuration:

```
show syslog
      all
      auditlog
      cplogs
      filename
      mgmtauditlogs
```

Syntax for Remote System Logging configuration

- To send Gaia system logs to a remote syslog server:

```
add syslog log-remote-address <IPv4 Address> level
<Severity>
```

- To show the Gaia system logging configuration:

```
show syslog
      all
      log-remote-address <IPv4 Address>
      log-remote-addresses
```

- To stop sending Gaia system logs to the specific remote server:

```
delete syslog log-remote-address <IPv4 Address> [level
<Severity>]
```

CLI Parameters

Parameter	Description
`cplogs {on | off}`	Specifies if the Gaia sends the Gaia system logs to a Check Point Management Server: ■ `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**.

Parameter	Description
`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 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** in Gaia Portal does not let you configure this setting.
`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

Parameter	Description
<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>
```

Syslog Configuration Files

By default, Gaia OS saves the Syslog configuration in these files:

- `/etc/syslog.conf`
- `/etc/sysconfig/syslog`

If it is necessary to add specific settings manually in these files (that Gaia OS does not have), then it is necessary to make these files immutable, so Gaia OS does not overwrite them:

1. Connect to the command line on Gaia OS.
2. Log in to the Expert mode.
3. Edit the applicable Syslog configuration file as required in your environment.
4. Examine the current attributes on the applicable configuration file you edited:
   - `lsattr /etc/syslog.conf`
   - `lsattr /etc/sysconfig/syslog`
5. Add the immutable attribute on the applicable configuration file you edited:
   - `chattr +i /etc/syslog.conf`
   - `chattr +i /etc/sysconfig/syslog`
6. Examine the current attributes on the applicable configuration file you edited:
   - `lsattr /etc/syslog.conf`
   - `lsattr /etc/sysconfig/syslog`
7. Restart the Syslog service:

   ```
   service syslog restart
   ```

Warning - While the Syslog configuration files are immutable:

- Gaia OS cannot save the changes in the Syslog configuration you make in Gaia Portal or Gaia Clish.
- Gaia OS cannot restore a Gaia Backup.

To remove the immutable attribute from a file, use this command:

```
chattr -i <file>
```

Redirecting RouteD System Logging Messages

It is possible to configure the RouteD daemon to write its log messages (for example, OSPF or BGP errors) to one of these log files:

Log File	Description
`/var/log/routed_messages`	Dedicated file that contains only the RouteD log messages. In Gaia versions R80 and higher, the RouteD writes to this file by default.
`/var/log/messages`	This file contains log messages from different daemons and from the operating system. In Gaia versions R77.30 and lower, the RouteD writes to this file by default. **Important** - When you upgrade Gaia from R77.30 and lower, the RouteD continues to write to this file. **Best Practice** - Configure the RouteD to write its log messages to the `/var/log/routed_messages` file.

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- When you change this configuration, it is **not** necessary to restart the RouteD daemon, or reboot.

Configuration in the Gaia Portal

Step	Instructions
1	From the left navigation tree, click **Advanced Routing** > **Routing Options**.
2	In the **Routing Process Message Logging Options** section, select **Log Routed Separately**.
3	In the **Maximum File Size** field, enter the size (in megabytes) for each log file. The default size is 1 MB. When the active log file `/var/log/routed_messages` reaches the maximal configured size, the Gaia OS rotates it and creates the new `/var/log/routed_messages` file.
4	In the **Maximum Number of Files** field, enter the maximal number of log files to keep. The default is to keep 10 log files: ■ `/var/log/routed_messages` ■ `/var/log/routed_messages.0` ■ `/var/log/routed_messages.1` ■ ... ■ `/var/log/routed_messages.9` If the number of all log files reaches the maximal configured number, the Gaia OS deletes the oldest file, and rotates the existing files. The file names end with a number suffix. The greater the suffix number, the older the file.
5	Click **Apply**.

Configuration in Gaia Clish

Step	Instructions
1	Connect to the command line on Gaia.
2	Log in to Gaia Clish.
3	Enable the logging of RouteD messages to a dedicated log file: `set routedsyslog on`
4	Configure the size (in megabytes) for each log file: `set routedsyslog size <Number of MB between 1 and 2047>` The default size is 1 MB. When the active log file `/var/log/routed_messages` reaches the maximal configured size, the Gaia OS rotates it and creates the new `/var/log/routed_messages` file.
5	Configure the maximal number of log files to keep: `set routedsyslog maxnum <Number of Files between 1 and 4294967295>` The default is to keep 10 log files: ■ `/var/log/routed_messages` ■ `/var/log/routed_messages.0` ■ `/var/log/routed_messages.1` ■ ... ■ `/var/log/routed_messages.9` When the number of log files reaches the maximal configured number, the Gaia OS deletes the oldest log file and rotates the existing log files. The file names end with a number suffix. The greater the suffix number, the older the log file.
6	Save the configuration: `save config`

How to examine the configuration in CLI

Examine the configuration in Gaia Clish, or the Expert mode.

Shell	Command	Expected output

Gaia Clish	`show configuration routedsyslog`	■ If default values were used for "`maxnum`" and "`size`":
		`set routedsyslog on`
		■ If custom values were configured for "`maxnum`" and "`size`":
		`set routedsyslog on`
		`set routedsyslog maxnum <Configured_Value>`
		`set routedsyslog size <Configured_Value>`

Expert mode	`grep routedsyslog /config/active`	■ If default values were used for "`maxnum`" and "`size`":
		`routed:instance:default:routedsyslog t`
		■ If custom values were configured for "`maxnum`" and "`size`":
		`routed:instance:default:routedsyslog t`
		
		`routed:instance:default:routedsyslog:size <Configured_Value>`
		
		`routed:instance:default:routedsyslog:files <Configured_Value>`

Configuring Log Volume

If there is enough available disk space, you can increase the size of the log partition.

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

Use the **lvm_manager** tool in the Expert mode.

Step	Instructions
1	Connect to the Gaia system **over console**.
2	Reboot: `reboot`
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: `lvm_manager`
7	Reboot: `reboot`

Network Access

Introduction

Telnet is **not** recommended for remote login, because it is not secure.

SSH, for example, provides much of the functionality of Telnet with good security.

Network access to Gaia using Telnet is disabled by default. You can allow Telnet access.

Configuring Telnet Access in Gaia Portal

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

Configuring Telnet Access in Gaia Clish

Syntax

- To configure Telnet access:

```
set net-access telnet {on | off}
```

- To show the configured Telnet access:

```
show net-access telnet
```

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

Host Access

You can configure hosts or networks that are allowed to connect to the Gaia Portal or Gaia Clish on the Gaia device.

Configuring Allowed Gaia Clients in Gaia Portal

Step	Instructions
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 IPv4 address of one host. ■ **Network** - Enter the IPv4 address of a network and subnet mask.
4	Click **OK**.

Configuring Allowed Gaia Clients in 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
gaia>
```

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 *R80.40 Gaia Advanced Routing Administration Guide*.

User Management

This chapter describes how to manage passwords, user accounts, roles, authentication servers, system groups, and Gaia Portal clients.

Note - When a user logs in to Gaia, the Gaia Portal navigation tree displayed and Gaia Clish commands that are available depend on the role or roles assigned to the user. If the user's roles do not provide access to a feature, the user does not see the feature in the Gaia Portal navigation tree or in the list of commands. If the user has read-only access to a feature, they can see the Gaia Portal page, but the controls are disabled. Similarly, the user can run "`show` commands, but not "`set`", "`add`" or "`delete`" commands.

Change My Password

A Gaia user can change their Gaia password.

Changing My Password in Gaia Portal

Step	Instructions
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 in 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:

User	Description
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 the new users can log in.

Notes:

- You can assign permissions to all Gaia features or a subset of the features without assigning a user ID of 0.
  If you assign a user ID of 0 to a user account (you can do this only in the Gaia Clish), the user is equivalent to the Admin user and the roles assigned to that account cannot be modified.
- Do not define a new user for external users.
  An external user is one that is configured on an authentication server (such as RADIUS or TACACS), and not on the local Gaia system.

When you create a user, you can add predefined roles (privileges) to the user. For more information, see *"Roles" on page 316*.

Warning - A user with read and write permission to the Users feature can change the password of another user, or an admin user. Therefore, write permission to the Users feature should be assigned with caution.

Managing User Accounts in Gaia Portal

Viewing the list of all configured users

In the navigation tree, click **User Management** > **Users**.

You can also see your username in the top right corner of the Gaia Portal.

Adding a new user

Step	Instructions
1	In the navigation tree, click **User Management** > **Users**.
2	Click **Add**.
3	In the **Login Name** field, enter the username. The valid characters (between 1 and 32 characters) are alphanumeric characters, dash (-), and underscore (_).
4	In the **Password** field, enter 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 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 sub-directory of `/home/` directory. If the sub-directory does not already exist, it is created.
8	In the **Shell** field, select the user's default login shell. See the explanations in the **"Login Shells"** section below.
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.

Step	Instructions
10	**Optional:** In the **UID** field, enter or select the applicable User ID: ■ **0** for administrator users (this is the default option) ■ An integer between **103** and **65533** for non-administrator users (for example, for users with the default shell `/usr/bin/scponly` - see sk88981)
11*	In the **Access Mechanisms** section: ■ 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: i. Press and hold the **CTRL** key on the keyboard. ii. 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 configure these settings in Gaia Clish, see *"Configuring Roles in Gaia Clish" on page 321*.

Login Shells

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** in the assigned roles makes it possible to add more Linux commands that can be used (see *"List of Available Extended Commands in Roles" on page 346*). 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.

Shell	Description
`/bin/csh`	CSH Linux shell. User can run the `clish` command to enter the Gaia Clish.
`/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. Other commands are forbidden.
`/sbin/nologin`	User is not allowed to log in to Gaia.
`/bin/p1shell`	Obsolete. Do **not** use this option anymore. **Important** - The `p1shell` is **not** supported (Known Limitation PMTR-45085).

Changing the user configuration

Step	Instructions
1	In the navigation tree, click **User Management** > **Users**.
2	Select the user.
3	Click **Edit**.
4	In the **Real Name** field, enter the user's real name or other informative text.
5	In the **Home Directory** field, enter the user's home directory.
6	In the **Shell** field, select the user's default login shell.
7	Select **User must change password at next logon**, if you wish to force the user to change the configured password during the next login.
8	In the **Available Roles** list, select the roles you wish to assign to this user and click **Add >**.
9	In the **Assigned Roles** list, select the roles you wish to remove from this user and click **Remove >**.
10	Click **OK**.

Note - For the default users **admin** and **monitor**, you can only change the Shell and Roles.

Deleting a user

Step	Instructions
1	In the navigation tree, click **User Management** > **Users**.
2	Select the user.
3	Click **Delete**.
4	Click **OK** to confirm.

Note - You cannot delete the default users **admin** and **monitor**.

Managing User Accounts in Gaia Clish

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

Syntax

Adding a local user account

```
add user <UserName> uid <User ID> homedir <Path>
```

Adding a RADIUS user account

```
add user <UserName> uid 0 homedir <Path>
```

Editing a user account

```
set user <UserName>
      force-password-change {yes | no}
      gid <System Group ID>
      homedir <Path>
      lock-out off
      newpass <Password>
      password
      password-hash <Password Hash>
      realname <Name>
      shell <Login Shell>
      uid <User ID>
```

Note - For the default users **admin** and **monitor**, you can only change the Shell and Roles.

Viewing the summary information about all users

```
show users
```

Viewing information about a specific user

```
show user <UserName>
      [force-password-change]
      [gid]
      [homedir]
      [lock-out]
      [realname]
      [shell]
      [uid]
```

Deleting a configured user

```
delete user <User ID>
```

Note - You cannot delete the default users **admin** and **monitor**.

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

Parameters

CLI Parameters

Parameter	Description
`user <UserName>`	Configures unique login username - an alphanumeric string, from 1 to 32 characters long, that can contain dashes (-) and underscores (_), but not spaces: `a-z A-Z 0-9 - _`
`uid <User ID>`	Optional. Configures unique User ID to identify permissions of the user: ■ `0` for administrator users and RADIUS user account (this is the default option) ■ An integer between `103` and `65533` for non-administrator user **Notes:** • Configure this UID for users with the default shell `/usr/bin/scponly` - see sk88981. • If you do not enter a value, Gaia OS automatically assigns the next free sequential number.
`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 sub-directory of the `/home/` directory. If the sub-directory 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, use the value "`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.

Parameter	Description
`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. Gaia does not ask 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 is not visible on the terminal command line.

Parameter	Description
`password-hash <Password Hash>`	The password as an MD5, SHA256, or SHA512 salted hash instead of plain text (the password string must contain at least 6 characters). Use this option when you upgrade or restore using backup scripts. You can generate the hash of the password with the "`cpopenssl`" command (run: `cpopenssl passwd -help`). To configure the default hash algorithm, see: ■ *"Password Hashing Algorithm" on page 359* (in Gaia Portal) ■ *"Configuring Hashing Algorithm" on page 368* (in Gaia Clish) **Best Practice** - Do **not** use MD5 hash because it is not secure. **Notes:** ■ Format: `$<Hash Standard>$<Salt>$<Encrypted>` ■ The length of this hash string must be less than 128 characters. ■ *<Hash Standard>* One of these digits: • `1` = MD5 • `5` = SHA256 • `6` = SHA512 ■ *<Salt>* A string of these characters: `a-z A-Z 0-9 . / [ ] _ ` ^` The length of this string must be between 2 and 16 characters. ■ *<Encrypted>* A string of these characters: `a-z A-Z 0-9 . / [ ] _ ` ^` The length of this string must be: • For MD5, less than 22 characters. • For SHA256, less than 43 characters. • For SHA512, less than 86 characters.
`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 the capitalized first letter.
`shell <Login Shell>`	Configures the user's default login shell. See the explanations in the "**Login Shells**" section below.

Login Shells

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** in the assigned roles makes it possible to add more Linux commands that can be used (see *"List of Available Extended Commands in Roles" on page 346*). 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.
`/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. Other commands are forbidden.
`/sbin/nologin`	User is not allowed to log in to Gaia.
`/bin/p1shell`	Obsolete. Do **not** use this option anymore. **Important** - The `p1shell` is **not** supported (Known Limitation PMTR-45085).

Roles

Role-based administration (RBA) lets you create administrative roles for users. With RBA, an administrator can allow Gaia users to access specified features by including those features in a role and assigning that role to users. Each role can include a combination of administrative (read/write) access to some features, monitoring (read-only) access to other features, and no access to other features.

You can also specify which access mechanisms (Gaia Portal, or Gaia Clish) are available to the user.

Note - When users log in to the Gaia Portal, they see only those features to which they have read-only or read/write access. If they have read-only access to a feature, they can see the settings pages, but cannot change the settings.

