



QUANTUM

30 April 2024

GAIA

R81.20

Administration Guide



Check Point Copyright Notice

© 2022 - 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 R81.20

For more about this release, see the R81.20 [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
30 April 2024	Updated: <ul style="list-style-type: none"> ▪ "Introduction to the Gaia Portal" on page 20
17 April 2024	Updated: <ul style="list-style-type: none"> ▪ "Configuring Cloning Groups in Gaia Portal" on page 299
13 March 2024	Updated: <ul style="list-style-type: none"> ▪ "Configuring SNMP in Gaia Clish" on page 330 ▪ "Configuring SNMP in Gaia Portal" on page 319
23 December 2023	Updated: <ul style="list-style-type: none"> ▪ "Running the First Time Configuration Wizard in Gaia Portal" on page 59
17 August 2023	Added a new section: <ul style="list-style-type: none"> ▪ "Hardware Diagnostics" on page 590
16 August 2023	Updated: <ul style="list-style-type: none"> ▪ "Expert Mode" on page 53 Added a new section: <ul style="list-style-type: none"> ▪ "Appendix" on page 664
11 July 2023	Added a new topic: <ul style="list-style-type: none"> ▪ "Configuring SSH Authentication with RSA Key Files" on page 470 Updated: <ul style="list-style-type: none"> ▪ "GRE Interfaces" on page 202
05 July 2023	Added a new topic: <ul style="list-style-type: none"> ▪ "Getting Started" on page 34
21 June 2023	Updated: <ul style="list-style-type: none"> ▪ "Authentication Servers" on page 474

Date	Description
07 May 2023	Updated: <ul style="list-style-type: none"> ▪ "Configuring SNMP in Gaia Clish" on page 330 ▪ "Configuring SNMP in Gaia Portal" on page 319
16 April 2023	Updated: <ul style="list-style-type: none"> ▪ "Configuring System Logging in Gaia Clish" on page 378 ▪ "Configuring System Logging in Gaia Portal" on page 374
03 April 2023	Updated: <ul style="list-style-type: none"> ▪ "Restoring a Factory Default Image on Check Point Appliance" on page 582
27 March 2023	Updated: <ul style="list-style-type: none"> ▪ "Configuring Cloning Groups in Gaia Portal" on page 299
23 February 2023	Updated: <ul style="list-style-type: none"> ▪ "GRE Interfaces" on page 202
30 January 2023	Updated: <ul style="list-style-type: none"> ▪ "Backing Up and Restoring the System" on page 597 ▪ "System Backup" on page 596 ▪ "Proxy" on page 286
24 January 2023	Updated: <ul style="list-style-type: none"> ▪ "System Management" on page 276
17 January 2023	Updated: <ul style="list-style-type: none"> ▪ "Backing Up and Restoring the System" on page 597 ▪ "Configuring Scheduled Backups" on page 606
12 January 2023	Updated: <ul style="list-style-type: none"> ▪ "Snapshot Management in Gaia Portal" on page 549 ▪ "Snapshot Management in Gaia Clish - Regular Snapshots" on page 555 ▪ "System Backup" on page 596 ▪ "Backing Up and Restoring the System" on page 597

Date	Description
11 January 2023	Updated: <ul style="list-style-type: none">▪ "Configuring SNMP in Gaia Portal" on page 319▪ "Configuring SNMP in Gaia Clish" on page 330
08 January 2023	Updated: <ul style="list-style-type: none">▪ "Configuring SNMP in Gaia Portal" on page 319▪ "Configuring SNMP in Gaia Clish" on page 330▪ "Configuring Gaia as a TACACS+ Client" on page 491▪ "Snapshot Management" on page 545 - Maestro Security Groups that contain different Security Appliance models do not support Gaia Snapshot operations▪ "System Backup" on page 596 - Maestro Security Groups that contain different Security Appliance models do not support Gaia Backup operations▪ "Advanced Gaia Configuration" on page 625 - added "Configuring Supported SSH Ciphers, MACs, and KexAlgorithms" on page 627
20 November 2022	First release of this document

Table of Contents

Gaia Overview	19
Introduction to the Gaia Portal	20
Gaia Portal Overview	20
Working with the Configuration Lock	26
Using the Gaia Portal Interface Elements	27
Toolbar Accessories	27
Search Tool	27
Navigation Tree	27
Status Bar	28
Configuration Tab	28
Monitoring Tab	28
Unsupported Characters and Words	29
System Information Overview	30
Showing System Overview Information in Gaia Portal	30
Showing System Overview Information in Gaia Clish	32
Getting Started	34
Introduction to the Command Line Interface	35
Syntax Legend	37
Command Completion	39
Commands and Features	41
Command History	43
Command Line Movement and Editing	45
Configuration Locks	46
Environment Commands	48
Client Environment Output Format	51
Expert Mode	53
User Defined (Extended) Commands	54

Summary of Gaia Clish Commands	56
Configuring Gaia for the First Time	58
Running the First Time Configuration Wizard in Gaia Portal	59
Running the First Time Configuration Wizard in CLI Expert mode	77
Centrally Managing Gaia Device Settings	90
Introduction of Gaia Central Management	90
Managing Gaia in SmartConsole	92
Running Command Scripts	92
Understanding One-Time Scripts	95
Running Repository Scripts	95
Backup and Restore	96
Backing up the System	97
Restoring the System	98
Opening Gaia Portal and Gaia Clish	99
Network Management	100
Network Interfaces	101
Physical Interfaces	102
Configuring Physical Interfaces in Gaia Portal	103
Configuring Physical Interfaces in Gaia Clish	105
Aliases	109
Configuring Aliases in Gaia Portal	109
Configuring Aliases in Gaia Clish	111
Configuring Aliases on Scalable Platforms	113
VLAN Interfaces	117
Configuring VLAN Interfaces in Gaia Portal	117
Configuring VLAN Interfaces in Gaia Clish	120
Access Mode VLAN and Trunk Mode VLAN	123
VXLAN Interfaces	125
Configuring VXLAN Interfaces in Gaia Portal	126
Configuring VXLAN Interfaces in Gaia Clish	128

Configuring VXLAN Interfaces on Cluster Members	130
Bond Interfaces (Link Aggregation)	132
Configuring Bond Interfaces in Gaia Portal	135
Configuring Bond Interfaces in Gaia Clish	138
Making Sure that Bond Interface is Working	149
Configuring Bond High Availability in VRRP Cluster	152
MAGG Interfaces	154
Configuring MAGG Interfaces in Gaia Portal	154
Configuring MAGG Interfaces in Gaia Clish	157
Bridge Interfaces	165
Configuring Bridge Interfaces in Gaia Portal	166
Configuring Bridge Interfaces in Gaia Clish	168
Accept, or Drop Ethernet Frames with Specific Protocols	175
Loopback Interfaces	177
Configuring Loopback Interfaces in Gaia Portal	177
Configuring Loopback Interfaces in Gaia Clish	180
VPN Tunnel Interfaces	182
6in4 Tunnel Interfaces	191
Configuring 6in4 Tunnel Interfaces in Gaia Portal	192
Configuring 6in4 Tunnel Interfaces in Gaia Clish	194
PPPoE Interfaces	196
Configuring PPPoE Interfaces in Gaia Portal	197
Configuring PPPoE Interfaces in Gaia Clish	199
GRE Interfaces	202
Configuring GRE Interfaces in Gaia Portal	203
Configuring GRE interfaces in Gaia Clish	205
Configuring GRE Interfaces on Cluster Members	208
Gaia Management Interface	210
Selecting Management Interface in Gaia Portal	210
Selecting Management Interface in Gaia Clish	211

Detection of IP Address Conflicts	212
Configuration in Gaia Clish	212
Log Messages	215
Additional Information	216
Interface Link Status	217
CLI Reference (interface)	218
ARP	219
Configuring ARP in Gaia Portal	220
Configuring ARP in Gaia Clish	222
DHCP Server	224
Configuring a DHCP Server in Gaia Portal	225
Configuring a DHCP Server in Gaia Clish	228
Hosts and DNS	234
System Name	235
Configuring Host Name and Domain Name in Gaia Portal	235
Configuring Host Name and Domain Name in Gaia Clish	235
Hosts	237
Configuring Hosts in Gaia Portal	237
Configuring Hosts in Gaia Clish	239
DNS	241
Configuring DNS in Gaia Portal	241
Configuring DNS in Gaia Clish	243
IPv4 Static Routes	245
Configuring IPv4 Static Routes in Gaia Portal	246
Configuring IPv4 Static Routes in Gaia Clish	251
IPv6 Static Routes	256
Configuring IPv6 Static Routes in Gaia Portal	256
Configuring IPv6 Static Routes in Gaia Clish	258
Troubleshooting	262
Configuring IPv6 Neighbor Entries	263