Gaia includes these predefined roles:

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

Notes:

- You *cannot* delete or change the predefined roles.
- Do **not** define a new user for external users.
  An external user is one that is configured on an authentication server (such as RADIUS or TACACS), and not on the local Gaia system.

Configuring Roles in Gaia Portal

You define roles on the **User Management** > **Roles** page of the Gaia Portal.

This page also shows a list of existing roles.

To add a new role

Step	Instructions
1	In the navigation tree, click **User Management** > **Roles**.
2	Click **Add**.
3	In the **Role Name** field, enter the applicable name. 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 *"List of Available Features in Roles" on page 326*.
5	On the **Extended Commands** tab: Select the commands you wish to configure in this role. ■ To select several commands: a. Press and hold the **CTRL** key on the keyboard. b. Left-click the applicable commands (in the **Name**, **Description**, or **Path** column). The selected commands become highlighted. c. In the top right corner, select the option **Check selected as**. The checkboxes of the selected commands become checked. ■ To clear several selected commands: a. Press and hold the **CTRL** key on the keyboard. b. Left-click the applicable commands (in the **Name**, **Description**, or **Path** column). The selected commands become highlighted. c. In the top right corner, clear the option **Check selected as**. The checkboxes of the selected commands become cleared. See *"List of Available Extended Commands in Roles" on page 346*.
6	Click **OK**.

To change features and commands in an existing role

Step	Instructions
1	In the navigation tree, click **User Management** > **Roles**.
2	Select the role.
3	Click **Edit**.
4	On the **Features** tab: 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!
5	On the **Extended Commands** tab: Select the commands you wish to configure in this role. ■ To select several commands: a. Press and hold the **CTRL** key on the keyboard. b. Left-click the applicable commands (in the **Name**, **Description**, or **Path** column). The selected commands become highlighted. c. In the top right corner, select the option **Check selected as**. The checkboxes of the selected commands become checked. ■ To clear several selected commands: a. Press and hold the **CTRL** key on the keyboard. b. Left-click the applicable commands (in the **Name**, **Description**, or **Path** column). The selected commands become highlighted. c. 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	Instructions
1	In the navigation tree, click **User Management** > **Roles**.
2	Select the role.
3	Click **Delete**.
4	Click **OK** to confirm.

Note - You cannot delete the default roles **adminRole** and **monitorRole**.

To assign users to a role

Step	Instructions
1	In the navigation tree, click **User Management** > **Roles**.
2	Select the role.
3	Click **Assign Members**.
4	In the **Available Users** list, left-click the user you wish to add to the role. 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	Instructions
1	In the navigation tree, click **User Management** > **Roles**.
2	Select the role.
3	Click **Assign Members**.
4	In the **Users with Role** list, left-click the user you wish to remove from the role. 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 on the **Users** page (see *"Users" on page 306*).

Configuring Roles in Gaia Clish

You can:

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

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 configured roles.
- You cannot delete the default roles **adminRole** or **monitorRole**.

Parameters

CLI Parameters

Parameter	Description
`role <Role Name>`	Role name as a character string that contains letters, numbers or the underscore (_) character. The role name must start with a letter.
`domain-type System`	Reserved for future use.

Parameter	Description
`virtual-system-access {0 | all | VSID1, VSID2, ..., VSIDn}`	Specifies which VSX Virtual Systems this role can access: ■ `0` - Access only to VSX Gateway (VSX Cluster Member) itself (context of 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 is equivalent to the **admin** role!
`readonly-features <List of RO Features>`	A comma-separated list of Gaia features that have read-only permissions in the specified role. See: ■ *"List of Available Features in Roles" on page 326* ■ *"List of Available Extended Commands in Roles" on page 346* **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.

Parameter	Description
`readwrite-features <List of RW Features>`	A comma-separated list of Gaia features that have read-write permissions in the specified role. See: ■ *"List of Available Features in Roles" on page 326* ■ *"List of Available Extended Commands in Roles" on page 346* **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

Table: List of Available Features in Roles

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

Authentication Servers	`aaa-servers`	Configure authentication through external RADIUS or TACACS+ server.	`set aaa radius-servers *`
			`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 *`

Table: List of Available Features in Roles (continued)

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

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.	`cpca_client`
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 *`

Cloning Group Management	`CloningGroupMana gement`	Control management of Gaia Cloning Groups.	`set cloning-group- management *`

Cloud Config	`cloud-config`	Control of Zero Touch.	`show cloud-config *`
			`set cloud-config *`
			`delete cloud-config *`

Table: List of Available Features in Roles (continued)

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

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 *`

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
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.	N / A

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
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 OS to Factory Defaults.	`set fcd *` `show fcd *`
Firewall Management	`firewall_management`	Control Login and Logout from Management Server.	`mgmt *`

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
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 all` `cpstat -f sensors os`

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 *`
IGMP	`igmp`	Control multicast group memberships through the Internet Group Management Protocol (IGMP).	`set igmp *` `show igmp *`

Table: List of Available Features in Roles (continued)

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

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
IP Broadcast Helper	`iphelper`	Control forwarding of UDP broadcast traffic to other interfaces.	`set iphelper *` `show iphelper *`
IP Reachability Detection	`ipreachdetect`	Control reachability of IP Addresses.	`set ip-reachability-detection *` `show ip-reachability-detection *`
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`
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 *`

Table: List of Available Features in Roles (continued)

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

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".	`cplic`
License Configuration	`license`	Access to "Manage License".	`cplic`
Lights Out Management (LOM) Configuration	`lom`	Show Lights Out Management (LOM) Configuration.	`show lom *`
Mail Notification	`ssmtp`	Control mail notifications sent by Gaia.	`set mail-notification *` `show mail-notification *`
Management Interface	`management_ interface`	Control which interface is used for management (main interface).	`set management *` `show management *`

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

Table: List of Available Features in Roles (continued)

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

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 *`

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 *`

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

Table: List of Available Features in Roles (continued)

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

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

Table: List of Available Features in Roles (continued)

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

Policy Based Routing	`pbr-combine-static`	Control policy based routing rules and action tables.	`set pbr *`
			`set pbrroute *`
			`show pbr *`
			`show pbrroute *`

Policy Routing	`pbr-routing-group`	Overview page for Policy Based Routing.	`set pbr *`
			`set pbrroute *`
			`show pbr *`
			`show pbrroute *`

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.	`raidconfig` `raid_diagnostic`
RIP	`rip`	Control dynamic routing through the Routing Information Protocol for IPv4 (RIP).	`set rip *` `show rip *`

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
RIPng	`ripng`	Control dynamic routing through the Routing Information Protocol for IPv6 (RIPng).	`set ipv6 ripng *` `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 *`

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

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
Route Redistribution	`export`	Control advertisement of IPv4 routing information from one protocol to another.	`set route-redistribution *`
Route Redistribution	`export6`	Control advertisement of IPv6 routing information from one protocol to another.	`set ipv6 route-redistribution *`
Routed ClusterXL	`routed-cluster`	Control how RouteD daemon interacts with ClusterXL on Gaia.	`set routed-clusterxl *` `show routed-clusterxl *`
Router Discovery	`rdisc`	Control ICMP Router Discovery on Gaia.	`set rdisc *` `show rdisc *`
Routing Monitor	`show-route-all`	View summary information about routes on Gaia.	`show route *`

Table: List of Available Features in Roles (continued)

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

Routing 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 *`

SAM (Accelerator Card)	`sam`	Deprecated - SAM card is not supported. 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.	N / A

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
Security Management GUI Clients	`mgmt-gui-clients`	Control allowed Security Management GUI Clients.	
Shutdown	`reboot_halt`	Shut down and reboot the Gaia.	`halt *` `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.	For more information, see sk92449.
			`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 *`

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
System Asset	`asset`	Show hardware asset summary.	`show asset *`

System Backup	`backup`	Create backup of the Gaia system for events of data loss.	`add backup *`
			`set backup *`
			`backup *`
			`restore *`
			`delete backup *`
			`show backups`
			`show backup *`
			`show restore *`

System Configuration	`sysconfig`	System Configuration.	`show configuration *`

System Groups	`group`	Control Gaia OS 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 Status	`sysenv`	Hardware sensor monitoring.	`show sysenv *`
TACACS_Enable	`tacacs_enable`	Control TACACS+ mechanism on Gaia.	`tacacs_enable *` `show tacacs_enable *`

Table: List of Available Features in Roles (continued)

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

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

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

Upgrades (CPUSE)	`installer`	CPUSE - Show the update packages status and manage package downloads and installations on Gaia.	For more information, see sk92449.
			`show installer *`
			`add installer *`
			`installer *`
			`set installer *`

Upgrades (CPUSE)	`software-updates-group`	Overview page for CPUSE.	For more information, see sk92449.
			`show installer *`
			`set installer *`
			`installer agent *`

Users	`user`	Control user accounts on Gaia.	`add user *`
			`set user *`
			`delete user *`
			`show user *`
			`show users *`

Table: List of Available Features in Roles (continued)

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

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 *`

Table: List of Available Features in Roles (continued)

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

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 / Gaia gClish	Description
api	ext_api	Starts, stops, or checks the status of the API server
config_system	ext_config_system	Runs the Gaia First Time Configuration tool in Expert mode.
cp_conf	ext_cp_conf	Runs the Check Point configuration utility for some local settings.
cpca	ext_cpca	Runs the Check Point Internal Certificate Authority (ICA).
cpca_client	ext_cpca_client	Controls the Check Point Internal Certificate Authority (ICA).
cpca_create	ext_cpca_create	Creates the Check Point Internal Certificate Authority (ICA) database.
cpca_dbutil	ext_cpca_dbutil	Controls the Check Point Internal Certificate Authority (ICA) database.
cpconfig	ext_cpconfig	Runs the Check Point Configuration Tool for Security Management Server and Security Gateway.
cphaprob	ext_cphaprob	Access to clustering commands.
cphastart	ext_cphastart	Enables the clustering feature on Security Gateway.
cphastop	ext_cphastop	Disables the clustering feature on Security Gateway.
cpinfo	ext_cpinfo	Collects the Check Point diagnostics information.
cplic	ext_cplic	Controls the Check Point licenses.
cpshared_ver	ext_cpshared_ver	Shows the Check Point SVN Foundation version.
cpstart	ext_cpstart	Starts the installed Check Point products.

Command name in Gaia Portal	Command name in Gaia Clish / Gaia gClish	Description
cpstat	ext_cpstat	Shows the Check Point statistics history information for Software Blades and Gaia.
cpstop	ext_cpstop	Stops the installed Check Point products.
cpview	ext_cpview	Shows the advanced Check Point statistics information for Software Blades and Gaia in real-time.
cpwd_admin	ext_cpwd_admin	Controls the Check Point WatchDog administration tool.
diag	ext_diag	Sends the system diagnostics information.
dtps	ext_dtps	Controls the Endpoint Policy Server commands.
etmstart	ext_etmstart	Starts the QoS Software Blade.
etmstop	ext_etmstop	Stops the QoS Software Blade.
fgate	ext_fgate	Controls the QoS Software Blade.
fips	ext_fips	Controls the FIPS mode.
fw	ext_fw	Access to Security Gateway commands for IPv4.
fw6	ext_fw6	Access to Security Gateway commands for IPv6.
fwaccel	ext_fwaccel	Access to SecureXL commands for IPv4.
fwaccel6	ext_fwaccel6	Access to SecureXL commands for IPv6.
fwm	ext_fwm	Access to Security Management commands.
ifconfig	ext_ifconfig	Deprecated. Use "show interface", or "set interface" commands instead.
ips	ext_ips	Controls the IPS Software Blade.
lomipset	ext_lomipset	Configures the LOM Card IP address.

Command name in Gaia Portal	Command name in Gaia Clish / Gaia gClish	Description
LSMcli	ext_LSMcli	Access to SmartProvisioning command line.
LSMenabler	ext_LSMenabler	Enables the SmartProvisioning.
mds_backup	ext_mds_backup	Creates backup of the Multi-Domain Server.
mds_restore	ext_mds_restore	Restores the backup of the Multi-Domain Server.
mdscmd	ext_mdscmd	Access to Multi-Domain Server command line.
mdsconfig	ext_mdsconfig	Runs the Check Point Configuration Tool for Multi-Domain Server.
mdsstart	ext_mdsstart	Starts the Multi-Domain Server.
mdsstart_ customer	ext_mdsstart_ customer	Starts a specific Domain Management Server.
mdsstat	ext_mdsstat	Shows the status of the Multi-Domain Server and all Domain Management Servers.
mdsstop	ext_mdsstop	Stops the Multi-Domain Server.
mdsstop_ customer	ext_mdsstop_ customer	Stops a specific Domain Management Server.
netstat	ext_netstat	Shows network connections, routing tables, and interface statistics.
ping	ext_ping	Sends pings to a host using IPv4.
ping6	ext_ping6	Sends pings to a host using IPv6.
raid_diagnostic	ext_raid_ diagnostic	Access to RAID Monitoring tool.
raidconfig	ext_raidconfig	Access to RAID Configuration and Monitoring tool.
rtm	ext_rtm	Controls the Monitoring Software Blade.

Command name in Gaia Portal	Command name in Gaia Clish / Gaia gClish	Description
rtmstart	ext_rtmstart	Starts the Monitoring Software Blade.
rtmstop	ext_rtmstop	Stops the Monitoring Software Blade.
rtmtopsvc	ext_rtmtopsvc	Monitors top services using the Monitoring Software Blade.
SDSUtil	ext_SDSUtil	Access to Software Distribution Server utility.
sim	ext_sim	Access to SecureXL SIM device commands for IPv4.
SnortConvertor	ext_ SnortConvertor	Access to the IPS Snort conversion tool.
tecli	ext_tecli	Access to the Threat Emulation Software Blade shell.
top	ext_top	Shows the most active system processes.
traceroute	ext_traceroute	Runs the trace tool.
vpn	ext_vpn	Controls the VPN kernel module for IPv4.
vpn6	ext_vpn6	Controls the VPN kernel module for IPv6.
vsx_util	ext_vsx_util	Controls the managed VSX Gateways and VSX Clusters on a Management Server.

Password Policy

This section explains how to configure your platform:

- To enforce creation of strong passwords.
- To monitor and prevent use of already used passwords.
- To force users to change passwords at regular intervals.

One of the important elements of securing your Check Point cyber security platform is to set user passwords and create a good *password policy*.

Note - The password policy does not apply to non-local users that authentication servers such as RADIUS manage their login information and passwords. In addition, it does not apply to non-password authentication, such as the public key authentication supported by SSH.

To set and change user passwords, see *"Users" on page 306* and *"User Management" on page 304*.