NetFlow Export	265
Introduction	265
Configuration Procedure	267
Available Commands in Gaia Clish	272
System Management	276
System Passwords	277
Configuring System Passwords in Gaia Portal	278
Configuring the Expert mode password	278
Configuring the GRUB password	279
Configuring System Passwords in Gaia Clish	280
Configuring the Expert mode password	280
Configuring the GRUB password	283
Proxy	286
Proxy for Gaia Operating System	286
Proxy for Check Point Servers	286
Security Gateway as an HTTP/HTTPS Proxy	286
Configuring Proxy in Gaia Portal	287
Configuring Proxy in Gaia Clish	289
Time	290
Configuring the Time and Date in Gaia Portal	291
Configuring the Time and Date in Gaia Clish	293
Cloning Group	298
Configuring Cloning Groups in Gaia Portal	299
Configuring Cloning Groups in Gaia Clish	306
Cloning Group Modes	306
CLI Syntax	307
SNMP	314
Introduction	314
SNMP v3 - User-Based Security Model (USM)	316
Enabling SNMP	316

SNMP Agent Address	316
SNMP Traps	317
Configuring SNMP in Gaia Portal	319
Configuring SNMP in Gaia Clish	330
Interpreting SNMP Error Messages	340
SNMP PDU	340
GetRequest	342
GetNextRequest	342
GetBulkRequest	343
Job Scheduler	344
Configuring Job Scheduler in Gaia Portal	345
Configuring Job Scheduler in Gaia Clish	348
Mail Notification	353
Introduction	353
Configuring Mail Notification in Gaia Portal	354
Configuring Mail Notification in Gaia Clish	355
Messages	357
Comparison	357
Configuring Messages in Gaia Portal	357
Configuring Messages in Gaia Clish	358
Limits	361
Display Format	362
Configuring Display Format in Gaia Portal	362
Configuring Display Format in Gaia Clish	363
Session	364
Configuring the Session in Gaia Portal	364
Configuring the Session in Gaia Clish	364
Crash Data	366
Introduction	366
Configuring Core Dumps in Gaia Portal	366

Configuring Core Dumps in Gaia Clish	368
System Configuration	370
Configuring IPv6 Support in Gaia Portal	371
Configuring IPv6 Support in Gaia Clish	371
System Logging	373
Configuring System Logging in Gaia Portal	374
Configuring System Logging in Gaia Clish	378
Redirecting Routed System Logging Messages	384
Configuring Log Volume	388
Network Access	389
Introduction	389
Configuring Telnet Access in Gaia Portal	389
Configuring Telnet Access in Gaia Clish	389
Host Access	390
Configuring Allowed Gaia Clients in Gaia Portal	390
Configuring Allowed Gaia Clients in Gaia Clish	391
LLDP	393
Configuring LLDP in Gaia Portal	393
Configuring LLDP in Gaia Clish	396
Viewing the LLDP neighbors in the Expert mode	400
Advanced Routing	401
User Management	402
Change My Password	403
Changing My Password in Gaia Portal	403
Changing My Password in Gaia Clish	403
Users	404
Managing User Accounts in Gaia Portal	406
Managing User Accounts in Gaia Clish	410
Roles	415
Configuring Roles in Gaia Portal	416

Configuring Roles in Gaia Clish	420
List of Available Features in Roles	425
List of Available Extended Commands in Roles	446
Password Policy	450
Configuring Password Policy in Gaia Portal	453
Procedure	453
Password Strength	454
Password History	455
Mandatory Password Change	456
Denying Access to Unused Accounts	457
Denying Access After Failed Login Attempts	458
Password Hashing Algorithm	459
Configuring Password Policy in Gaia Clish	460
Password Strength	460
Password History	462
Mandatory Password Change	463
Denying Access to Unused Accounts	465
Denying Access After Failed Login Attempts	466
Configuring Hashing Algorithm	468
Monitoring Password Policy in Gaia Clish	469
Configuring SSH Authentication with RSA Key Files	470
Prerequisites	470
Procedure	470
Authentication Servers	474
Configuring RADIUS Servers	476
Configuring RADIUS Servers in Gaia Portal	476
Configuring RADIUS Servers in Gaia Clish	478
Configuring Gaia as a RADIUS Client	481
Configuring RADIUS Servers for Non-Local Gaia Users	482
Configuring TACACS+ Servers	485

Configuring TACACS+ Servers in Gaia Portal	485
Configuring TACACS+ Servers in Gaia Clish	488
Checking if the Logged In User is Enabled for TACACS+	490
Configuring Gaia as a TACACS+ Client	491
Configuring TACACS+ Servers for Non-Local Gaia Users	494
System Groups	495
Introduction	495
Configuring System Groups in Gaia Portal	496
Configuring System Groups in Gaia Clish	498
GUI Clients	500
Configuring GUI Clients in Gaia Portal	500
Configuring GUI Clients in Command Line	501
High Availability	502
Understanding VRRP	502
VRRP Terminology	503
VRRP on Gaia OS	504
VRRP Configuration Methods	505
Monitoring of VRRP Interfaces	506
How VRRP Failover Works	506
Typical VRRP Use Cases	508
Preparing a VRRP Cluster	511
Configuring Network Switches	511
Preparing VRRP Cluster Members	511
Configuring Global Settings for VRRP	512
Configuring Monitored Circuit/Simplified VRRP	514
Configuring Monitored Circuit/Simplified VRRP in Gaia Portal	514
Configuring Monitored Circuit/Simplified VRRP in Gaia Clish	518
Configuring the VRRP Cluster for Simplified VRRP in SmartConsole	522
Configuring Advanced VRRP	523
Changing from Advanced VRRP to Monitored Circuit/Simplified VRRP	523

Configuring Advanced VRRP in Gaia Portal	524
Configuring Advanced VRRP in Gaia Clish	528
Configuring the VRRP Cluster for Advanced VRRP in SmartConsole	534
Troubleshooting VRRP	535
Traces (Debug) for VRRP	535
General Configuration Considerations	537
Firewall Policies	537
Monitored-Circuit VRRP in Switched Environments	537
Maintenance	539
License Status	540
On Check Point Appliances	540
On Check Point Maestro	540
On Open Servers and Virtual Machines	541
Activating a License in Gaia Portal	542
Snapshot Management	545
Snapshot Options	547
Snapshot Prerequisites	548
Snapshot Management in Gaia Portal	549
Snapshot Management in Gaia Clish - Regular Snapshots	555
Snapshot Management in Gaia Clish - Scheduled Snapshots	562
Working with Snapshot Management in the Expert mode (g_snapshot)	578
SMO Image Cloning	580
Restoring a Factory Default Image on Check Point Appliance	582
Download SmartConsole	583
Hardware Health Monitoring	584
Showing Hardware Health Information in Gaia Portal	584
Showing Hardware Health Information in Gaia Clish	585
Showing Hardware Information	587
Hardware Diagnostics	590
Introduction	590

Requirement	590
Running the tool through the LCD (recommended)	590
Running the tool over the Console connection (recommended)	590
Running the tool in the Expert mode (optional)	591
Limitations	591
Monitoring RAID Synchronization	592
Showing RAID Information in Gaia Portal	592
Showing RAID Information in Command Line	592
Shut Down	594
Rebooting and Shutting Down in Gaia Portal	594
Rebooting and Shutting Down in Gaia Clish	595
System Backup	596
Backing Up and Restoring the System	597
Excluding Files from the Gaia Backup	597
Backing Up and Restoring the System in Gaia Portal	600
Backing Up the System in Gaia Clish	603
Restoring the System in Gaia Clish	605
Configuring Scheduled Backups	606
Configuring Scheduled Backups in Gaia Portal	606
Configuring Scheduled Backups in Gaia Clish	609
Troubleshooting	621
Working with System Configuration in Gaia Clish	622
LVM Overview	624
Advanced Gaia Configuration	625
Configuring the Gaia Portal Web Server	625
Resetting the Expert Mode Password on a Security Gateway	627
Configuring Supported SSH Ciphers, MACs, and KexAlgorithms	627
Monitoring Transceivers	634
Background	634
Viewing Information About an Interface Transceiver	634

Viewing Detailed Information About an Interface Transceiver	635
Viewing Information About Transceivers for All Interfaces	637
Viewing Detailed Information About Transceivers for All Interfaces	638
CPUSE - Software Updates	643
Gaia API Proxy	644
Running Check Point Commands in Shell Scripts	651
On a Security Management Server / Log Server / SmartEvent Server	651
On a Multi-Domain Server / Multi-Domain Log Server	652
On a Security Gateway / Cluster Members (non-VSX)	652
On a VSX Gateway / VSX Cluster Members	653
Glossary	654
Appendix	664

Gaia Overview

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

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

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

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

Gaia CPUSE:

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

Gaia API:

See [sk143612](#) and [Check Point Gaia API Reference](#).

Introduction to the Gaia Portal

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

Gaia Portal Overview

- The Gaia Portal is an advanced, web-based interface for Gaia platform configuration. You can do almost all system configuration tasks through this Web-based interface.

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

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



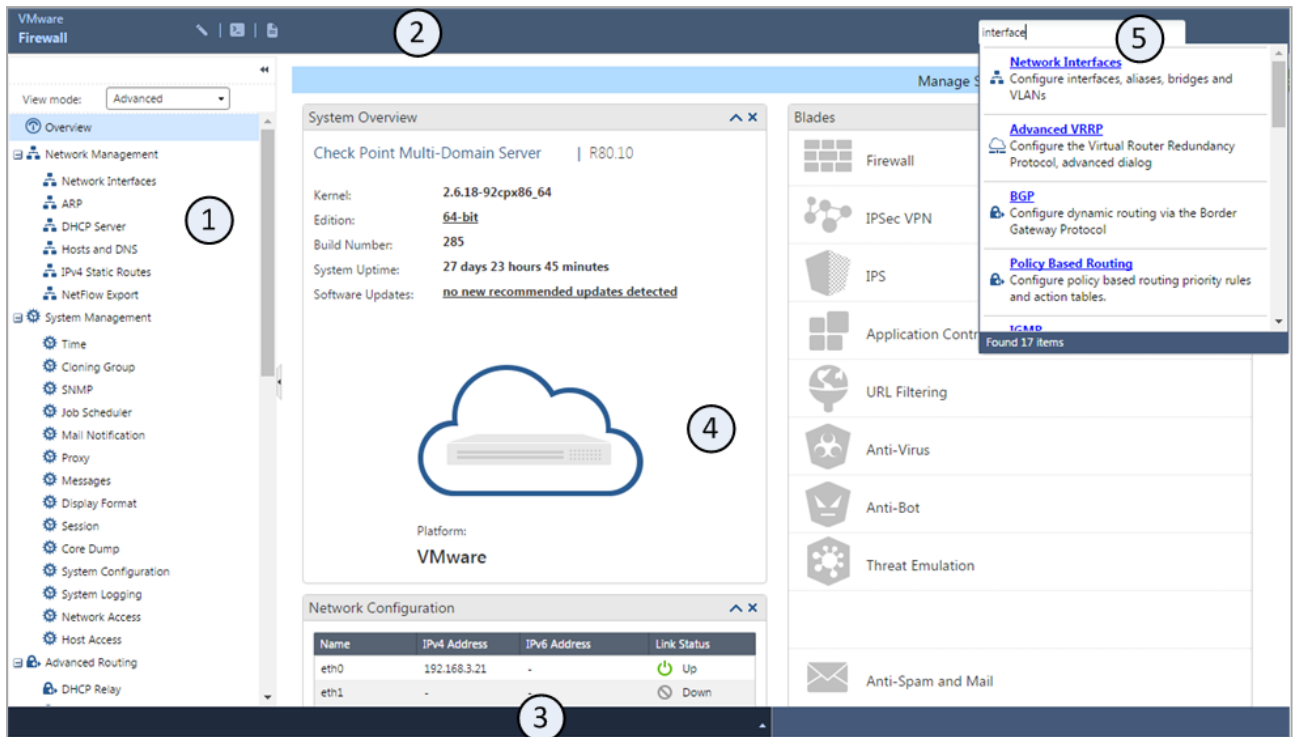
Important - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

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

You can easily change these modes.

- Web-Based Access to Command Line - Clientless access to the Gaia Clish directly from your web browser.

The Gaia Portal interface





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

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

Logging in to the Gaia Portal

To log in to the Gaia Portal:

Step	Instructions
1	<p>Enter this URL in your browser:</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"><code>https://<IP Address of Gaia Management Interface></code></div> <p> Important - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.</p>
2	<p>Enter your user name and password.</p>

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

 **Important:**

SSL connection ports on Security Management Servers R81 and higher

- A Security Management Server listens to SSL traffic for *all* services on the TCP port **443** in these cases:
 - If you performed a clean installation of a Security Management Server R81.20 and enabled the **Endpoint Policy Management** Software Blade.
 - If you upgraded a Security Management Server with disabled **Endpoint Policy Management** Software Blade to R81.20 and enabled this Software Blade after the upgrade.

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

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

- If you upgraded a Security Management Server with enabled **Endpoint Policy Management** Software Blade to R81.20, then the SSL port configuration *remains* as it was in the previous version, from which you upgraded:

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

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

In R81 and higher, an administrator can manually configure different TCP ports for the Gaia Portal (and other services) and Endpoint Security - **443** or **4434**. For the applicable procedures, see the [R81.20 Harmony Endpoint Security Server Administration Guide](#) > Chapter *Endpoint Security Architecture* > Section *Connection Port to Services on an Endpoint Security Management Server*.

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

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

- **Gaia Portal**

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

- **SmartView Web Application**

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

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

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

- 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 415](#)).

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 tree 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	30
Showing System Overview Information in Gaia Clish	32

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

Showing System Overview Information in Gaia Portal

Important:

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

The **Overview** page shows status widgets.

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

Widgets

Widget	Description
System Overview	System information, including: <ul style="list-style-type: none"> ▪ Installed product (for example: Check Point Security Management Server, Check Point Security Gateway) ▪ Product version number (for example: R81.20) ▪ 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.

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

Adding a widget to the page

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

Moving a widget on the page

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

Showing System Overview Information in Gaia Clish

Important for Scalable Platforms:

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

You can use these commands to show system status:

The "show uptime" command

Description

Shows how long the Gaia system is up and running.

Syntax

```
show uptime
```


The "show version" command

Description

Shows the name and versions of the Gaia OS components.

Syntax

- To show the full system version information:

```
show version all
```

- To show version information for OS components:

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

- To show name of the installed product:

```
show version product
```

Parameters

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

Getting Started

1. Install the Gaia OS.
See the [R81.20 Installation and Upgrade Guide](#).
2. Run the Gaia First Time Configuration Wizard.
See ["Configuring Gaia for the First Time" on page 58](#).
3. Configure the required interfaces:
 - A. Enable the required physical interfaces and assign the required IP addresses.
See ["Physical Interfaces" on page 102](#).
 - B. Configure the required special interfaces (Bond, VLAN, Bridge, and so on).
See ["Network Interfaces" on page 101](#).
4. Configure the required DNS settings.
See ["Hosts and DNS" on page 234](#).
5. Configure the required IPv4 and IPv6 static routes.
See:
 - ["IPv4 Static Routes" on page 245](#)
 - ["IPv6 Static Routes" on page 256](#)
6. Configure the required Proxy Server.
See ["Proxy" on page 286](#).
7. Configure the required Roles.
See ["Roles" on page 415](#).
8. Configure the required Users.
See ["Users" on page 404](#).
9. Configure the required Password Policy.
See ["Password Policy" on page 450](#).
10. Install the required license.
See ["License Status" on page 540](#).
11. Install the applicable software updates.
See ["CPUSE - Software Updates" on page 643](#).

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: <ul style="list-style-type: none"> ▪ In SmartConsole (see "Centrally Managing Gaia Device Settings" on page 90). ▪ 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 <code>admin</code> and <code>admin</code> .

Using the Gaia Clish on Security Groups

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

Step	Instructions
1	Connect to the command line on the applicable Security Group.
2	Log in to Gaia Clish.
3	Type this command and press Enter: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <code>gclish</code> </div>

Notes for Security Groups:

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

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

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

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

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

- To see the current config-lock, run:

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

- To acquire the config-lock, run:

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

- The Gaia gClish traffic runs in Security Groups on the Sync interface, on the TCP port 1129.
- Similarly to Gaia Clish, Gaia gClish is capable of running extended commands.