Password Strength

Strong, unique passwords that use a variety of character types and require password changes, are key factors in your overall cyber security.

Password History Checks

The *password history* feature prevents users from using a password they have used before when they change their password.

The number of already used passwords that this feature checks against is defined by the *history length*.

Password history check is enabled by default.

The password history check:

- Applies to user passwords set by the administrator and to passwords set by the user.
- Does not apply to SNMPv3 USM user pass phrases.

These are some considerations when using password history:

- The password history for a user is updated only when the user successfully changes password.

  If you change the history length, for example: from ten to five, the stored passwords number does not change.

  Next time the user changes password, the new password is examined against all stored passwords, maybe more than five.

  After the password change succeeds, the password file is updated to keep only the five most recent passwords.
- The password history is only stored if the password history feature is enabled when the password is created.
- The new password is checked against the previous password, even if the previous password is not stored in the password history.

Mandatory Password Change

The *mandatory password change* feature requires users to use a new password at defined intervals.

Forcing users to change passwords regularly is important for a strong security policy.

You can set user passwords to expire after a specified number of days.

When a password expires, the user is forced to change the password the next time the user logs in.

This feature works together with the password history check to get users to use new passwords at regular intervals.

The mandatory password change feature does not apply to SNMPv3 USM user pass phrases.

Denying Access to Unused Accounts

You can deny access to unused accounts. If there were no successful login attempts within a set time, the user is locked out and cannot log in.

You can also configure the allowed number of days of non-use before a user is locked-out.

Denying Access After Failed Login Attempts

You can deny access after too many failed login attempts. The user cannot log in during a configurable time.

You can also allow access again after a user was locked out.

In addition, you can configure the number of failed login attempts that a user is allowed before being locked out.

When one login attempt succeeds, counting of failed attempts stops, and the count is reset to zero.

Configuring Password Policy in Gaia Portal

In This Section:

Procedure 353
Password Strength 354
Password History 355
Mandatory Password Change 356
Denying Access to Unused Accounts 357
Denying Access After Failed Login Attempts 358
Password Hashing Algorithm 359

Procedure

Step	Instructions
1	In the navigation tree, click **User Management** > **Password Policy**.
2	Configure the password policy options: ■ **Password Strength** (see *"Password Strength" on the next page*) ■ **Password History** (see *"Password History" on page 355*) ■ **Mandatory Password Change** (see *"Mandatory Password Change" on page 356*) ■ **Deny Access to Unused Accounts** (see *"Denying Access to Unused Accounts" on page 357*) ■ **Deny Access After Failed Login Attempts** (see *"Denying Access After Failed Login Attempts" on page 358*) ■ **Password hashing algorithm** (see *"Password Hashing Algorithm" on page 359*)
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 (default) ■ `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.

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, does 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 is unable to log in - the user is 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

Denying 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

Denying Access After Failed Login Attempts

Parameter	Description
Deny access after failed login attempts	If the configured limit is reached, the user is locked out (unable to log in) for a configured time. **Warning** - Enabling this leaves you open to a "denial of service" - if an attacker makes unsuccessful login attempts often enough, the affected user account is locked out. Consider the advantages and disadvantages of this option, in light of your security policy, before enabling it. ■ **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 fail. When one login attempt succeeds, counting of failed attempts stops, and the count is reset to zero. ■ **Range**: 2 - 1000 ■ **Default**: 10

Parameter	Description
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

Password Hashing Algorithm

Parameter	Description
Password hashing algorithm	Configures the hashing algorithm to store new passwords in the Gaia database. ■ **Range**: `MD5`, `SHA256`, or `SHA512` ■ **Default**: `MD5`

Configuring Password Policy in Gaia Clish

In This Section:

Password Strength 360
Password History 362
Mandatory Password Change 363
Denying Access to Unused Accounts 365
Denying Access After Failed Login Attempts 366
Configuring Hashing Algorithm 368

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
```

Parameters

Parameter	Description
`complexity <1-4>`	The required number of character types: ■ `1` - Don't check ■ `2` - Require two character types (default) ■ `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**: 2
`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
```

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
```

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 is unable to log in - the user is 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, does not see this warning. ■ **Range**: 1 - 366 ■ **Default**: 7

Parameter	Description
`force-change-when {no | password}`	Forces a user to change password at first login, after the user's password was changed using the command "`set user <UserName> password`", or from the Gaia Portal **User Management** > **Users** page. ■ **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`

Note - To see when Gaia OS changed the password for a specific user, run this command in the Expert mode:

```
date -d @"$(dbget passwd:<username>:lastchg)"
```

- The command "`dbget passwd:<username>:lastchg`" returns the time stamp in the Epoch format.
- The command "`date -d @<Epoch Time>`" converts it to the human-readable time stamp.

Example:

```
[Expert@MyGaia:0] date -d @"$(dbget
passwd:admin:lastchg)"
Mon May 24 15:39:46 UTC 2021
[Expert@MyGaia:0]
```

Denying Access to Unused Accounts

Syntax

- To configure the denial of access to unused accounts based on the number of days:

```
set password-controls deny-on-nonuse
      allowed-days <30-1827>
      enable {on | off}
```

- To show the configured denial of access to unused accounts:

```
show password-controls deny-on-nonuse
```

```
show password-controls all
```

Parameters

Parameter	Description
`deny-on-nonuse allowed-days <30-1827>`	Configures the number of days of non-use before locking out the unused account. This only takes effect, if the "`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`

Denying Access After Failed Login Attempts

Syntax

- To configure the denial of access to unused accounts based on the number of failed login attempts:

```
set password-controls deny-on-fail
      allow-after <60-604800>
      block-admin {on | off}
      enable {on | off}
      failures-allowed <2-1000>
```

- To show the configured denial of access to unused accounts:

```
show password-controls deny-on-fail
```

```
show password-controls all
```

Parameters

Parameter	Description
`allow-after <60-604800>`	Allow access again after a user was locked out (due to failed login attempts). 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`

Parameter	Description
`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 is 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 fail. When one login attempt succeeds, counting of failed attempts stops, and the count is reset to zero, ■ **Range:** 2 - 1000 ■ **Default:** 10

Configuring Hashing Algorithm

Syntax

- To configure the hashing algorithm:

```
set password-controls password-hash-type {MD5 | SHA256 |
SHA512}
```

- To show the configured hashing algorithm:

```
show password-controls password-hash-type
```

```
show password-controls all
```

Parameters

Parameter	Description
`{MD5 | SHA256 | SHA512}`	Configures the hashing algorithm to store new passwords in the Gaia database. ■ **Range**: `MD5`, `SHA256`, or `SHA512` ■ **Default**: `MD5`

Monitoring Password Policy in Gaia Clish

Syntax

```
show password-controls
      all
      complexity
      deny-on-fail
            allow-after
            block-admin
            enable
            failures-allowed
      deny-on-nonuse
            allowed-days
            enable
      expiration-lockout-days
      expiration-warning-days
      force-change-when
      history-checking
      history-length
      min-password-length
      palindrome-check
      password-expiration
      password-hash-type
```

Example

```
gaia> show password-controls all

Password Strength
    Minimum Password Length 6
    Password Complexity 2
    Password Palindrome Check on

Password History
    Password History Checking off
    Password History Length 10

Mandatory Password Change
    Password Expiration Lifetime 5
    Password Expiration Warning Days 8
    Password Expiration Lockout Days never
    Force Password Change When no

Configuration Deny Access to Unused Accounts
    Deny Access to Unused Accounts off
    Days Nonuse Before Lockout 365

Configuration Password hash
    Password hashing algorithm MD5
gaia>
```

Configuring SSH Authentication with RSA Key Files

Prerequisites

- Console access / LOM access to the Gaia server
- Administrator access to the Gaia server, or an equivalent user with the required permission
- The Gaia server must run version R80.40 with Take 83, or a higher version.

Notes:

- For the initial setup, it is necessary to do each step only one time.
- To configure more SSH users, it is necessary to do only steps 1 through 7.

Procedure

1. Create a pair of SSH keys.

   You can use these tools:

   - On a Windows OS computer - the PuTTYgen tool.
   - On the Gaia server (or on a OS computer) - the "`ssh-keygen`" command.

     Important:
     - To use the "`ssh-keygen`" command on the Gaia server:
       a. Connect to the command line and log in to the Expert mode.
       b. Save the pair of key files in some directory.
     - Save the private SSH key file on your SSH client computer.
     - You configure the public SSH key on the Gaia server later.

2. Configure a new user on the Gaia server for the SSH connection and assign the administrator role.

   You can create and configure a new user in Gaia Portal or Gaia Clish.

- In Gaia Portal:

  Create a new user with these settings:

  - Default shell: `/bin/bash`
  - Assigned Role: `adminRole` (you can create another more limited role)

    In our example, the username is: `filecopy`

    See:

    - *"Managing User Accounts in Gaia Portal" on page 307*
    - *"Configuring Roles in Gaia Portal" on page 317*

  In Gaia Clish:

  a. Create a new user.

     See *"Managing User Accounts in Gaia Clish" on page 311*.

     Example:

```
MyGW> add user filecopy uid 103 homedir
/home/filecopy
WARNING Must set password and a role before user can
login.
- Use 'set user USER password' to set password.
- Use 'add rba user USER roles ROLE' to set a role.
MyGW> set user filecopy password
New password:
Verify new password:

MyGW>
```

  b. Assign the administrator role to the new user.

     See *"Configuring Roles in Gaia Clish" on page 321*

     Note - You can create another more limited role.

     Example:

```
MyGW> add rba user filecopy roles adminRole
```

c. Configure the default shell /bin/bash for the new user.

   See *"Configuring Roles in Gaia Clish" on page 321*.

   Example:

```
MyGW> set user filecopy shell /bin/bash
```

d. Save the configuration:

```
MyGW> save config
```

3. Connect with an SSH client to the Gaia server.
4. Log in with the new user.

   In our example, the username is: `filecopy`.
5. Make sure you are in the home directory:

```
cd ~ ; pwd
```

6. Configure the required directory "`.ssh`":
   a. Create the directory "`.ssh`":

```
mkdir -v .ssh
```

   b. Assign the required permissions to the new directory "`.ssh`":

```
chmod -v u=rwx,g=,o= ~/.ssh
```

7. Configure the required file "`authorized_keys`":
   a. Create the required file "`authorized_keys`":

```
touch ~/.ssh/authorized_keys
```

   b. Assign the required permissions to the new file "`authorized_keys`":

```
chmod -v u=rw,g=,o= ~/.ssh/authorized_keys
```

   c. Edit the "`authorized_keys`" file:

```
vi ~/.ssh/authorized_keys
```

   d. Paste the SSH key you created earlier into this file.
   e. Save the changes in the file and exit the editor.

8. Make the required changes in the SSH configuration template for the GaiaOperating System:
   a. Back up the `sshd_config.templ` file:

      ```
      cp -v /etc/ssh/templates/sshd_config.templ{,_BKP}d
      ```

   b. Edit the `sshd_config.templ` file:

      ```
      vi /etc/ssh/templates/sshd_config.templ
      ```

   c. At the bottom of the file, change the line:

      from

      ```
      PasswordAuthentication yes
      ```

      to:

      ```
      PasswordAuthentication no
      ```

   d. Save the changes in the file and exit the editor.
9. Import the changes from the SSH configuration template into the running Gaia configuration:

   ```
   /usr/bin/sshd_template_xlate < /config/active
   ```

10. Restart the SSHD process:

    ```
    service sshd restart
    ```

11. Close the current SSH connection for the new user.
12. Connect with an SSH client to the Gaia server.
13. Log in with the new user with the private SSH key.

    In our example, the username is: `filecopy`

    Example:

    ```
    login as: filecopy
    This system is for authorized use only.
    Authenticating with public key "rsa-key-20230207"
    Last login: Sun Jul  2 15:08:58 2023 from 172.20.213.71
    [Expert@MyGW:0]#
    ```

Authentication Servers

You can configure Gaia to authenticate Gaia users even when they are not configured locally.

This is a good way of centrally managing the credentials of multiple Security Gateways.

To define non-local Gaia users, you define Gaia as a client of an authentication server.

Gaia supports these types of authentication servers:

Server	Description
RADIUS	RADIUS (Remote Authentication Dial-In User Service) is a client/server authentication system that supports remote-access applications. User profiles are kept in a central database on a RADIUS authentication server. Client computers or applications connect to the RADIUS server to authenticate users. 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 *R80.40 VSX Administration Guide*.

When you configure Gaia OS to use several authentication methods, it uses them in this order:

1. RADIUS
2. TACACS+
3. Local

Authentication flow when a user enters the credentials:

1. Authenticate the user on the configured RADIUS servers.
    - If successful, the user logs in.
    - If failed, go to the next step.
2. Authenticate the user on the configured TACACS+ servers.
    - If successful, the user logs in.
    - If failed, go to the next step.
3. Authenticate the user based on the local configuration.
    - If successful, the user logs in.
    - If failed, deny the login.

Configuring RADIUS Servers

In This Section:

Configuring RADIUS Servers in Gaia Portal 376
Configuring RADIUS Servers in Gaia Clish 378

Configuring RADIUS Servers in Gaia Portal

To configure a RADIUS server

Step	Instructions
1	In the navigation tree, click **User Management** > **Authentication Servers**.
2	In the **RADIUS Servers** section, click **Add**.
3	Enter the RADIUS Server parameters: ■ **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 configured on the Gaia matches the shared string configured 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	Instructions
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 configured in RFC 2865. If no NAS IP Address is chosen, the IPv4 address of the Gaia Management Interface is used (click **Network Management > Network Interfaces >** see the **Management Interface** section).
6	**Optional:** Select **RADIUS Users Default Shell** (for details about the shells, see *"Users" on page 306*). 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 (see *"Configuring RADIUS Servers for Non-Local Gaia Users" on page 382*).
8	Click **Apply**.

To edit a RADIUS server

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

To delete a RADIUS server

Step	Instructions
1	In the navigation tree, click **User Management** > **Authentication Servers**.
2	Select the RADIUS server.
3	Click **Delete**.
4	Click **OK** to confirm.

Configuring RADIUS Servers in Gaia Clish

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

CLI 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.

Parameter	Description
`prompt secret`	The system will prompt you to enter the Shared Secret.
`secret <Shared Secret>`	Configures the shared secret used for authentication between the RADIUS server and the Gaia. Enter the shared secret text string up to 256 characters, without any whitespace characters and without a backslash. Make sure that the shared string configured on the Gaia matches the shared string configured 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 *"Users" on page 306*).
`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 (see *"Configuring RADIUS Servers for Non-Local Gaia Users" on page 382*).
`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 configured in RFC 2865. 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	Instructions

1	Define the role for the RADIUS client:
	■ If no group is configured on the RADIUS server for the client, define this role:
	`radius-group-any`
	■ If a group is configured 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 *"Roles" on page 316*.

Note - Do **not** define a new user for external users. An external user is one that is configured 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 configured on a RADIUS server and not in Gaia.

When a non-local user logs in to Gaia, the RADIUS server authenticates the user and assigns the applicable permissions.

You must configure the RADIUS server to correctly authenticate and authorize non-local users.

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

To configure a RADIUS server for non-local Gaia users

In addition, see sk72940.

Step	Instructions
1	Copy the applicable dictionary file to your RADIUS server.

	Example for the "*Steel-Belted RADIUS server*"
	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"`

	Example for the "*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"`

Step	Instructions
	Example for the "*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`

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 configured 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 configured in the `/etc/passwd` file.

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

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

Configuring TACACS+ Servers

In This Section:

Configuring TACACS+ Servers in Gaia Portal 385
Configuring TACACS+ Servers in Gaia Clish 388
Checking if the Logged In User is Enabled for TACACS+ 390

Configuring TACACS+ Servers in Gaia Portal

To configure a TACACS+ server

Step	Instructions
1	In the navigation tree, click **User Management** > **Authentication Servers**.
2	In the **TACACS+ Configuration** section, select **Enable TACACS+ authentication**. This setting applies to all configured TACACS+ servers.
3	Click **Apply**.
4	In the **TACACS+ Servers** section, click **Add**.

Step	Instructions
5	Configure the TACACS+ parameters: ■ **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	Instructions
1	In the navigation tree, click **User Management** > **Authentication Servers**.

Step	Instructions
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	Instructions
1	In the navigation tree, click **User Management** > **Authentication Servers**.
2	In the **TACACS+ Servers** section, select a TACACS+ server.
3	Click **Delete**.
4	Click **OK** to confirm.

Configuring TACACS+ Servers in Gaia Clish

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 TACACS+ 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

CLI 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

Parameter	Description
`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
```