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

```
show commands extended
```

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

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

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

Saving the configuration changes

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

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

```
save config
```

Syntax Legend

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	<p>Shows the available nested subcommands:</p> <pre data-bbox="523 568 1458 797">main command → nested subcommand 1 → → nested subsubcommand 1-1 → → nested subsubcommand 1-2 → nested subcommand 2</pre> <p>Example:</p> <pre data-bbox="523 846 1458 1160">cpwd_admin config -a <options> -d <options> -p -r del <options></pre> <p>Meaning, you can run only one of these commands:</p> <ul style="list-style-type: none"> ▪ This command: <pre data-bbox="603 1272 1458 1339">cpwd_admin config -a <options></pre> ▪ Or this command: <pre data-bbox="603 1384 1458 1451">cpwd_admin config -d <options></pre> ▪ Or this command: <pre data-bbox="603 1496 1458 1563">cpwd_admin config -p</pre> ▪ Or this command: <pre data-bbox="603 1608 1458 1675">cpwd_admin config -r</pre> ▪ Or this command: <pre data-bbox="603 1720 1458 1787">cpwd_admin del <options></pre>
Curly brackets or braces { }	<p>Enclose a list of available commands or parameters, separated by the vertical bar .</p> <p>User can enter only one of the available commands or parameters.</p>

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>	<p>Complete or fetch the keyword.</p> <p>Example:</p> <pre>HostName> set in<TAB> inactivity-timeout - Set inactivity timeout interface - Displays the interface related parameters HostName> set in</pre>
<SPACE><TAB>	<p>Show the arguments that the command for that feature accepts.</p> <p>Example:</p> <pre>HostName> set interface<SPACE><TAB> eth0 eth1 lo HostName> set interface</pre>
<ESC><ESC>	<p>See possible command completions.</p> <p>Example:</p> <pre>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</pre>

Press ...	To do this ...
?	<p>Get help on a feature or keyword.</p> <p>Example:</p> <pre>HostName> set interface <?> interface: specifies the interface name This operation configures an existing interface HostName></pre>
UP arrow DOWN arrow	Browse the command history.
LEFT arrow RIGHT arrow	Edit the command.
Enter	<p>Run the command.</p> <p>The cursor does not have to be at the end of the line.</p> <p>You can usually abbreviate the command to the smallest number of unambiguous characters.</p>

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 56.

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

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
<code>0</code>	The operation word.
<code>n</code>	The <code>n</code> th word.

Word Designator	Meaning
^	The first argument; that is, word 1.
\$	The last argument.
%	The word matched by the most recent <code>\?str\?</code> 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 <code>str1</code> with <code>str2</code> in the first occurrence of the word, to which you refer.
g	Apply changes over the entire command. Use this modified in conjunction with <code>s</code> , as in <code>gs/str1/str2</code> .

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 415](#)).

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

<pre>set config-lock off on [timeout <5-900>] override</pre>
<pre>show config-lock config-state</pre>

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

Viewing the client environment

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

Configuring the client environment

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

Saving the client environment configuration permanently

```
save clienv
```


Parameters

Parameter	Description
<code>config-lock</code> {on off}	<p>Default value of the Clish <code>config-lock</code> parameter.</p> <p>If set to <code>on</code>, Gaia Clish locks the configuration when invoked. Otherwise, it continues without a configuration lock.</p> <p>When the configuration is locked by Gaia Clish, no configuration changes are possible in Gaia Portal, until the lock is released.</p>
<code>debug</code> {0-6}	<p>Debug level.</p> <p>Predefined levels are:</p> <ul style="list-style-type: none"> ▪ 0 - (Default) Do not debug, display error messages only ▪ 5 - Show the <code>confd</code> daemon requests and responses ▪ 6 - Show handler invocation parameters and results
<code>echo-cmd</code> {on off}	<p>If set to <code>on</code>, echoes all commands before executing them, when the command execution is done through the "<code>load configuration</code>" command.</p> <p>The default is <code>off</code>.</p>
<code>on-failure</code> {continue stop}	<p>Action performed on failure:</p> <ul style="list-style-type: none"> ▪ <code>continue</code> - Show error messages, but continue running commands from a file or a script ▪ <code>stop</code> - (Default) Stop running commands from a file or a script
<code>output</code> {pretty structured xml}	<p>Command line output format.</p> <p>The default is <code>pretty</code>.</p> <p>See "Client Environment Output Format" on page 51.</p>
<code>prompt</code> <Prompt String>	<p>Command prompt string.</p> <p>A valid prompt string can consist of any printable characters and a combination of these variables:</p> <ul style="list-style-type: none"> ▪ <code>%H</code> - Replaced with the Command number ▪ <code>%I</code> - Replaced with the User ID ▪ <code>%M</code> - Replaced with the Hostname ▪ <code>%P</code> - Replaced with the Product ID ▪ <code>%U</code> - Replaced with the Username <p>To set the prompt back to the default, use the keyword <code>default</code>.</p>
<code>rows</code> <Number of Rows>	<p>Number of rows to show in your terminal window.</p> <p>If the window size is changed, the number of rows also changes, unless the value is set to 0 (zero).</p>

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 <code>off</code> .

Client Environment Output Format

Gaia Clish supports these output formats:

Pretty

Output is formatted to be clear.

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

```
gaia> set clienv output pretty

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

Structured

Output is delimited by semi-colons.

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

```
gaia> set clienv output structured

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

XML


Adds XML tags to the output.

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

```
gaia> set clienv output xml

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

Expert Mode

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

The default Gaia shell is called `clish`.

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

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

For low-level configuration, use the more permissive Expert mode shell. In addition, see [sk144112](#).

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

Notes:

- If a command is supported in Gaia Clish, it is **not** supported to run the corresponding command in Expert mode.
For example, to work with interfaces, Gaia Clish provides the commands "`show interface`" and "`set interface`".
Therefore, it is **not** supported to run the `ifconfig` command in the Expert mode.
- Expert mode does not provide more privileges, only more configuration abilities.
- Expert mode is not a security feature. Rather, it offers protection against mistakes.
- Refer to [sk181230](#) to receive audit logs for the Expert mode login on Gaia servers.

For instructions to configure the Expert mode password, see "[System Passwords](#)" on [page 277](#).

User Defined (Extended) Commands

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

Description

Manage user defined (extended) commands in Gaia Clish.

Extended commands include:

1. Built in extended commands.

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

2. User defined commands.

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

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

Syntax

- To show all extended commands:

```
show extended commands
```

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

```
show command <Command>
```

- To add an extended command:

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

- To delete an extended command:

```
delete command <Command>
```

Parameters

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

See "[List of Available Extended Commands in Roles](#)" on page 446.

Example

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

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

Summary of Gaia Clish Commands

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

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

To show the list of all available Gaia Clish commands:

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

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

Step	Instructions
1	Connect to the command line on your Gaia system.
2	Log in to Gaia Clish.
3	Type: 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	<p>Connect a computer to the Gaia computer.</p> <p>On Scalable Platforms, connect a computer to the Gaia Management Interface of the Security Group.</p> <p>You must connect to the interface you configured during the Gaia installation (for example, eth0).</p>
2	<p>On your connected computer, configure a static IPv4 address in the same subnet as the IPv4 address you configured during the Gaia installation.</p>
3	<p>On your connected computer, in a web browser, connect to the IPv4 address you configured during the Gaia installation:</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>https://<IP address of Gaia Management Interface></pre> </div>
4	<p>Enter the default username and password: <code>admin</code> and <code>admin</code>.</p>
5	<p>Click Login.</p> <p>The Check Point First Time Configuration Wizard opens.</p>
6	<p>Follow the instructions on the First Time Configuration Wizard windows.</p> <p>See the applicable chapters below for installing specific Check Point products.</p>

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



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

"Deployment Options" window

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

Section	Options	Description
Setup	Continue with R81.20 configuration	Use this option to configure the installed Gaia and Check Point products.
Installation	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 chooses and installs major versions available on Check Point Cloud. The Gaia CPUSE performs the installation.
- **Pull appliance configuration** - This option applies the initial deployment configuration that includes different OS version on the appliance. You must prepare the initial deployment configuration with the Zero Touch Cloud Service. For more information, see [sk116375](#).

Scalable Platforms (Maestro and Chassis) do **not** support this feature

"Authentication Details" window

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



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

-  **Note** - You can change each password after you complete the Gaia First Time Configuration Wizard. See ["System Passwords" on page 277](#).
-  **Best Practice** - For security reasons, we recommend to configure a different passwords for the Expert mode and for the Maintenance Mode.

"Management Connection" window

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

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

Field	Description
Interface	By default, First Time Configuration Wizard selects the interface you configured during the Gaia installation (for example, eth0).  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: <ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> ▪ Manually - You configure the IPv6 settings in the next fields. ▪ Off - None.
IPv6 Address	Enter the applicable IPv6 address.  Important - R81.20 does not support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313).
Mask Length	Enter the applicable IPv6 mask length.
Default Gateway	Enter the IPv6 address of the applicable default gateway.

"Internet Connection" window

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

Field	Description
Interface	Select the applicable interface.
Configure IPv4	Select how the applicable interface gets its IPv4 address: <ul style="list-style-type: none"> ▪ 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	Optional: Select how the applicable interface gets its IPv6 address: <ul style="list-style-type: none"> ▪ 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.

"Device Information" window

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

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



"Date and Time Settings" window

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

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

"Installation Type" window




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


Field	Description
Security Gateway and/or Security Management	Select this option to install: <ul style="list-style-type: none"> ▪ A Single Security Gateway. ▪  Important - Scalable Platforms (Maestro and Chassis) support only this option. ▪ 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: <ul style="list-style-type: none"> ▪ A Multi-Domain Server, including Management High Availability. ▪ A dedicated single Multi-Domain Log Server. <p> Important - Scalable Platforms (Maestro and Chassis) do not support this feature</p>


"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	<p>Select this option to install:</p> <ul style="list-style-type: none"> • A single Security Gateway. •  Important - Scalable Platforms (Maestro and Chassis) support only this option. • A Cluster Member. • A Standalone.
Security Management	<p>Select this option to install:</p> <ul style="list-style-type: none"> • A Security Management Server, including Management High Availability. • An Endpoint Security Management Server. • An Endpoint Policy Server. • A CloudGuard Controller. • A dedicated single Log Server. • A dedicated single SmartEvent Server. • A Standalone. •  Important - Scalable Platforms (Maestro and Chassis) do not support this feature
Unit is a part of a cluster	<p>This option is available only if you selected Security Gateway.</p> <p>Select this option to install a cluster of dedicated Security Gateways, or a Full High Availability Cluster.</p> <p>Select the cluster type:</p> <ul style="list-style-type: none"> • ClusterXL - For a cluster of dedicated Security Gateways, or a Full High Availability Cluster. • VRRP Cluster - For a VRRP Cluster on Gaia. •  Important - Scalable Platforms (Maestro and Chassis) do not support this feature

Field	Description
Define Security Management as	<p>Select Primary to install:</p> <ul style="list-style-type: none"> • A Security Management Server. • An Endpoint Security Management Server. • An Endpoint Policy Server. • A CloudGuard Controller. <p>Select Secondary to install:</p> <ul style="list-style-type: none"> • A Secondary Management Server in Management High Availability. <p>Select Log Server / SmartEvent only to install:</p> <ul style="list-style-type: none"> • A dedicated single Log Server. • A dedicated single SmartEvent Server. <p> Important - Scalable Platforms (Maestro and Chassis) do not support this feature</p>

 **Notes** - In this window, you can select to install this Scalable Chassis 60000 / 40000 as a VSX Gateway.

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


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

 **Note** - By default, the option **Automatically download Blade Contracts, new software, and other important data** is enabled. See [sk111080](https://www.hpe.com/learn/sk111080).

"Dynamically Assigned IP" window

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

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

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

"Secure Communication to Management Server" window

This window appears only if:

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

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

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

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

"Security Management Administrator" window

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

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

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

"Security Management GUI Clients" window

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

Field	Description
Any IP Address	Select this option to allow all computers to connect.
This machine	Select this option to allow only a specific computer to connect. 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

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

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

Field	Description
Select leading interface	Select the applicable interface.

"Multi-Domain Server GUI Clients" window

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

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

Field	Description
Any host	Select this option to allow all computers to connect.
IP address	Select this option to allow only a specific computer to connect. 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 links at the bottom of this window:

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

For information about these settings, see [sk175504](#).

Field	Description
Automatically download and install Software Blade Contracts, security updates and other important data (highly recommended)	Controls the download of "Security" data from online Check Point servers: <ul style="list-style-type: none"> • Allows to update the installed Check Point products that are defined as "Security". For example, CPUSE Deployment Agent, Threat Emulation Engine. • Allows to download data that is defined as "Security". For example, signatures for the IPS Software Blade.
Automatically download software updates and new features (highly recommended)	Controls the download of "Non-Security" data from online Check Point servers: <ul style="list-style-type: none"> • Allows to update the installed Check Point products that are defined as "Non-Security". For example, updates for the CPinfo tool. • Allows to download data that is defined as "Non-Security".

Field	Description
<p>Help Check Point improve the product by sending anonymous information</p>	<p>Controls the upload of anonymous data to online Check Point servers:</p> <ul style="list-style-type: none"> • Allows to upload anonymous logs. For example, the upload of logs from the CPUSE tool. • Allows to upload anonymous diagnostics information. For example, the upload of data from the CPinfo and CPUSE tools. <p>Check Point uses this data internally for bug analysis and to improve the products. All data is subject to the European privacy policy (GDPR).</p>
<p>I approve sharing core dump files and other relevant crash data which might contain personal information</p>	<p>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. See "Crash Data" on page 366.</p> <p> Warning - Because core dump files contain a snapshot of the memory, they can contain personal and sensitive information.</p>