Checking if the Logged In User is Enabled for TACACS+

Procedure

Step	Instructions
1	Connect to the command line on Gaia.
2	Log in to Gaia Clish.
3	Run: `show tacacs_enable`

Configuring Gaia as a TACACS+ Client

Gaia acts as a TACACS+ client for Gaia users that are configured on the TACACS+ server and are not configured locally on Gaia.

The **admin** user must define a role called `TACP-0` for the TACACS+ users, and the allowed features for the `TACP-0` role.

Important:

1. All TACACS+ users must log in to Gaia OS with the password assigned to the default role `TACP-0`.
2. To get their applicable TACP role in Gaia OS, after this initial login, TACACS+ users must log in for the second time with the password assigned to their applicable TACP role.

Privilege Escalation

The Gaia admin user can define roles that make it possible for Gaia users to get temporarily higher privileges, than their regular privileges.

For example, Gaia user Fred needs to configure the interfaces, but his role does not support interfaces configuration. To configure the interfaces, Fred enters his user name together with a password given him by the admin user. This password lets him change his default role to the role that allows him to configure the interfaces.

There are sixteen different privilege levels (0 - 15) configured 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	Instructions
1	Connect to Gaia OS as the `admin` user.

Step	Instructions
2	Define the role `TACP-0`.
3	Define the features for the role. For instructions, see *"Roles" on page 316*.
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

You can raise the "TACP" privileges in either Gaia Portal, or Gaia Clish.

Raising "TACP" privileges in Gaia Portal

Step	Instructions
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.

Raising "TACP" privileges in Gaia Clish

Step	Instructions
1	Connect to the command line.
2	Log in to the Gaia Clish using the username and password of the TACACS+ user.
3	After you are authenticated by the TACACS server, you get 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.

Note - Do **not** define a new user for external users. An external user is one that is configured on an authentication server (such as RADIUS, or TACACS), and not on the local Gaia system.

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

Step	Instructions
1	Connect to the command line on Gaia.
2	Log in to Gaia Clish.
3	Run: `show tacacs_enable`

Configuring TACACS+ Servers for Non-Local Gaia Users

You can define Gaia users on a TACACS server instead of defining them on the Gaia computer.

Gaia users that are configured on a TACACS server are called non-local users.

Cisco ACS servers are the most commonly used TACACS+ servers.

For help with the configuration of a Cisco ACS server as a TACACS+ server for Gaia clients, see sk98733 (as an example of best practices and **not** a replacement for the official Cisco documentation).

When a non-local user logs in to Gaia, the TACACS server authenticates the user and assigns the permissions to the user.

You must configure the TACACS server to correctly authenticate and authorize non-local Gaia users.

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

System Groups

In This Section:

Introduction 395
Configuring System Groups in Gaia Portal 396
Configuring System Groups in Gaia Clish 398

Introduction

You can define and configure groups with Gaia as you can with equivalent Linux-based systems.

This function is retained in Gaia for advanced applications and for retaining compatibility with Linux.

Use groups for these purposes:

- Specify Linux file permissions.
- Control who can log in through SSH.

For other functions that are related to groups, use the role-based administration feature, described in *"Roles" on page 316*.

All users are assigned by default to the `users` group. You can edit a user's primary group ID (using Gaia Clish) to be something other than the default. However, you can still add the user to the `users` group. The list of members of the `users` group includes only users, who are explicitly added to the group. The list of does not include users added by default.

Configuring System Groups in Gaia Portal

To see a list of all groups

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

To add a System Group

Step	Instructions
1	In the navigation tree, click **User Management** > **System Groups**.
2	Click **Add**.
3	In the **Group Name** field, enter the applicable unique name - between 1 and 16 alphanumeric characters without spaces.
4	In the **Group ID** field, enter a unique Group ID number - between 101 and 65530: ■ 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	Instructions
1	In the navigation tree, click **User Management** > **System Groups**.
2	Select the System Group.
3	Click **Edit**.
4	In the **Available Members** list, select a user. 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.

Step	Instructions
6	Click **OK**.

To remove a user from a System Group

Step	Instructions
1	In the navigation tree, click **User Management** > **System Groups**.
2	Select the System Group.
3	Click **Edit**.
4	In the **Members of Group** list, select a user. 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	Instructions
1	In the navigation tree, click **User Management** > **System Groups**.
2	Select the System Group.
3	Click **Delete**.
4	Click **OK** to confirm.

Configuring System Groups in Gaia Clish

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

CLI Parameters

Parameter	Description
`group <Group Name>`	Unique name of System Group - between 1 and 16 alphanumeric characters without spaces

Parameter	Description
`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

In This Section:

Configuring GUI Clients in Gaia Portal 400
Configuring GUI Clients in Command Line 401

If this is a Security Management Server, you can configure which computers can connect to this Security Management Server with SmartConsole.

Note - This section does **not** show, if this is a Multi-Domain Server.

Configuring GUI Clients in Gaia Portal

Step	Instructions
1	In the navigation tree, click **User Management > GUI Clients**.
2	Click **Add**. 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 configured during the initial configuration. ■ **This machine - IP address** ■ **Network** ■ **Range of IPv4 addresses**

Configuring GUI Clients in Command Line

Step	Instructions
1	Connect to the command line on the Security Management Server.
2	Run: `cpconfig` For more information, see the *R80.40 CLI Reference Guide* > Chapter *Security Management Server Commands* > Section *cpconfig*.
3	Enter **3** for the **GUI Clients** option.
4	A list of hosts selected to be GUI clients shows. You can add or delete hosts, or create a new list. You can add new GUI clients in these formats: ■ **IP address** - One computer configured by its IPv4 or IPv6 address. ■ **Machine name** - One computer configured 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 addresses (for example, `192.168.10.0/255.255.255.0`) or IPv6 addresses (for example, `2001::1/128`). ■ **A range of addresses** - A limited range of IPv4 addresses (for example, `192.168.10.8-192.168.10.16`), or IPv6 addresses (for example, `2001::1-2001::10`). ■ **Wild cards (IPv4 only)** - A limited range of IPv4 addresses only (for example, `192.168.10.*`).

High Availability

In This Section:

Understanding VRRP 402
VRRP Terminology 403
VRRP on Gaia OS 404
VRRP Configuration Methods 405
Monitoring of VRRP Interfaces 406
How VRRP Failover Works 406
Typical VRRP Use Cases 408

Understanding VRRP

Virtual Routing Redundancy Protocol (VRRP) is a high-availability solution, where two Gaia Security Gateways can provide backup for each other. Gaia offers two ways to configure VRRP:

- **Monitored Circuit/Simplified VRRP** - All the VRRP interfaces automatically monitor other VRRP interfaces.
- **Advanced VRRP** - Every VRRP interface must be explicitly configured to monitor every other VRRP interface.

Important:

- You cannot have a Standalone deployment (Security Gateway and Security Management Server on the same computer) in a Gaia VRRP cluster.
- You cannot use both the Monitored Circuit/Simplified VRRP and Advanced VRRP together on the same Cluster Member.

Virtual Router Redundancy Protocol (VRRP) provides dynamic failover of IP addresses from one router to another in the event of failure. This increases the availability and reliability of routing paths through gateway selections on an IP network. Each VRRP router has a unique identifier known as the Virtual Router Identifier (VRID), which is associated with at least one Virtual IP Address (VIP). Neighboring network nodes connect to the VIP as a next hop in a route or as a final destination. Gaia supports VRRP as configured in RFC 3768.

VRRP Terminology

The conceptual information and procedures in this chapter use standard VRRP terminology.

This glossary contains basic VRRP terminology and a reference to related Check Point ClusterXL terms.

VRRP Term	ClusterXL Term	Definition
VRRP Cluster	Cluster	A group of Security Gateways that provides redundancy.
VRRP Router	Member	A Security Gateway using the VRRP protocol that is a member of one or more Virtual Router. In this guide, a VRRP Router is commonly called a Security Gateway.
Master	Active	The Security Gateway (Security Gateway) that handles traffic to and from a Virtual Router. The Master is the Security Gateway with the highest priority in a group. The Master inspects traffic and enforces the security policy.
Backup	Standby	A redundant Security Gateway (Security Gateway) that is available to take over for the Master in the event of a failure.
VRID	Cluster name	Unique Virtual Router identifier The VRID is the also last byte of the MAC address.
VIP	Cluster Virtual IP address	Virtual IP address assigned to a Virtual Router. VIPs are routable from internal and/or external network resources. The VIP is called **Backup Address** in the Gaia Portal.
VMAC	VMAC	Virtual MAC address assigned to a Virtual Router.
VRRP Transition	Failover	Automatic change over to a backup Security Gateway when the primary Security Gateway fails or is unavailable. The term 'failover' is used frequently in this guide.

VRRP on Gaia OS

On Gaia, VRRP can be used with ClusterXL enabled or with ClusterXL disabled.

VRRP with ClusterXL	Description
VRRP with ClusterXL *enabled*	This is the most common use case. You can deploy only an Active/Backup environments. VRRP supports a maximum of one VRID with one Virtual IP Address (VIP) for each interface. 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.
VRRP with ClusterXL *disabled*	You can deploy an Active/Active environment. You can configure two VRIDs on the same interface, with one VIP for each VRID. This configuration supports only static routes on the VRRP interfaces. You must disable the **VRRP monitoring of the Check Point Firewall** (see *"Preparing a VRRP Cluster" on page 411*).

VRRP Configuration Methods

VRRP Method	Description
Monitored Circuit/Simplified VRRP	To configure this simplified VRRP method, in the Gaia Portal go to **High Availability > VRRP**. This method contains all of the basic parameters, and is applicable for most environments. You configure each Virtual Router as one unit and configure the same VRID on all interfaces. Monitored Circuit VRRP automatically monitors all VRRP interfaces. This make a complete node failover possible. 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.
Advanced VRRP	To configure this advanced VRRP method, in the Gaia Portal go to **High Availability > Advanced VRRP**. This method allows configuration of different VRIDs on different interfaces. You configure a VRID on each interface individually. In addition, each VRRP-enabled interface must be monitored by each VRID together with an appropriate priority delta. This ensures that when one interface fails, all the other VRIDs can transition to VRRP Backup state ■ 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*, you can configure two VRIDs on each interface, with one VIP for each VRID.

Monitoring of VRRP Interfaces

The monitoring of all VRRP-enabled interfaces by all VRIDs is important to avoid connection issues with asymmetric routes.

For example, when an external interface fails, the VRRP Master fails over only for the external Virtual Router. The VRRP Master for the internal Virtual Router does not fail over. This can cause connectivity problems when the internal Virtual Router accepts traffic and is unable to connect to the new external VRRP Master.

Another tool for avoiding asymmetric issues during transitions is the VRRP *interface delay* setting. Configure this when the Preempt Mode of VRRP was turned off. This VRRP global setting is useful when the VRRP node with a higher priority is rebooted, but must not preempt the existing VRRP Master that handles the traffic, but is configured with a lower priority. Sometimes, interfaces that come up, take longer than the VRRP timeout to process incoming VRRP Hello packets. The interface delay extends the time that VRRP waits to receive VRRP Hello packets from the existing VRRP Master.

How VRRP Failover Works

Each Virtual Router (VRRP Group) is identified by a unique *Virtual Router ID* (VRID).

A Virtual Router contains one VRRP *Master* Security Gateway and at least one VRRP *Backup* Security Gateway.

The VRRP Master sends periodic VRRP advertisements (known as VRRP *Hello* messages) to the VRRP Backup Security Gateways.

VRRP advertisements broadcast the operational status of the VRRP Master to the VRRP Backup.

Gaia uses dynamic routing protocols to advertise the VIP of the Virtual Router (Virtual IP address or Backup IP address).

Notes:

- Gaia supports OSPF on VPN tunnels that terminate at a VRRP group.
- Active/Backup VRRP environments are supported with ClusterXL enabled. If ClusterXL is disabled, Active/Active environments can be deployed.
- Active/Active VRRP environments support only static routes. In addition, you must disable the monitoring of the Check Point Firewall by VRRP.

If the VRRP Master fails, or its VRRP-enabled interfaces fail, VRRP uses a priority algorithm to make the decision if failover to a VRRP Backup is necessary. Initially, the VRRP Master is the Security Gateway that has the highest configured priority value. You configure a priority for each Security Gateway when you create a Virtual Router or change its configuration. If two VRRP Security Gateways have same priority value, the platform that comes online and broadcasts its VRRP advertisements first becomes the VRRP Master.

Gaia also uses priorities to select a VRRP Backup Security Gateway upon failover (when there is more than one VRRP Backup available). In the event of failover, the Virtual Router priority value is decreased by a predefined *Priority Delta* value to calculate an *Effective Priority* value. The Virtual Router with the highest effective priority becomes the new VRRP Master. The *Priority Delta* value is a Check Point proprietary parameter that you configure when configuring a Virtual Router. If you configure your system correctly, the effective priority will be lower than the VRRP Backup Security Gateway priority in the other Virtual Routers. This causes the problematic VRRP Master to fail over for the other Virtual Routers as well.