Notes:

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

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

Run:

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

Example outputs:

- From a Security Gateway or Cluster Member:

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

- From a Security Management Server or a Standalone:

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

- From a Multi-Domain Server:

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

- From a Scalable Platform Security Group:

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


Running the First Time Configuration Wizard in CLI Expert mode

Description

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

Notes:

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

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

Syntax

Viewing the configurable parameters

Form	Command
Short form	<code>config_system -l</code>
Long form	<code>config_system --list-params</code>

Running the First Time Configuration Wizard from a specified configuration file

Form	Command
Short form	<code>config_system -f <Path and Filename></code>
Long form	<code>config_system --config-file <Path and Filename></code>

Running the First Time Configuration Wizard from a specified configuration string

Form	Command
Short form	<code>config_system -s <String></code>
Long form	<code>config_system --config-string <String></code>

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

Form	Command
Short form	<code>config_system -t <Path></code>
Long form	<code>config_system --create-template <Path></code>

Making sure the First Time Configuration Wizard configuration file is valid

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

Procedure**Running the First Time Configuration Wizard from a configuration string**

Step	Instructions
1	<p>Run this command in Expert mode:</p> <pre>config_system --config-string <String of Parameters and Values></pre> <p>A configuration string must consist of <i>parameter=value</i> pairs, separated by the ampersand (&). You must enclose the whole string between quotation marks. For example:</p> <pre>"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"</pre> <p>For more information on valid parameters and values, run the "<code>config_system --list-params</code>" command.</p>
2	Reboot the system.

Creating a configuration file

Step	Instructions
1	<p>Run this command in the Expert mode:</p> <pre>config_system -t <File Name></pre>

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

Making sure the First Time Configuration Wizard configuration file is valid

Run this command in Expert mode:

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

Running the First Time Configuration Wizard from a configuration file

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

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

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

Parameters

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


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

Table: The 'config_system' parameters


Parameter	Supports Scalable Platforms?	Description	Valid values
admin_hash		Configures the administrator's password.	A string of alphanumeric characters, enclosed between single quotation marks.
default_gw_v4		Specifies IPv4 address of the default gateway.	Single IPv4 address.
default_gw_v6		Specifies IPv6 address of the default gateway.	Single IPv6 address.
domainname		Configures the domain name (optional).	Fully qualified domain name. Example: somedomain.com
download_info		<p>If its value is set to "true":</p> <ul style="list-style-type: none"> ▪ Downloads and installs Check Point Software Blade contracts. ▪ Downloads and installs Check Point security updates. ▪ Downloads other important information. <p>For more information, see sk94508 and sk175504.</p> <p> Best Practice - We highly recommended you enable this optional parameter.</p>	<ul style="list-style-type: none"> ▪ true (default) ▪ false

Table: The 'config_system' parameters (continued)



Parameter	Supports Scalable Platforms?	Description	Valid values
download_from_checkpoint_non_security		<p>If its value is set to "true":</p> <ul style="list-style-type: none"> Downloads Check Point software updates. Downloads new Check Point features. <p>For more information, see sk94508 and sk175504.</p> <p> Best Practice - We highly recommended you enable this optional parameter.</p>	<ul style="list-style-type: none"> true (default) false
ftw_sic_key		Configures the Secure Internal Communication key, if the value of the "install_security_managment" parameter is set to "false".	A string of alphanumeric characters (between 4 and 127 characters long).
gateway_cluster_member		Configures the Security Gateway as member of ClusterXL, if its value is set to "true".	<ul style="list-style-type: none"> true false
gateway_daip		Configures the Security Gateway as Dynamic IP (DAIP) Security Gateway, if its value is set to "true".	<ul style="list-style-type: none"> true false (default) <p> Note - Must be set to "false", if ClusterXL or Security Management Server is enabled.</p>
hostname		Configures the name of the local host (optional).	A string of alphanumeric characters.

Table: The 'config_system' parameters (continued)





Parameter	Supports Scalable Platforms?	Description	Valid values
iface		Interface name (optional).	Name of the interface exactly as it appears in the device configuration. Examples: eth0, eth1
install_mds_interface		Specifies Multi-Domain Server management interface.	Name of the interface exactly as it appears in the device configuration. Examples: eth0, eth1
install_mds_primary		Makes the installed Security Management Server the Primary Multi-Domain Server.  Note - The value of the "install_security_management" parameter must be set to "true".	<ul style="list-style-type: none"> ■ 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_management" parameter must be set to "true".	<ul style="list-style-type: none"> ■ true ■ false  Note - Can only be set to "true", if the value of the "install_mds_primary" parameter is set to "false".

Table: The 'config_system' parameters (continued)



Parameter	Supports Scalable Platforms?	Description	Valid values
install_mgmt_primary		<p>Makes the installed Security Management Server the Primary one.</p> <p> Notes:</p> <ul style="list-style-type: none"> ▪ 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". 	<ul style="list-style-type: none"> ▪ true ▪ false
install_mgmt_secondary		<p>Makes the installed Security Management Server a Secondary one.</p> <p> Notes:</p> <ul style="list-style-type: none"> ▪ 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". 	<ul style="list-style-type: none"> ▪ true ▪ false

Table: The 'config_system' parameters (continued)

Parameter	Supports Scalable Platforms?	Description	Valid values
install_mlm		Installs Multi-Domain Log Server, if its value is set to "true".	<ul style="list-style-type: none"> ■ true ■ false
install_security_gw		Installs Security Gateway, if its value is set to "true".	<ul style="list-style-type: none"> ■ true ■ false
install_security_managment		Installs a Security Management Server or a dedicated Log Server, if its value is set to "true".	<ul style="list-style-type: none"> ■ true ■ false
install_security_vsx		Installs VSX Gateway, if its value is set to "true".	<ul style="list-style-type: none"> ■ true ■ false
ipaddr_v4		Configures the IPv4 address of the management interface.	Single IPv4 address.
ipaddr_v6		Configures the IPv6 address of the management interface.	Single IPv6 address.
ipstat_v4		Turns on static IPv4 configuration, if its value is set to "manually".	<ul style="list-style-type: none"> ■ manually (default) ■ off
ipstat_v6		Turns static IPv6 configuration on, if its value is set to "manually".	<ul style="list-style-type: none"> ■ manually ■ off (default)
maas_authentication_key		Configures the authentication key for Management as a Service (MaaS). Applies only to Security Gateways.	A string of alphanumeric characters, enclosed between single quotation marks.
masklen_v4		Configures the IPv4 mask length for the management interface.	A number from 0 to 32.

Table: The 'config_system' parameters (continued)



Parameter	Supports Scalable Platforms?	Description	Valid values
masklen_v6		Configures the IPv6 mask length for the management interface.	A number from 0 to 128.
mgmt_admin_name		Configures the management administrator's username.  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.

Table: The 'config_system' parameters (continued)


Parameter	Supports Scalable Platforms?	Description	Valid values
mgmt_admin_radio		Configures Management Server administrator.  Note - You must specify this parameter, if you install a Management Server.	<ul style="list-style-type: none"> ▪ 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_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_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
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
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

Table: The 'config_system' parameters (continued)

Parameter	Supports Scalable Platforms?	Description	Valid values
mgmt_gui_clients_radio		Specifies SmartConsole clients that can connect to the Security Management Server.	<ul style="list-style-type: none"> ■ any ■ range ■ network ■ this
mgmt_gui_clients_subnet_field		Specifies the netmask, if the value of the "mgmt_gui_clients_radio" parameter is set to "network".	A number from 1 to 32.
ntp_primary		Configures the IP address of the primary NTP server (optional).	IPv4 address.
ntp_primary_version		Configures the NTP version of the primary NTP server (optional).	<ul style="list-style-type: none"> ■ 1 ■ 2 ■ 3 ■ 4
ntp_secondary		Configures the IP address of the secondary NTP server (optional).	IPv4 address.
ntp_secondary_version		Configures the NTP version of the secondary NTP server (optional).	<ul style="list-style-type: none"> ■ 1 ■ 2 ■ 3 ■ 4
primary		Configures the IP address of the primary DNS server (optional).	IPv4 address.
proxy_address		Configures the IP address of the proxy server (optional).	IPv4 address, or Hostname.
proxy_port		Configures the port number of the proxy server (optional).	A number from 1 to 65535.

Table: The 'config_system' parameters (continued)




Parameter	Supports Scalable Platforms?	Description	Valid values
reboot_if_required		Reboots the system after the configuration, if its value is set to "true" (optional).	<ul style="list-style-type: none"> ■ true ■ false
secondary		Configures the IP address of the secondary DNS server (optional).	IPv4 address.
sg_cluster_id		For Check Point Support use only.	
tertiary		Configures the IP address of the tertiary DNS server (optional).	IPv4 address.