Note - If the effective priority for the current VRRP Master and VRRP Backup are the same, the Security Gateway with the highest IP address becomes the VRRP Master.

Typical VRRP Use Cases

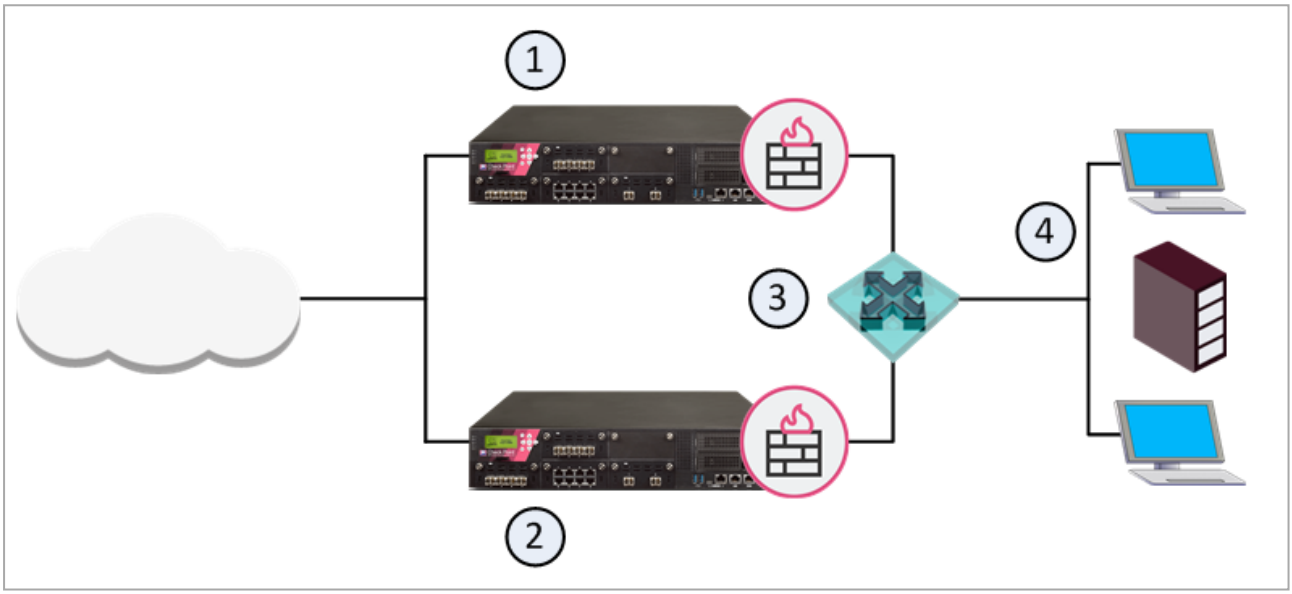
These are examples of some VRRP environments.

VRRP Use Case 1 - Internal Network High Availability

This is a simple VRRP use case, where Security Gateway 1 is the VRRP Master, and Security Gateway 2 is the VRRP Backup.

Virtual Router redundancy is available only for connections to and from the internal network.

There is no redundancy for external network traffic.



Item	Description
1	VRRP Master Security Gateway
2	VRRP Backup Security Gateway
3	Virtual Router VRID 5 - Virtual IP Address (Backup Address) is 192.168.2.5
4	Internal Network and hosts

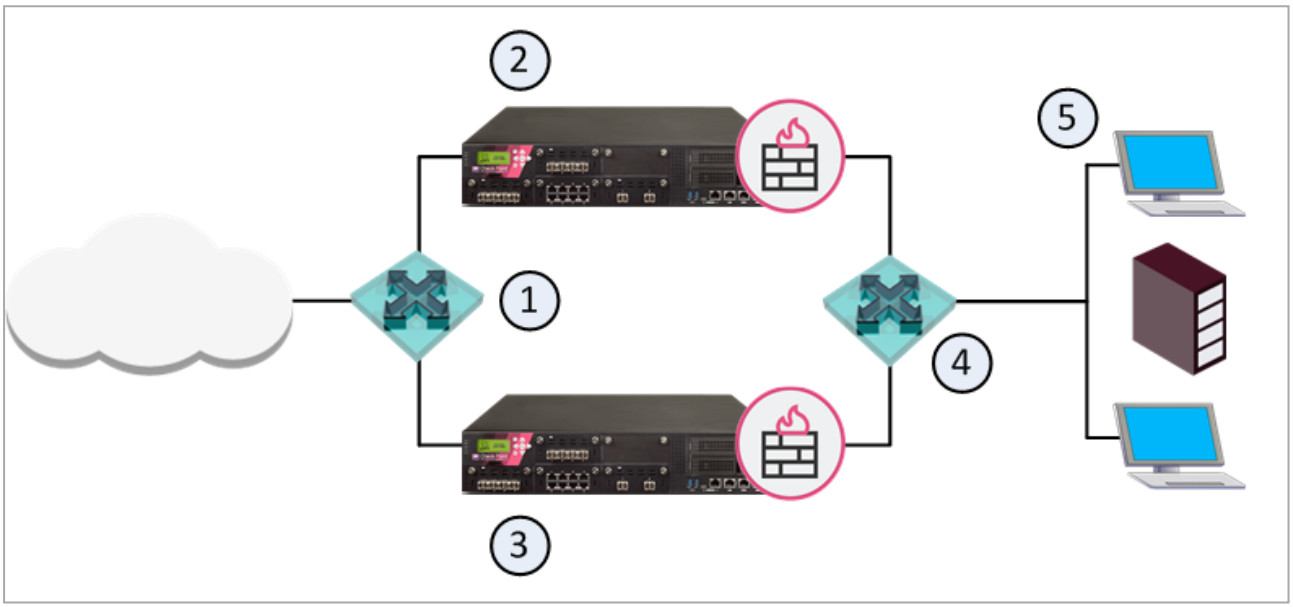
VRRP Use Case 2 - Internal and External Network High Availability

This use case shows an example of an environment, where there is redundancy for internal and external connections.

Here, you can use Virtual Routers for the two Security Gateways - for internal and for external connections.

The internal and external interfaces must be on different subnets.

Configure one Security Gateway as the VRRP Master and one Security Gateway as the VRRP Backup.



Item	Description
1	Virtual Router VRID 5 - External Virtual IP Address (Backup Address) is 192.168.2.5
2	VRRP Master Security Gateway
3	VRRP Backup Security Gateway
4	Virtual Router VRID 5 - Internal Virtual IP Address (Backup Address) is 192.168.3.5
5	Internal network and hosts

VRRP Use Case 3 - Internal Network Load Sharing

This use case shows an example of an Active/Active Load Sharing environment for internal network traffic.

This environment gives load balancing, as well as full redundancy.

This configuration is supported with ClusterXL disabled. Only Static Routes are supported.

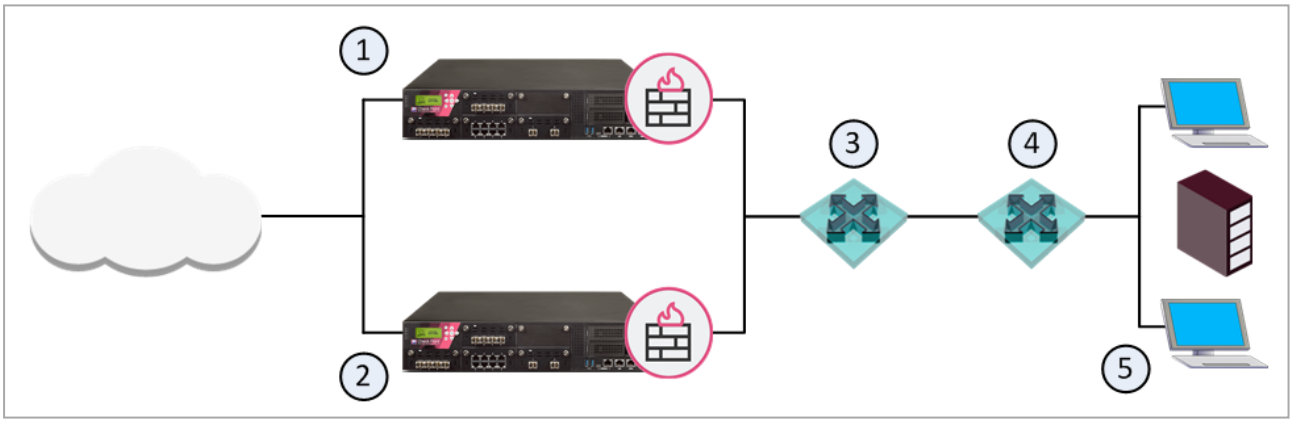
The monitoring of the Check Point Firewall by VRRP must be disabled (it is enabled by default).

A maximum of two VRIDs is supported per interface.

Security Gateway 1 is the VRRP Master for VRID 5, and Security Gateway 2 is the VRRP Backup.

Security Gateway 2 is the VRRP Master for VRID 7, and Security Gateway 1 is the VRRP Backup.

The two Security Gateways are configured to back each other up. If one fails, the other takes over its VRID and IP addresses.



Item	Description
1	VRRP Master Security Gateway for VRID 5 and VRRP Backup for VRID 7
2	VRRP Backup Security Gateway for VRID 5 and VRRP Master for VRID7
3	Virtual Router, VRID 5 Virtual IP Address (Backup Address) is 192.168.2.5
4	Virtual Router, VRID 7 Virtual IP Address (Backup Address) is 192.168.2.7
5	Internal network and hosts

Preparing a VRRP Cluster

In This Section:

Configuring Network Switches 411
Preparing VRRP Cluster Members 411
Configuring Global Settings for VRRP 412

Configuring Network Switches

Recommendations

Best Practice - If you use the Spanning Tree protocol on Cisco switches connected to Check Point VRRP clusters, we recommend that you enable PortFast. It sets interfaces to the Spanning Tree forwarding state, which prevents them from waiting for the standard forward-time interval.

If you use switches from a different vendor, we recommend that you use the equivalent feature for that vendor. If you use the Spanning Tree protocol without PortFast, or its equivalent, you may see delays during VRRP failover.

Preparing VRRP Cluster Members

Procedure

Step	Instructions
1	Install the VRRP Cluster Members See the *R80.40 Installation and Upgrade Guide* > Chapter *Installing a ClusterXL, VSX Cluster, VRRP Cluster* > Section *Installing a VRRP Cluster*..
2	Synchronize the system time on the VRRP Cluster Members. **Best Practice** - Enable NTP (Network Time Protocol) on all Security Gateways (see *"Time" on page 208*). 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.
3	**Optional:** Add host names and IP address pairs to the host table on each Security Gateway (see *"Hosts" on page 170*). This lets you use host names as an alternative to IP addresses or DNS servers.

Step	Instructions
4	Enable Virtual Routers: a. With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>` b. In the navigation tree, click **High Availability > VRRP**. c. Configure the VRRP Global Settings. See the section "**Configuring Global Settings for VRRP**" below. d. If the **Disable All Virtual Routers** option is currently selected, clear it. e. Click **Apply Global Settings**.
5	Configure your Virtual Routers in either Gaia Portal, or Gaia Clish. See: ■ *"Configuring Monitored Circuit/Simplified VRRP" on page 414* ■ *"Configuring Advanced VRRP" on page 423*

Configuring Global Settings for VRRP

This section shows you how to configure the global settings that apply to all Virtual Routers.

Procedure

Step	Instructions
1	In the navigation tree, click one of these: ■ **High Availability > VRRP**. ■ **High Availability >Advanced VRRP**.

Step	Instructions
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**.

Notes

Gaia starts to monitor the Firewall after the cold start delay completes.

This can cause some problems:

- If all the interfaces in a Virtual Router fail, all VRRP Cluster Members become VRRP Backups.

  None of the VRRP Cluster Members can become the VRRP Master and no traffic is allowed.

- If you change the time on any of the VRRP Cluster Members, a VRRP failover occurs automatically.

- In certain situations, installing a policy causes a failover.

  This can happen if it takes a long time to install the policy.

Configuring Monitored Circuit/Simplified VRRP

In This Section:

Configuring Monitored Circuit/Simplified VRRP in Gaia Portal 414
Configuring Monitored Circuit/Simplified VRRP in Gaia Clish 418
Configuring the VRRP Cluster for Simplified VRRP in SmartConsole 422

This section includes the procedure for configuring Monitored Circuit/Simplified VRRP.

Configuring Monitored Circuit/Simplified VRRP in Gaia Portal

Procedure

Step	Instructions
1	In the navigation tree, click **High Availability > VRRP**.
2	Configure the **VRRP Global Settings**. See *"Preparing a VRRP Cluster" on page 411*.
3	In the **Virtual Routers** section, click **Add**.

Step	Instructions
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 is 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.

Step	Instructions
	When this option is enabled, Priority Delta should be set equal to the Priority value, so that Priority becomes zero, if an interface goes down.
5	In the **Backup Addresses** section, click **Add**. 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 configured 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.

Step	Instructions
7	Click **Save**.

Configuring Monitored Circuit/Simplified VRRP in Gaia Clish

Syntax

To add Monitored Circuit/Simplified VRRP

1. Configure the priority:

```
add mcvr vrid VALUE priority VALUE priority-delta VALUE
[authtype {none | simple VALUE} hello-interval VALUE
```

2. Configure the backup address:

```
add mcvr vrid VALUE backup-address VALUE vmac-mode VALUE
```

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

CLI 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`
`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.

Parameter	Description
`vmac-mode {default-vmac | extended-vmac | interface-vmac | static-vmac` *VALUE*`}`	Configures how the Virtual MAC (VMAC) address is calculated for the given Virtual IP Address. 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 the Preempt Mode is *enabled*, if the Virtual Router has a higher Priority than the current VRRP Master, it preempts the VRRP Master. If the 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 the VRRP Cluster for Simplified VRRP in SmartConsole

Follow the *R80.40 Installation and Upgrade Guide* > Chapter *Installing a ClusterXL, VSX Cluster, VRRP Cluster* > Section *Installing a VRRP Cluster*.

Configuring Advanced VRRP

In This Section:

Changing from Advanced VRRP to Monitored Circuit/Simplified VRRP 423
Configuring Advanced VRRP in Gaia Portal 424
Configuring Advanced VRRP in Gaia Clish 428
Configuring the VRRP Cluster for Advanced VRRP in SmartConsole 434

Advanced VRRP lets you configure Virtual Routers at the interface level.

This section contains only those procedures that are directly related to Advanced VRRP configuration.

The general procedures for configuring VRRP clusters are described in *"Configuring Monitored Circuit/Simplified VRRP" on page 414*.

With Advanced VRRP, you must configure every Virtual Router to monitor every configured VRRP interface.

Changing from Advanced VRRP to Monitored Circuit/Simplified VRRP

Procedure

Step	Instructions
1	Delete all existing Virtual Routers.
2	Create new Virtual Routers in accordance with the procedures.

You cannot move a Backup Address from one interface to another while a Security Gateway is a VRRP Master.

Perform these steps to delete and add new interfaces with the necessary IP addresses:

Step	Instructions
1	Cause a failover from the VRRP Master to the VRRP Backup.
2	Reduce the priority, or disconnect an interface.
3	Delete the Virtual Router on the interface.
4	Create new Virtual Router using the new IP address.

Step	Instructions
5	Configure the Virtual Router as before.

Configuring Advanced VRRP in Gaia Portal

Procedure

Step	Instructions
1	In the navigation tree, click **High Availability >Advanced VRRP**.
2	Configure the VRRP Global Settings (see *"Preparing a VRRP Cluster" on page 411*).
3	In the **Virtual Routers** section, click **Add**.
4	In the **Add New Virtual Router** window, configure these parameters:
	■ **Interface** - Select the interface for the Virtual Router.
	■ **Virtual Router ID** - Enter or select the ID number of the Virtual Router.
	■ **Priority** - Enter or select the priority value. The priority value determines, which router takes over in the event of a failure. The router with the higher priority becomes the new VRRP Master. The range of values for priority is 1 to 254. The default value is 100.
	■ **Hello Interval** - Enter or select the number of seconds, at which the VRRP Master sends VRRP advertisements. 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).

Step	Instructions
	■ **Preempt Mode** - If you keep it selected (the default), when the original VRRP Master fails, a VRRP Backup system becomes the acting VRRP Master. When the original VRRP Master returns to service, it becomes VRRP Master again. If you clear it, when the original VRRP Master fails, a VRRP Backup system becomes the acting VRRP Master, and the original does not become VRRP Master again when it returns to service.
	■ **Auto-deactivation** - If you clear it (the default), a Virtual Router with the lowest priority available (1) can become VRRP Master, if no other Security Gateways exist on the network. If you selected it, the effective priority can become 0. With this priority, the Virtual Router does not become the VRRP Master, even if there are no other Security Gateways on the network. If you selected it, you should also configure the **Priority** and **Priority Delta** values to be equal, so that the effective priority becomes 0, if there is a VRRP failure.

Step	Instructions
	■ **VMAC Mode** - For each Virtual Router, a Virtual MAC (VMAC) address is assigned to the Virtual IP address. The VMAC address is included in all VRRP packets as the source MAC address. The physical MAC address is not used. 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 configured 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.
	■ **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.

Step	Instructions
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**.
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 in Gaia Clish

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

CLI 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`

Parameter	Description
`interface-delay <VALUE>`	The Interface Delay controls how long to wait (in seconds) after receiving an interface UP notification before VRRP assesses whether or not the related VRRP cluster member should increase its priority, and possibly become the new VRRP Master. The delay ensures that VRRP does not attempt to respond to interfaces, which are only momentarily active. Note - Same value should be configured for both VRRPv2 and VRRPv3 if both protocols are configured. ■ **Range:** 0 - 3600 ■ **Default:** 0
`interface VALUE`	The name of the interface, on which to enable the VRRP.
`authtype {none | simple VALUE}`	Configures authentication for the given Virtual Router. 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

Parameter	Description
`monitored-circuit vrid` *`VALUE`* `auto-deactivation {on | off}`	When an interface is reported as DOWN, a cluster member's Priority value is reduced by the configured Priority Delta amount. If another cluster member exists with a higher Priority, it will then take over as VRRP Master to heal the network. 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`
`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. If 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 the VRRP Cluster for Advanced VRRP in SmartConsole

Follow the *R80.40 Installation and Upgrade Guide* > Chapter *Installing a ClusterXL, VSX Cluster, VRRP Cluster* > Section *Installing a VRRP Cluster*.

Troubleshooting VRRP

In This Section:

Traces (Debug) for VRRP 435
General Configuration Considerations 437
Firewall Policies 437
Monitored-Circuit VRRP in Switched Environments 437

This section shows known issues with VRRP configurations and fixes.

Read this section before contacting *Check Point Support*.

Traces (Debug) for VRRP

You can log information about errors and events for troubleshooting VRRP.

To enable traces for VRRP

Step	Instructions
1	In the navigation tree, click **Routing** > **Routing Options**.
2	In the **Trace Options** section, in the **Filter Visible Tables Below** drop down list, select **VRRP**.
3	In the **VRRP** table, select the applicable options. 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.

Step	Instructions
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.

To disable traces for VRRP

Step	Instructions
1	In the navigation tree, click **Routing** > **Routing Options**.
2	In the **Trace Options** section, in the **Filter Visible Tables Below** drop down list, select **VRRP**. 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 all Security Gateways of the Virtual Router. You can also manually change the time and time zone on each Security Gateway to match the other Security Gateways. It must be no more than seconds apart.
- All routers of a Virtual Router must have the same VRRP Hello Interval.
- The Priority Delta must be sufficiently large for the Effective Priority to be lower than the VRRP Master router. Otherwise, when you pull an interface for a Monitored-Circuit VRRP test, other interfaces do not release IP addresses.
- Each unique Virtual Router ID must be configured with the same Backup Address on each Security Gateway.
- The VRRP monitor in the Gaia Portal might show one of the interfaces in *initialize* state. This might suggest that the IP address used as the Backup Address on that interface is invalid or reserved.
- An SNMP "Get" request on interfaces may list the incorrect IP addresses. This results in incorrect policy. An SNMP "Get" request fetches the lowest IP address for each interface. If interfaces are created when the Security Gateway is the VRRP Master, the incorrect IP address might be included. Repair this problem. Edit the interfaces by hand, if necessary.

Firewall Policies

Configure the Access Control Policy to accept VRRP packets to and from the Gaia platform. The multicast destination assigned by the IANA for VRRP is 224.0.0.18. If the Access Control Policy does not accept packets sent to 224.0.0.18, Security Gateways in one Virtual Router take on VRRP Master state.

Monitored-Circuit VRRP in Switched Environments

With Monitored-Circuit VRRP, some Ethernet switches might not recognize the VRRP MAC address after a change from VRRP Master to VRRP Backup. This is because many switches cache the MAC address related to the Ethernet device attached to a port. When failover to a VRRP Backup router occurs, the Virtual Router MAC address becomes associated with a different switch port. Switches that cache the MAC address might not change the associated cached MAC address to the new port during a VRRP change.

To repair this problem, you can take one of these actions

1. Replace the switch with a hub.
2. Disable MAC address caching on the switch, or switch ports, to which the VRRP cluster members are connected.

It might be not possible to disable the MAC address caching. If so, set the address aging value sufficiently low that the MAC addresses age out after a one second or two seconds. This causes more overhead on the switch. Therefore, find out if this is a viable option for your switch model.

The Spanning Tree Protocol (STP) prevents Layer 2 loops across multiple bridges. Spanning-Tree can be enabled on the ports connected to the two sides of a VRRP cluster. It can also "see" multicast VRRP Hello packets coming for the same MAC address on two different ports. When the two occur, it can suggest a loop, and the switch blocks traffic on one port. If a port is blocked, the VRRP cluster members cannot get VRRP Hello packets from each other. As a result, both VRRP cluster members enter the VRRP Master state.

If possible, turn off Spanning-Tree on the switch to resolve this issue. However, this can have harmful effects, if the switch is involved in a bridging loop. If you cannot disable Spanning-Tree, enable PortFast on the ports connected to the VRRP cluster members. PortFast causes a port to enter the Spanning-Tree forwarding state immediately, by passing the listening and learning states.

Maintenance

This chapter includes procedures and reference information for:

- Working with License
- Snapshot Management
- Download of SmartConsole
- Hardware Health Monitoring
- Monitoring RAID Synchronization
- Shut Down and Reboot
- System Backup

License Status

In This Section:

On Check Point Appliances 440

On Open Servers and Virtual Machines 440

Activating a License in Gaia Portal 441

You can view, add, or delete licenses in one of these ways:

- In Gaia Portal > **Maintenance** section > **License Status** page.
- With the "`cplic db_add`" and "`cplic del`" commands (see the *R80.40 CLI Reference Guide*).

  Note - While all the "`cplic`" commands are available in Gaia, they are not grouped into a Gaia feature.

On Check Point Appliances

If a Management Server and its managed Security Gateways are *able* to connect to Check Point User Center, licenses and contracts activated and updated automatically.

If a Management Server and its managed Security Gateways are **not** able to connect to Check Point User Center, then manage licenses and contracts in either SmartConsole or the command line.

On Open Servers and Virtual Machines

If a Management Server and its managed Security Gateways are *able* to connect to Check Point User Center, then activate the license during the Gaia First Time Configuration Wizard, or later in Gaia Portal, SmartConsole, or the command line. After the activation is completed, licenses and contracts are updated automatically.

If a Management Server and its managed Security Gateways are **not** able to connect to Check Point User Center, then manage licenses and contracts in either SmartConsole or the command line.

Activating a License in Gaia Portal

To activate a license manually online

Step	Instructions
1	If this Security Management Server, Domain Management Server, or Security Gateway (or Cluster Members) connects to the Internet through a proxy server, then configure the applicable proxy in SmartConsole: **Note** - The prerequisite for Security Gateways and Cluster Members is to establish a Secure Internal Communication (SIC Trust) with a Management Server. ■ To configure the same default proxy for all objects: a. Click **Menu** > **Global properties** > **Proxy**. b. Select **Use proxy server**. c. Enter the proxy server address (Hostname or IP address). d. Enter the proxy server port. e. Click **OK**. f. Publish the SmartConsole session. g. Click **Menu** > **Install database** > select all objects > click **Install**. h. Install the Access Control Policy on all managed Security Gateways and Clusters. ■ To configure specific proxy in an object: a. From the left navigation panel, click **Gateways & Servers**. b. Double-click the applicable object. c. From the left tree, click **Network Management** > **Proxy**. d. Select **Use custom proxy settings for this network object**. e. Select **Use proxy server**. f. Enter the proxy server address (Hostname or IP address). g. Enter the proxy server port. h. Click **OK**. i. Publish the SmartConsole session. j. Complete the configuration: • If this object is a Management Server: Click **Menu** > **Install database** > select the Management Server object > click **Install**. • If this object is a Security Gateway or Cluster: Install the Access Control Policy.
2	With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
3	In the navigation tree, click **Maintenance** > **License Status**.

Step	Instructions
4	Click **Activate Now**. Gaia fetches the license, and the status changes to **Activated**. The Software Blades enabled by the license appear in the table.

To activate a license manually offline

Step	Instructions
1	With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
2	In the navigation tree, click **Maintenance** > **License Status**.
3	Click **Offline Activation**.
4	Click **New**.
5	Enter the license data manually, or click **Paste License** to enter the data automatically. The **Paste License** button only appears in Internet Explorer. For other web browsers, paste the license strings into the empty text field.
6	Click **OK**.

To delete an installed license

Step	Instructions
1	With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
2	In the navigation tree, click **Maintenance** > **License Status**.
3	Click **Offline Activation**.
4	Select the license.
5	Click **Delete**.
6	Click **OK**.

Note - To delete a license in the command line, use the "`cplic del`" command (see the *R80.40 CLI Reference Guide*).

Snapshot Management

A snapshot is a backup of the system settings and products. It includes:

- File system, with customized files
- System configuration (interfaces, routing, hostname, and similar)
- Software Blades configuration
- Management database (on a Security Management Server or a Multi-Domain Server)

A snapshot is very large. A snapshot includes the entire root partition, part of the `/var/log` partition, and other important files.

For this reason, snapshots cannot be scheduled the same way that Backups can.

Backup and Restore is the preferred method of recovery.

Notes:

- When Gaia creates a snapshot, all system processes and services continue to run.
  Policy enforcement is not interrupted.
- You can import a snapshot created on a different software release or on this software release.
  You must import a snapshot on the appliance or open server of the same hardware model, from which it was exported.
- After importing the snapshot, you must activate the device license from the Gaia Portal or the User Center.
- We do not recommend to use snapshots as a way of regularly backing up your system.
  System Backup is the preferred method.
  Schedule system backups on a regular basis, daily or weekly, to preserve the Gaia OS configuration and Firewall database.

Important - See sk98068: Gaia Limitations after Snapshot Recovery.

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.

Snapshot Options

Option	Description
Revert	Reverts to a user created image. Reverts to a factory default image, which is automatically created on Check Point appliances by the installation or upgrade procedure.
Delete	Deletes an image from the local system.
Export	Exports 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.
Import	Imports an exported image.
View	Shows a list of images that are stored locally.

Notes:

- You must not rename the exported image. If you rename a snapshot image, it is not possible to revert to it.
- You can import a snapshot only on the machine of the same hardware type, from which it was exported.

Snapshot Prerequisites

- Before you **revert** to a snapshot on a new appliance, or after a reset to factory defaults, you must run the Gaia First Time Configuration Wizard and configure the same settings as before you created the snapshot.
- Before you **create** a new snapshot image, make sure the appliance or storage destination meets these prerequisites:
  - The required free disk space is the size of the system root partition multiplied by 1.15.

    Note - A snapshot image is created in unallocated space on the disk. Not all of the unallocated space on a disk can be used for snapshots. To find out if you have enough free space for snapshots:

Step	Instructions
1	Connect to the command line on the Gaia computer.
2	Log in to Gaia Clish.
3	Run: `show snapshots` The output shows the amount of space on the disk available for snapshots. 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.

Working with Snapshot Management in Gaia Portal

Before you create a snapshot image, make sure the appliance or storage destination meets the prerequisites.

Creating a new snapshot image

Step	Instructions
1	In the navigation tree, click **Maintenance > Snapshot Management**.
2	In the **Snapshot Management** section, click **New**. 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**.

Exporting an existing snapshot image

Step	Instructions
1	In the navigation tree, click **Maintenance > Snapshot Management**.
2	In the **Snapshot Management** section, select a snapshot.
3	Check the snapshot size.
4	Make sure that there is enough free disk space in the `/var/log/` partition: a. Connect to the command line on Gaia. b. Log in to the Expert mode. c. Run: `df -kh | egrep "Mounted|/var/log"` Check the value in the `Avail` column.
5	In Gaia Portal, select a snapshot.
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.

Importing a snapshot

To use the snapshot on another appliance, it has to be the same type of appliance you used to export the image.

Step	Instructions
1	In the navigation tree, click **Maintenance > Snapshot Management**.
2	In the **Snapshot Management** section, click **Import**. The **Import Image** window opens.
3	Click **Browse** to select the snapshot file for upload.
4	Click **Upload**.
5	Click **OK**.