timezone		Configures the Area/Region (optional).	<p>The Area/Region must be enclosed between single quotation marks. Examples: 'America/New_York' 'Asia/Tokyo'</p> <p> 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></p>

Table: The 'config_system' parameters (continued)

Parameter	Supports Scalable Platforms?	Description	Valid values
upload_crash_data		<p>Uploads core dump files that help Check Point resolve stability issues, if its value is set to "true". For more information, see "Crash Data" on page 366.</p> <p> Warning - The core dump files may contain personal data.</p>	<ul style="list-style-type: none"> ▪ true ▪ false (default)
upload_info		<p>Uploads data that helps Check Point provide you with optimal services, if its value is set to "true". For more information, see sk94509.</p> <p> Best Practice - We highly recommended you enable this optional parameter.</p>	<ul style="list-style-type: none"> ▪ true ▪ false (default)

Centrally Managing Gaia Device Settings

In This Section:

Introduction of Gaia Central Management	90
Managing Gaia in SmartConsole	92
Running Command Scripts	92
Understanding One-Time Scripts	95
Running Repository Scripts	95
Backup and Restore	96
Opening Gaia Portal and Gaia Clish	99

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

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

Introduction of Gaia Central Management

SmartConsole lets you:

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

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

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

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

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

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

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

Managing Gaia in SmartConsole

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



Running Command Scripts

One Time scripts


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

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

Running a one-time script

Step	Instructions
1	Right-click the Security Gateway.
2	Select Scripts > Run One Time Script .
3	<p>The Run One Time Script window opens You can:</p> <ul style="list-style-type: none"> ▪ Enter the command in the Script Body text box and specify script arguments, or ▪ Load the complete command from a text file <p> Notes:</p> <ul style="list-style-type: none"> • 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	<p>Click Run. The output from the script shows in the Tasks tab > Results column.</p> <ul style="list-style-type: none"> ▪ 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 <p> Notes:</p> <ul style="list-style-type: none"> • 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.

Running a script from the repository

Step	Instructions
1	Right-click the Security Gateway.
2	Select Scripts > Run Repository Script .
3	<p>The Select Script window opens. You can:</p> <ul style="list-style-type: none"> ▪ Select a script from the drop-down box, or click New to create a new script for the repository. ▪ Enter script arguments. <p> Note - The Select Script window does not support interactive or continuous scripts. To run interactive or continuous scripts, open a command shell.</p>
4	<p>Click Run. The output from the script shows in the Tasks tab > Results column.</p> <ul style="list-style-type: none"> ▪ 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.

Managing scripts

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

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

Understanding One-Time Scripts

If you specify a script:

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

Running Repository Scripts

You can run a predefined script from the script repository.

Running a script from the repository

Step	Instructions
1	In the Gateways & Servers view, right-click the Security Gateways or Security Management Servers, on which you want to run scripts.
2	Select Scripts > Scripts Repository . The Scripts Repository window opens.
3	Do one of these steps: <ul style="list-style-type: none"> ▪ 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.

Backing up the system

Step	Instructions
1	In the Gateways & Servers view, right-click the Security Gateway object you want to back up.
2	Select Actions > System Backup . The System Backup window opens.
3	<p>Select the backup location. Use one of these options:</p> <ul style="list-style-type: none"> ▪ 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 <p>Note - The path to the backup directory must start and end with forward slash (/) character. For example: <code>/ftroot/backup/</code>, or just <code>/</code> for the root directory of the server.</p> <p>The file name must be according to this convention:</p> <pre>backup_<Name of Security Gateway object>_<Date of Backup>.tgz</pre>
4	Click OK . The status of the backup operation shows in Tasks .
5	<p>When the task is complete, double-click the entry to see the file path and name of the backup file.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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

Restoring the system

Step	Instructions
1	In the Gateways & Servers view, right-click the Security Gateway object you want to restore.
2	Select Actions > System Restore . The System Restore window opens.
3	<p>Enter the required information.</p> <p> 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:</p> <ol style="list-style-type: none"> Right-click the Security Gateway object. Select Actions > Open Shell. On the Security Gateway, run the Gaia Clish command: <div data-bbox="493 882 1458 947" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>show backup logs</pre> </div> Find the name of the compressed backup file. The file is named according to this convention: <div data-bbox="493 1037 1458 1137" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>backup_<Name of Security Gateway object>_<Date of Backup>.tgz</pre> </div>
4	<p>Click OK.</p> <ol style="list-style-type: none"> Connectivity to the Security Gateway is lost. 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.

Opening a command line window on the Security Gateway

Step	Instructions
1	In SmartConsole, right-click the Security Gateway object.
2	<p>Select Actions > Open Shell.</p> <ul style="list-style-type: none"> ▪ 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. <p>A command line window opens with default shell that was configured for the specified user.</p>

Opening a Security Gateway Gaia Portal

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

Network Management


This chapter includes configuration procedures for:

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

Network Interfaces

Gaia supports these network interface types:

Interface Type	Comments
Ethernet physical	
Alias	<p>This feature adds Secondary IP addresses on different interface types.</p> <ul style="list-style-type: none"> ▪ ClusterXL does not support this feature. ▪ On Scalable Platforms (Maestro and Chassis), it is necessary to set the value of the kernel parameter <code>fwha_arp_support_aliases</code> to 1 before the configuration. The feature is not supported in VSX mode.
VLAN	
VxLAN	Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation PMTR-60874).
Bond	
MAGG	This section applies only to Scalable Platforms (Maestro and Chassis).
Bridge	
Loopback	
VPN tunnel	Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation 00737055).
6in4 tunnel	Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation MBS-12823).
PPPoE	Scalable Platforms (Maestro and Chassis) do not support this feature.
GRE	Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation PMTR-60868).

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

Physical Interfaces

In This Section:

Configuring Physical Interfaces in Gaia Portal	103
Configuring Physical Interfaces in Gaia Clish	105

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

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

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

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


Adding or removing an interface card


Step	Instructions
1	Turn off the Gaia computer: <ul style="list-style-type: none"> ▪ In Gaia Portal: Click Maintenance > Shut Down, and click Halt ▪ In Gaia Clish: Run: <code>halt</code>
2	Add, remove, or replace the interface cards.
3	Turn on the Gaia computer.

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




Configuring Physical Interfaces in Gaia Portal

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

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

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

Configuring a physical interface

Step	Instructions
1	In the navigation tree, click Network Management > Network Interfaces .
2	Select an interface from the list and click Edit .
3	Select the Enable option to set the interface status to UP.
4	In the Comment field, enter the applicable comment text (up to 100 characters).
5	On the IPv4 tab, do one of these: <ul style="list-style-type: none"> ▪ Select Obtain IPv4 address automatically to get the IPv4 address from the DHCPv4 server. <ul style="list-style-type: none">  Important - Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation MBS-3246). ▪ Enter the IPv4 address and subnet mask in the applicable fields.
6	Optional: On the IPv6 tab, do one of these: <ul style="list-style-type: none"> ▪ Select Obtain IPv6 address automatically to get the IPv6 address from the DHCPv6 server. <ul style="list-style-type: none">  Important - Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation MBS-3246). ▪ Enter the IPv6 address and mask length in the applicable fields. <p> Important:</p> <ul style="list-style-type: none"> ▪ First, you must enable the IPv6 Support and reboot (see "System Configuration" on page 370). ▪ R81.20 does not support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313). ▪ Multi-Domain Server does not support IPv6 at all (Known Limitation PMTR-14989).

Step	Instructions
7	<p>On the Ethernet tab:</p> <ul style="list-style-type: none"> ▪ 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 the configuration procedure: <ul style="list-style-type: none"> • On a Security Gateway and ClusterXL, see the R81.20 Installation and Upgrade Guide > Chapter <i>Special Scenarios for Security Gateways</i> > Section <i>Deploying a Security Gateway in Monitor Mode</i>. • On Maestro, see the R81.20 Quantum Maestro Administration Guide > Chapter <i>Deploying a Security Group in Monitor Mode</i>. • On Scalable Chassis, see the R81.20 Quantum Scalable Chassis Administration Guide > Chapter <i>Deploying a Security Group in Monitor Mode</i>.
8	Click OK .

Configuring Physical Interfaces in Gaia Clish

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

Syntax

Configuring an interface

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

Viewing all configured settings of all interfaces