Reverting to an existing snapshot image

Important:

- Reverting to the selected snapshot overwrites the existing running configuration and settings. Make sure you know credentials of the snapshot, to which you revert.
- Before you **revert** to a snapshot on a new appliance, or after a reset to factory defaults, you must run the Gaia First Time Configuration Wizard and configure the same settings as before you created the snapshot.

Step	Instructions
1	In the navigation tree, click **Maintenance > Image Management**.
2	In the **Snapshot Management** section, select a snapshot.
3	Click **Revert**. The **Revert** window opens. **Important** - Pay close attention to the warnings about overwriting settings, the credentials, and the reboot and the image details.
4	Click **OK**.
5	If you reverted a snapshot on a Security Gateway / Cluster Member, install the Security Policy.

Deleting a snapshot

Step	Instructions
1	In the navigation tree, click **Maintenance > Snapshot Management**.
2	In the **Snapshot Management** section, select a snapshot.
3	Click **Delete**. The **Delete Image** window opens.
4	Click **OK**.

Working with Snapshot Management in Gaia Clish

Before you create a snapshot image, make sure the appliance or storage destination meets the prerequisites.

Description

Manage system images (snapshots).

Syntax

Viewing information about existing snapshot images

```
show snapshots
```

```
show snapshot <Name of Snapshot>
      all
      date
      desc
      size
```

Creating a new snapshot image

```
add snapshot <Name of Snapshot> desc "<Description of Snapshot>"
```

Exporting an existing snapshot image

```
set snapshot export<SPACE><TAB>
```

```
set snapshot export <Name of Snapshot> path <Path> name <Name of Exported Snapshot>
```

Importing a snapshot image

```
set snapshot import <External Name of Snapshot> path <Path> name <Name of Imported Snapshot>
```

Reverting to an existing snapshot image

Important:

- Reverting to the selected snapshot overwrites the existing running configuration and settings. Make sure you know credentials of the snapshot, to which you revert.
- Before you **revert** to a snapshot on a new appliance, or after a reset to factory defaults, you must run the Gaia First Time Configuration Wizard and configure the same settings as before you created the snapshot.
- If you reverted a snapshot on a Security Gateway / Cluster Member, install the Security Policy.

```
set snapshot revert<SPACE><TAB>
```

```
set snapshot revert <Name of Snapshot>
```

Deleting a snapshot image

```
delete snapshot <Name of Snapshot>
```

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
```

Restoring a Factory Default Image on Check Point Appliance

Factory default images on Check Point appliances are created automatically when you install or upgrade an appliance to another release.

You can restore your Check Point appliance to the factory default image for a specified release.

Important - This procedure overwrites all existing configuration settings.

Best Practices:

>
- Create a snapshot image before you restore a factory default image.
- Export all existing snapshots from the appliance before you restore a factory default image.

Restoring a Factory Default image in Gaia Portal

Step	Instructions
1	In the navigation tree, click **Maintenance > Factory Defaults**.
2	Select the factory image.
3	Click **Apply**.

Restoring a Factory Default image in Gaia Clish

Step	Instructions
1	Connect to the command line on your appliance.
2	Log in to Gaia Clish.

3	Run:
	`set fcd revert<SPACE><TAB>`
	`set fcd revert <Name of Default Image>`

4	Follow the instructions on the screen.
5	Reboot: `reboot`

Download SmartConsole

You can download the SmartConsole application package from the Gaia Portal of your Security Management Server / Multi-Domain Server / Standalone Server.

Important - For the latest R80.40 SmartConsole package, refer to R80.40 SmartConsole Releases.

Step	Instructions
1	With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
2	There are two options to get the SmartConsole package. Option 1: a. In the navigation tree, click **Overview**. b. At the top of the page, click the **Download Now!** button. c. Save the package. Option 2: a. In the navigation tree, click **Maintenance** > **Download SmartConsole**. b. Click the **Download** button. c. Save the package.
3	Double-click the SmartConsole package and follow the installation wizard instructions.

For next steps in SmartConsole, refer to the *R80.40 Security Management Administration Guide*.

Hardware Health Monitoring

In This Section:

Showing Hardware Health Information in Gaia Portal *455*

Showing Hardware Health Information in Gaia Clish *456*

Showing Hardware Information *458*

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.

Showing Hardware Health Information in Gaia Portal

In the navigation tree, click **Maintenance** > **Hardware Health**.

Note - The **Hardware Health** page appears only on supported hardware.

You can see the status of the machine fans, system temperature, the voltages, and (for supported hardware only) the power supply.

For each component sensor, the table shows the value of its operation, and the status: **OK**, **Low**, or **High**.

- To see the health history of a component, select the component sensor. A graph shows the values over time.
- To change the time intervals that the graph shows, click the **Minute** arrows.
- To view different times, click the **Forward/Backward** arrows.
- To refresh, click **Refresh**.

Showing Hardware Health Information in Gaia Clish

Description

These commands display the status for various system hardware components.

Components, for which the status can be shown, include BIOS, cooling fans, power supplies, temperature, and voltages.

Note - The command returns information only for installed hardware components and only on supported hardware.

Syntax

```
show sysenv
      all
      bios
      fans
      ps
      temp
      volt
```

Parameters

Parameter	Description
`all`	Shows all system and hardware information.
`bios`	Shows BIOS information.
`fans`	Shows speed of cooling fans.
`ps`	Shows voltages and states of power supplies.
`temp`	Shows information from temperature sensors.
`volt`	Shows voltages information.

Example

```
gaia> show sysenv all

Hardware Information

Name   Value    unit      type     status  Maximum  Minimum
+12V   29.44    Volt      Voltage    0      12.6      11.4
+5V     6.02    Volt      Voltage    0      5.3       4.75
VBat    3.23    Volt      Voltage    0      3.47      2.7

gaia>
```

Showing Hardware Information

You can see information about the hardware, on which Gaia is installed using these commands:

Command	Description
`show asset<SPACE><TAB>`	You can run it in Gaia Clish only.
`cpstat os -f sensors`	You can run it in Gaia Clish, or Expert mode.

The "`show asset`" command

Description

Shows information about the hardware, on which Gaia is installed.

You can run this command in Gaia Clish only.

The information shown depends on the type of hardware.

Common types of information shown are:

- Serial number
- Amount of physical RAM
- CPU frequency
- Number of disks in the system
- Disk capacity

Syntax

```
show asset<SPACE><TAB>
show asset all
show asset <Category Name>
```

Parameters

Parameter	Description
`<SPACE><TAB>`	Press these keys to show a list of asset categories, such as `system` and `disk`. The available categories depend on the type of hardware.

Parameter	Description
`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 output

```
gaia> show asset system
Platform: Check Point 5800
Serial Number: XXX
CPU Model: Intel(R) Xeon(R) E3-1285Lv4
CPU Frequency: 3400
Disk Size: 500GB
Number of Cores: 8
CPU Hyperthreading: Enabled
gaia>
```

The "`cpstat os -f sensors`" command

Description

Shows information from supported hardware sensors.

You can run this command in Gaia Clish, or the Expert mode.

Syntax

```
cpstat os -f sensors
```

Example output

```
Temperature Sensors
------------------------------------------------
|Name        |Value|Unit     |Type       |Status|
------------------------------------------------
|CPU1 Temp   |49.50|degrees C|Temperature|     0|
|CPU0 Temp   |52.75|degrees C|Temperature|     0|
|Outlet Temp|27.50|degrees C|Temperature|     0|
|Intake Temp|28.75|degrees C|Temperature|     0|
------------------------------------------------

Fan Speed Sensors
-------------------------------------
|Name         |Value|Unit|Type|Status|
-------------------------------------
|System Fan 4|3349 |RPM |Fan |     0|
|System Fan 3|3375 |RPM |Fan |     0|
|System Fan 2|3383 |RPM |Fan |     0|
|System Fan 1|3333 |RPM |Fan |     0|
-------------------------------------

Voltage Sensors
----------------------------------------
|Name         |Value|Unit |Type  |Status|
----------------------------------------
|VBAT        |3.25 |Volts|Voltage|     0|
|5VSB        |5.04 |Volts|Voltage|     0|
|3VSB        |3.31 |Volts|Voltage|     0|
|VCC 5V      |5.03 |Volts|Voltage|     0|
|VCC 3V      |3.30 |Volts|Voltage|     0|
|VCC 12V     |12.07|Volts|Voltage|     0|
|CPU1 DDR4-2|1.19 |Volts|Voltage|     0|
|CPU1 DDR4-1|1.19 |Volts|Voltage|     0|
|CPU0 DDR4-2|1.19 |Volts|Voltage|     0|
|CPU0 DDR4-1|1.19 |Volts|Voltage|     0|
|CPU1 Vcore |1.81 |Volts|Voltage|     0|
|CPU0 Vcore |1.81 |Volts|Voltage|     0|
----------------------------------------
```

Hardware Diagnostics

Introduction

On Check Point appliances, you can run the built-in Hardware Diagnostics Tool that supports these tests:

- Spec Test
- Memory Test
- Network Test
- Disk Test
- Long Disk Test

Related Information

- *"Hardware Health Monitoring" on page 455*
- *"Monitoring RAID Synchronization" on page 463*
- sk171436 - HealthCheck Point (HCP) Release Updates

Requirement

To save the tool logs on a USB device, you must format it as FAT, FAT32, EXT2, or EXT3 file system. (NTFS or extFAT are not supported.)

Running the tool through the LCD (recommended)

1. In the LCD on your appliance, select the **HW Diagnostics** option.
2. Follow the instructions on the LCD.

Running the tool over the Console connection (recommended)

1. Connect a computer to the console port on your appliance.

   Configure the serial connection in your Terminal application.

   See the Getting Started Guide for your version.
2. Reboot your appliance.
3. In the Terminal application, press any key to get the Boot Menu.
4. In the **Boot Menu**, select the option **HW Diagnostics**.

5. Follow the instructions on the screen.
6. When you exit the **HW Diagnostics** tool, the appliance reboots.

Limitations

On 3100 and 3200 appliances: The Network Test using an external loopback device in interfaces eth1, eth2, eth3, and eth4 is not supported.

Monitoring RAID Synchronization

You can monitor the RAID status of the disks to see when the hard disks are synchronized.

If you reboot the appliance before the hard disks are synchronized, the synchronization starts again at the next boot.

Showing RAID Information in Gaia Portal

In the navigation tree, click **Maintenance** > **RAID Monitoring**.

You can see the information about **RAID Volumes** and **RAID Volume Disks**.

Showing RAID Information in Command Line

Run one of these commands in Gaia Clish or Expert mode:

- **The "`raid_diagnostic`" command**

  Description

  This command shows data about the RAID and hard disks, with the percent synchronization done.

  Syntax

  ```
  raid_diagnostic
  ```

  Example output from a Smart-1 225 appliance

  ```
  Raid Status:
  VolumeID:0 RaidLevel: RAID-1 NumberOfDisks:2 RaidSize:465GB State:DEGRADED Flags:
  ENABLED RESYNC _IN_PROGRESS
  DiskID:0 DiskNumber:0 Vendor:ATA     ProductID:<HDD Model> Size:465GB State:ONLINE
  Flags:NONE
  DiskID:1 DiskNumber:1 Vendor:ATA     ProductID:<HDD Model> Size:465GB
  State:INITIALIZING Flags:OUT_OF-SYNC SyncState: 12%
  ```

  - `DiskID 0` is the left hard disk.
  - `DiskID 1` is the right hard disk.

- **The "`cpstat os -f raidInfo`" command**

Description

This command shows almost the same information as the "`raid_diagnostic`" command, in tabular format.

Syntax

```
cpstat os -f raidInfo
```

Example output

```
Volume list
-------------------------------------------------------------------------------------
-----
|Volume id|Volume type|Number of disks|Max LBA  |Volume state|Volume flags|Volume size
(GB)|
-------------------------------------------------------------------------------------
-----
|        0|          2|              2|975175680|           0|           1|
465|
-------------------------------------------------------------------------------------
-----

Volume list
-------------------------------------------------------------------------------------
-----------------------------------------------------
|Volume id|Disk id|Disk number|Disk vendor|Disk product id|Disk revision|Disk max
LBA|Disk state|Disk flags|Disk sync state|Disk size (GB)|
-------------------------------------------------------------------------------------
-----------------------------------------------------
|        0|      0|          0|NONE       |NONE            |NONE         |            0|
       1|         0|              0|             0|
|        0|      1|          1|NONE       |NONE            |NONE         |            0|
       1|         0|              0|             0|
-------------------------------------------------------------------------------------
-----------------------------------------------------
```

Shut Down

There are two ways to shut down:

- **Reboot:** Shuts down the system and then immediately restarts it.
- **Halt:** Shuts down the system. You start the system manually with the power switch.

Rebooting and Shutting Down in Gaia Portal

To shut down the system and then immediately restart it

Step	Instructions
1	In the navigation tree, click **Maintenance** > **Shut Down**.
2	Click **Reboot**.

To shut down the system completely

Step	Instructions
1	In the navigation tree, click **Maintenance** > **Shut Down**.
2	Click **Halt**.

Rebooting and Shutting Down in Gaia Clish

To shut down the system and then immediately restart it

```
reboot
```

To shut down the system completely

```
halt
```

System Backup

- Back up the configuration of the Gaia operating system and of the Security Management Server database.

  You can restore a previously saved configuration.

  You can run the backup manually, or on a schedule.

  The configuration backup is saved in a `*.tgz` file in the `/var/log/CPbackup/backups/` directory (on Check Point Appliances and Open Servers.

  You can store backups locally, or remotely to a TFTP, SCP or FTP server.

- Save your Gaia system configuration settings as a ready-to-run CLI shell script.

  This lets you quickly restore your system configuration after a system failure or migration.

Note - You can only do a migration using the same Gaia version on the source and target computers.

Important - When you create a backup on a Security Management Server, make sure to close all SmartConsole clients. Otherwise, backup does not start.

Backing Up and Restoring the System

In This Section:

Excluding Files from the Gaia Backup *468*

Backing Up and Restoring the System in Gaia Portal *471*

Backing Up the System in Gaia Clish *474*

Restoring the System in Gaia Clish *476*

Important:

- You can restore a backup file on Gaia OS with the same software version, Jumbo Hotfix Accumulator, and hotfixes as installed on the source Gaia OS, on which you collected this backup file.
  Maestro Security Groups that contain different Security Appliance models do not support Gaia Backup operations (in the Global Gaia Portal or Global Gaia Clish).
- To collect or import a Gaia Backup in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.
- If you restored a backup on a Security Gateway / Cluster Member, install the Security Policy.

Note - Gaia Operating System uses these templates for the name of a manual backup output file:

Gaia Date Format	Template	Example for 20 November 2022, 18:04:43
dd/mm/yyyy	backup_ <HostName>.<Domain>_ <DD>_<MM>_<YYYY>_<HH>_ <MM>_<SS>.tgz	backup_ MyGW.MyDomain.com_ 20_11_2022_18_04_ 43.tgz
mm/dd/yyyy	backup_ <HostName>.<Domain>_ <MM>_<DD>_<YYYY>_<HH>_ <MM>_<SS>.tgz	backup_ MyGW.MyDomain.com_ 11_20_2022_18_04_ 43.tgz
yyyy/mm/dd	backup_ <HostName>.<Domain>_ <YYYY>_<MM>_<DD>_<HH>_ <MM>_<SS>.tgz	backup_ MyGW.MyDomain.com_ 2022_11_20_18_04_ 43.tgz
dd-mmm-yyyy	backup_ <HostName>.<Domain>_ <DD>_<MMM>_<YYYY>_<HH>_ <MM>_<SS>.tgz	backup_ MyGW.MyDomain.com_ 20_Nov_2022_18_04_ 43.tgz

Excluding Files from the Gaia Backup

Background

The Gaia Operating System contains backup configuration files (schema files) that control which files to collect during the backup for different software modules.

Filer	Software Blade / Feature	Security Gateway	Management Server, Log Server
/var/CPbackup/schemes/cvpn.cpbak	Mobile Access	✓	–
/var/CPbackup/schemes/dlp_gw.cpbak	Data Loss Prevention	✓	–
/var/CPbackup/schemes/dtps.cpbak	Desktop Policy Server and SecureClient	✓	–

Filer	Software Blade / Feature	Security Gateway	Management Server, Log Server
/var/CPbackup/schemes/fg1.cpbak	QoS	✓	–
/var/CPbackup/schemes/fw1.cpbak	Firewall	✓	–
/var/CPbackup/schemes/fw1logs.cpbak	Firewall Logs	✓	✓
/var/CPbackup/schemes/ioc.cpbak	External IoC Feeds	✓	✓
/var/CPbackup/schemes/mgmts.cpbak	Network Management	–	✓
/var/CPbackup/schemes/ppak.cpbak	SecureXL	✓	–
/var/CPbackup/schemes/rt.cpbak	SmartReporter	–	✓
/var/CPbackup/schemes/rtm.cpbak	Monitoring	✓	✓
/var/CPbackup/schemes/snapshot.cpbak	Snapshot Utility	✓	✓
/var/CPbackup/schemes/svn.cpbak	Common Infrastructure ($CPDIR)	✓	✓
/var/CPbackup/schemes/system_configuration.cpbak	Gaia Operating System	✓	✓
/var/CPbackup/schemes/te.cpbak	Threat Emulation	✓	–
/var/CPbackup/schemes/uepm.cpbak	Endpoint Policy Management	–	✓
/var/CPbackup/schemes/vsx.cpbak	VSX	✓	–
/var/CPbackup/schemes/vsx_mgmt.cpbak	VSX Policy	–	✓

Procedure

Step	Instruction
1	Connect to the command line on the Gaia server.
2	Log in to the Expert mode.
3	Back up the current configuration file: `cp -v /var/CPbackup/schemes/<Name-of-File>.cpbak{,_BKP}`
4	Edit the current configuration file: `vi /var/CPbackup/schemes/<Name-of-File>.cpbak`
5	Make the required changes in the applicable section: ■ The section <INCLUDE_FILES> controls which files to include during the backup. ■ The section <EXCLUDE_FILES> controls which files not to include during the backup.
6	Save the changes in the file and exit the editor.

Backing Up and Restoring the System in Gaia Portal

To create a backup

Step	Instructions
1	In the navigation tree, click **Maintenance** > **System Backup**. Refer to the **Backup** section.
2	Click **Backup**.
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.

Note - Gaia Portal does not support the change of backup file names. You can change a backup file name in the Expert mode. Make sure not to use special characters.

To restore from a locally saved backup

Step	Instructions
1	In the navigation tree, click **Maintenance** > **System Backup**. Refer to the **Backup** section.
2	Select the backup file.
3	Click **Restore**.

To restore from a remotely saved backup

Step	Instructions
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 an existing backup

Step	Instructions
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	Instructions
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	Instructions
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 the System in Gaia Clish

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 the 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>
```

Restoring the System in Gaia Clish

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`" feature (see *"Working with System Configuration in Gaia Clish" on page 483*).

Configuring Scheduled Backups

In This Section:

Configuring Scheduled Backups in Gaia Portal 478
Configuring Scheduled Backups in Gaia Clish 480

Important:

- When you create a backup on a Security Management Server, make sure to close all SmartConsole clients. Otherwise, scheduled backup does not start.
- You can configure only one schedule for one location. For example, you can configure only one schedule for an SCP server, and only one schedule for an FTP server.
- For regular backups, see *"Backing Up and Restoring the System" on page 467*.

Note - Gaia Operating System uses these templates for the name of a scheduled backup output file:

Gaia Date Format	Template	Example for 20 November 2022, 18:04:43
`dd/mm/yyyy`	`backup_ <HostName>.<Domain>_ <DD>_<MM>_<YYYY>_<HH>_ <MM>_<SS>.tgz`	`backup_ MyGW.MyDomain.com_ 20_11_2022_18_04_ 43.tgz`
`mm/dd/yyyy`	`backup_ <HostName>.<Domain>_ <MM>_<DD>_<YYYY>_<HH>_ <MM>_<SS>.tgz`	`backup_ MyGW.MyDomain.com_ 11_20_2022_18_04_ 43.tgz`
`yyyy/mm/dd`	`backup_ <HostName>.<Domain>_ <YYYY>_<MM>_<DD>_<HH>_ <MM>_<SS>.tgz`	`backup_ MyGW.MyDomain.com_ 2022_11_20_18_04_ 43.tgz`
`dd-mmm-yyyy`	`backup_ <HostName>.<Domain>_ <DD>_<MMM>_<YYYY>_<HH>_ <MM>_<SS>.tgz`	`backup_ MyGW.MyDomain.com_ 20_Nov_2022_18_04_ 43.tgz`

Configuring Scheduled Backups in Gaia Portal

To add a scheduled backup

Step	Instructions
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 the **Backup Schedule** section, configure the frequency (**Daily**, **Weekly**, **Monthly**) for this backup.
6	Click **Add**. The scheduled backup appears in the **Scheduled Backups** table.

To delete a scheduled backup

Step	Instructions
1	In the navigation tree, click **Maintenance** > **System Backup**. Refer to the **Scheduled Backup** section.
2	Select the backup to delete.
3	Click **Delete**.

Configuring Scheduled Backups in Gaia Clish

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

CLI 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.

Parameter	Description
`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 in Gaia Clish

You can save your Gaia configuration settings as a ready-to-run CLI shell script.

This feature lets you quickly restore your system configuration after a system failure or migration.

Note - You can only do a migration using the same Gaia version on the source and target computers.

Important - In a Management Data Plane Separation (MDPS) environment (see sk138672), you must run these commands in each plane. This applies to R80.40 Jumbo Hotfix Accumulator Take 114 and higher.

Syntax

To save the system configuration to a CLI script

```
save configuration <Name of Script>
```

To restore configuration settings

```
load configuration <Name of Script>
```

To see the latest configuration settings

```
show configuration
```

Example

This example shows part of the configuration settings as last saved to a CLI shell script:

```
mygaia> show configuration
#
# Configuration of mygaia
# Language version: 10.0v1
#
# Exported by admin on Mon Mar 19 15:06:22 2012
#
set hostname mygaia
set timezone Asia / Jerusalem
set password-controls min-password-length 6
set password-controls complexity 2
set password-controls palindrome-check true
set password-controls history-checking true
set password-controls history-length 10
set password-controls password-expiration never
set ntp active off
set router-id 6.6.6.103
set ipv6-state off
set snmp agent off
set snmp agent-version any
set snmp community public read-only
set snmp traps trap authorizationError disable
set snmp traps trap coldStart disable
set snmp traps trap configurationChange disable
... ... ...[truncated for brevity]... ... ...
mygaia>
```

Advanced Gaia Configuration

In This Section:

Configuring the Gaia Portal Web Server 485
Resetting the Expert Mode Password on a Security Gateway 487
Configuring Supported SSH Ciphers, MACs, and KexAlgorithms 487

Configuring the Gaia Portal Web Server

Description

You can 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`
`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 must 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.

Configuring Supported SSH Ciphers, MACs, and KexAlgorithms

Description

You can configure different settings for the SSH daemon on the Gaia Operating System.

You can configure these SSH settings in Gaia Clish.

Procedure for the R80.40 Jumbo Hotfix Accumulator, Take 83 and higher

1. Connect to the command line on the Management Server / Security Gateway.
2. Log in to the Expert mode.
3. Back up the current configuration file:

   ```
   cp -v /etc/ssh/templates/sshd_config.templ{,BKP}
   ```

4. Edit the current configuration file:

   ```
   vi /etc/ssh/templates/sshd_config.templ
   ```

5. Configure the applicable SSH Ciphers, edit the line that starts with the word **Ciphers**:

   ```
   Ciphers VALUE1,VALUE2,...,VALUEx
   ```

   Notes:
   - If this line does not exist, add it.
   - By default, Gaia OS uses the first configured Cipher.
   - Values must be separated by commas without spaces.

6. Configure the applicable SSH Message Authentication Codes (MACs), edit the line that starts with the word **Macs**:

   ```
   Macs VALUE1,VALUE2,...,VALUEx
   ```

Notes:
- If this line does not exist, add it.
- By default, Gaia OS uses the first configured MAC.
- Values must be separated by commas without spaces.

7. Configure the applicable SSH Key Exchange Algorithms, edit the line that starts with the word **KexAlgorithms**:

```
KexAlgorithms VALUE1,VALUE2,...,VALUEx
```

Notes:
- If this line does not exist, add it.
- By default, Gaia OS uses the first configured KexAlgorithm.
- Values must be separated by commas without spaces.

8. Save the changes in the file and exit the editor.
9. Import the updated configuration into the Gaia OS database:

```
/bin/sshd_template_xlate < /config/active
```

10. Restart the SSH server:

```
service sshd restart
```

Procedure for R80.40 and the R80.40 Jumbo Hotfix Accumulator, Take lower than 83

1. Connect to the command line on the Gaia OS server.
2. Log in to the Expert mode.
3. Back up each of these configuration files:

```
cp -v /etc/ssh/ssh_config{,BKP}
```

```
cp -v /etc/ssh/sshd_config{,BKP}
```

4. Edit each of these configuration files:

```
vi /etc/ssh/ssh_config
```

```
vi /etc/ssh/sshd_config
```

5. Configure the applicable SSH Ciphers, edit the line that starts with the word **Ciphers**:

```
Ciphers VALUE1,VALUE2,...,VALUEx
```

Notes:
- If this line does not exist, add it.
- By default, Gaia OS uses the first configured Cipher.
- Values must be separated by commas without spaces.

6. Configure the applicable SSH Message Authentication Codes (MACs), edit the line that starts with the word **Macs:**

```
Macs VALUE1,VALUE2,...,VALUEx
```

Notes:
- If this line does not exist, add it.
- By default, Gaia OS uses the first configured MAC.
- Values must be separated by commas without spaces.

7. Configure the applicable SSH Key Exchange Algorithms, edit the line that starts with the word **KexAlgorithms**:

```
KexAlgorithms VALUE1,VALUE2,...,VALUEx
```

Notes:
- If this line does not exist, add it.
- By default, Gaia OS uses the first configured KexAlgorithm.
- Values must be separated by commas without spaces.

8. Save the changes in the file and exit the editor.
9. Restart the SSH server:

```
service sshd restart
```

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 configure a CPUSE policy before you download and run upgrades.

For details, see sk92449.

Running Check Point Commands in Shell Scripts

To run Check Point commands in your shell scripts, it is necessary to add the calls to the required Check Point shell scripts.

You must add these calls below the top line "`#!/bin/bash`".

On a Security Management Server / Log Server / SmartEvent Server

You must add the call to the `/etc/profile.d/CP.sh` script.

```
#!/bin/bash

source /etc/profile.d/CP.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

On a Multi-Domain Server / Multi-Domain Log Server

You must add the calls to these scripts (in the order listed below):

1. `/etc/profile.d/CP.sh`
2. `$MDSDIR/scripts/MDSprofile.sh`
3. `$MDS_SYSTEM/shared/mds_environment_utils.sh`
4. `$MDS_SYSTEM/shared/sh_utilities.sh`

```
#!/bin/bash

source /etc/profile.d/CP.sh
source $MDSDIR/scripts/MDSprofile.sh
source $MDS_SYSTEM/shared/mds_environment_utils.sh
source $MDS_SYSTEM/shared/sh_utilities.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

On a Security Gateway / Cluster Members (non-VSX)

You must add the call to the `/etc/profile.d/CP.sh` script.

```
#!/bin/bash

source /etc/profile.d/CP.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

On a VSX Gateway / VSX Cluster Members

You must add the calls to these scripts (in the order listed below):

1. `/etc/profile.d/CP.sh`
2. `/etc/profile.d/vsenv.sh`

```
#!/bin/bash

source /etc/profile.d/CP.sh
source /etc/profile.d/vsenv.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

Glossary

A

Anti-Bot
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

Audit Log
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

B

Bridge Mode
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
Security Gateway that is part of a cluster.

Compliance
Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness
Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

CoreXL
Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

D

DAIP Gateway
Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Loss Prevention
Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type
Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Distributed Deployment
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

Dynamic Object
Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Endpoint Policy Management
Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

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

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia Portal
Web interface for the Check Point Gaia operating system.

H

Hotfix
Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection
Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Identity Awareness
Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Logging
Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPS
Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN
Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

L

Log Server
Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Management Interface
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

Management Server
Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

Manual NAT Rules
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Mobile Access
Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server
Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Server
Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

N

Network Object
Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Policy Management
Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

O

Open Server
Physical computer manufactured and distributed by a company, other than Check Point.

P

Provisioning
Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Q

QoS
Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

R

Rule
Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base
All rules configured in a given Security Policy. Synonym: Rulebase.

S

SecureXL
Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Management Server
Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

Security Policy
Collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

SmartConsole
Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard
Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartProvisioning
Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate
Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

Software Blade
Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

Standalone
Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

T

Threat Emulation
Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Extraction
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Directory
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

V

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Z

Zero Phishing
Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.

Appendix

This section contains various notes about the Gaia Operating System.

- The default value of the Linux kernel parameter */proc/sys/net/ipv6/conf/all/accept_dad* is set to '0'. The IPv6 Duplicate Address Detection (DAD) feature continues to be enabled by default ('*set neighbor duplicate-detection state on*').