```
show interfaces all
```

Viewing all configured settings of a specific interface

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

Viewing the specific configured setting of a specific interface


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


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

Parameters

CLI Parameters

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

Parameter	Description
<pre>auto-negotiation {on off}</pre>	<p>Configures automatic negotiation of interface link speed and duplex settings:</p> <ul style="list-style-type: none"> ▪ on - Enabled ▪ off - Disabled
<pre>comments "Text"</pre>	<p>Configures an optional free text comment.</p> <ul style="list-style-type: none"> ▪ 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.
<pre>ipv4-address <IPv4 Address></pre>	<p>Configures the IPv4 address.</p>
<pre>ipv6-address <IPv6 Address></pre>	<p>Configures the IPv6 address.</p> <p> Important:</p> <ul style="list-style-type: none"> ▪ First, you must enable the IPv6 Support and reboot (see "System Configuration" on page 370). ▪ R81.20 does not support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313).
<pre>links <Number></pre>	<p>Configures the minimal number of required link interfaces for a ClusterXL Bond Load Sharing.</p>
<pre>subnet-mask <Mask></pre>	<p>Configures the IPv4 subnet mask using dotted decimal notation (X.X.X.X).</p>
<pre>mask-length <Mask Length></pre>	<p>Configures the IPv4 or IPv6 subnet mask length using the CIDR notation (integer between 2 and 32).</p>

Parameter	Description
<pre>ipv6-autoconfig {on off}</pre>	<p>Configures if this interface gets an IPv6 address from a DHCPv6 Server:</p> <ul style="list-style-type: none"> ▪ <code>on</code> - Gets an IPv6 address from a DHCPv6 Server ▪ <code>off</code> - Does not get an IPv6 address from a DHCPv6 Server (you must assign it manually) <p> Important:</p> <ul style="list-style-type: none"> ▪ First, you must enable the IPv6 Support and reboot (see "System Configuration" on page 370). ▪ Scalable Platforms (Maestro and Chassis) do not support this feature
<pre>link-speed {10M/half 10M/full 100M/half 100M/full 1000M/full 1000M/full}</pre>	<p>Configures the interface link speed and duplex status. Available speed and duplex combinations are:</p> <ul style="list-style-type: none"> ▪ 10M/half ▪ 10M/full ▪ 100M/half ▪ 100M/full ▪ 1000M/full ▪ 10000M/full
<pre>mac-addr <MAC Address></pre>	<p>Configures the hardware MAC address.</p>
<pre>monitor-mode {on off}</pre>	<p>Configures Monitor Mode on this interface:</p> <ul style="list-style-type: none"> ▪ <code>on</code> - Enabled ▪ <code>off</code> - Disabled <p>Default: <code>off</code></p> <p>For the configuration procedure:</p> <ul style="list-style-type: none"> ▪ On a Security Gateway and ClusterXL, see the R81.20 Installation and Upgrade Guide > Chapter <i>Special Scenarios for Security Gateways</i> > Section <i>Deploying a Security Gateway in Monitor Mode</i>. ▪ On Maestro, see the R81.20 Quantum Maestro Administration Guide > Chapter <i>Deploying a Security Group in Monitor Mode</i>. ▪ On Scalable Chassis, see the R81.20 Quantum Scalable Chassis Administration Guide > Chapter <i>Deploying a Security Group in Monitor Mode</i>.

Parameter	Description
<code>mtu <68-16000 1280-16000></code>	<p>Configures the Maximum Transmission Unit size for an interface.</p> <p>For IPv4:</p> <ul style="list-style-type: none"> ▪ Range: 68 - 16000 bytes ▪ Default: 1500 bytes <p>For IPv6:</p> <ul style="list-style-type: none"> ▪ Range: 1280 - 16000 bytes ▪ Default: 1500 bytes
<code>rx-ringsize <0-4096></code>	<p>Configures the receive buffer size.</p> <ul style="list-style-type: none"> ▪ Range: 0 - 4096 bytes ▪ Default: Depends on the interface driver
<code>state {on off}</code>	<p>Configures the interface state:</p> <ul style="list-style-type: none"> ▪ <code>on</code> - Enabled ▪ <code>off</code> - Disabled
<code>tx-ringsize <0-4096></code>	<p>Configures the transmit buffer size.</p> <ul style="list-style-type: none"> ▪ 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	109
Configuring Aliases in Gaia Clish	111
Configuring Aliases on Scalable Platforms	113

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

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

Notes:


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

Configuring Aliases in Gaia Portal

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

Adding an interface alias

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

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

Deleting an interface alias

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

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

Configuring Aliases in Gaia Clish

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

Syntax

Adding an alias

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

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

Viewing the configured aliases

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

Deleting an alias

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

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

Parameters

CLI Parameters

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

Example

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


Configuring Aliases on Scalable Platforms

Notes:

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

Important:

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




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

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



For additional information, see [sk167073](#).

Adding an alias

Step	Instructions
1	<p>Set the value of the kernel parameter fwha_arp_support_aliases to 1:</p> <ol style="list-style-type: none"> Connect to the command line on the Security Group. Log in to the Expert mode. Configure the value <i>temporarily</i> (does not survive reboot): <pre>g_fw ctl set int fwha_arp_support_aliases 1</pre> Make sure the new value is set: <pre>g_fw ctl get int fwha_arp_support_aliases</pre> Configure the value <i>permanently</i> (requires reboot - you can reboot later at any time): <pre>g_update_conf_file \$FWDIR/boot/modules/fwkern.conf fwha_arp_support_aliases=1</pre>

Step	Instructions
2	<p>In Gaia gClish of the applicable Security Group, add the applicable interface alias:</p> <ol style="list-style-type: none"> Connect to the command line on the Security Group. Log in to Gaia Clish. On Scalable Platforms, go to Gaia gClish: Type <code>gclish</code> and press Enter. Add the applicable interface alias: <div data-bbox="432 506 1460 609" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>add interface <Name of Interface> alias <IPv4 Address>/<Mask Length></pre> </div> <ul style="list-style-type: none">  Important - After you add, configure, or delete features, run the "save config" command to save the settings permanently.  Note - A new alias interface name is automatically created by adding a sequence number to the original interface name. For example, the name of first alias added to eth1 is eth1:1. The second alias added is eth1:2, and so on.
3	<p>Update the topology of the Security Gateway object in SmartConsole:</p> <ol style="list-style-type: none"> Connect with SmartConsole to the Management Server that manages this Security Group. Open the applicable Security Gateway object. From the left tree, click Network Management. Click Get Interfaces > Get Interfaces with Topology. <ul style="list-style-type: none">  Best Practice - In the Topology > Leads To section, use the default topology settings in the interface, on which you add an interface alias (and not the Override option). Otherwise, it is not possible to link alias networks to the applicable interface. Make sure the information is correct and click Accept. Click OK.
4	<p>Install the Access Control Policy on this Security Gateway object.</p>
5	<p>Make sure the configuration is consistent on all Security Group Members:</p> <ol style="list-style-type: none"> Connect to the command line on the Security Group. Log in to the Expert mode. Run: <div data-bbox="432 1720 1460 1787" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>config_verify -v</pre> </div>

Deleting an alias

Step	Instructions
1	<p>In Gaia gClish of the applicable Security Group, delete the applicable interface alias:</p> <ol style="list-style-type: none"> Connect to the command line on the Security Group. Log in to Gaia Clish. On Scalable Platforms, go to Gaia gClish: Type <code>gclish</code> and press Enter. Add the applicable interface alias: <div data-bbox="432 566 1460 669" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>delete interface <Name of Interface> alias <Name of Alias Interface></pre> </div> <p> Important - After you add, configure, or delete features, run the "save config" command to save the settings permanently.</p>
2	<p>Update the topology of the Security Gateway object in SmartConsole:</p> <ol style="list-style-type: none"> Connect with SmartConsole to the Management Server that manages this Security Group. Open the applicable Security Gateway object. From the left tree, click Network Management. Click Get Interfaces > Get Interfaces with Topology. <ul style="list-style-type: none">  Best Practice - In the Topology > Leads To section, use the default topology settings in the interface, on which you delete an interface alias (and not the Override option). Make sure the information is correct and click Accept. Click OK.
3	<p>Install the Access Control Policy on this Security Gateway object.</p>
4	<p>Make sure the configuration is consistent on all Security Group Members:</p> <ol style="list-style-type: none"> Connect to the command line on the Security Group. Log in to the Expert mode. Run: <div data-bbox="432 1574 1460 1637" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>config_verify -v</pre> </div>

Viewing the configured aliases

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

CLI Parameters

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

Example

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

VLAN Interfaces

In This Section:

Configuring VLAN Interfaces in Gaia Portal	117
Configuring VLAN Interfaces in Gaia Clish	120
Access Mode VLAN and Trunk Mode VLAN	123

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

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

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

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



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



Notes:




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

Configuring VLAN Interfaces in Gaia Portal




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

Adding a VLAN interface

Step	Instructions
1	In the navigation tree, click Network Management > Network Interfaces .
2	Make sure that the physical interface, on which you add a VLAN interface, does not have an IP address.
3	Click Add > VLAN .
4	In the Add VLAN window, select the Enable option to set the VLAN interface to UP.
5	<p>On the IPv4 tab, do one of these:</p> <ul style="list-style-type: none"> ▪ Select Obtain IPv4 address automatically to get the IPv4 address from the DHCPv4 server. <ul style="list-style-type: none">  Important - Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation MBS-3246). ▪ Enter the IPv4 address and subnet mask in the applicable fields.
6	<p>Optional: On the IPv6 tab, do one of these:</p> <ul style="list-style-type: none"> ▪ Select Obtain IPv6 address automatically to get the IPv6 address from the DHCPv6 server. <ul style="list-style-type: none">  Important - Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation MBS-3246). ▪ Enter the IPv6 address and mask length in the applicable fields. <p> Important:</p> <ul style="list-style-type: none"> ▪ First, you must enable the IPv6 Support and reboot (see "System Configuration" on page 370). ▪ R81.20 does not support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313). ▪ Multi-Domain Server does not support IPv6 at all (Known Limitation PMTR-14989).
7	On the VLAN tab, enter or select a VLAN ID (VLAN tag) between 2 and 4094.
8	In the Member Of field, select the applicable physical interface.
9	Click OK .

Editing a VLAN interface

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

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

Deleting a VLAN interface

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

Configuring VLAN Interfaces in Gaia Clish

Important:

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


Syntax

Adding a new VLAN interface

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

Configuring a VLAN interface

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

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


Viewing the configuration of a specific VLAN interface

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

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



Deleting a VLAN interface

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

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

Parameters

CLI Parameters

Parameter	Description
<i><Name of Physical Interface></i>	Specifies a physical interface.
comments "Text"	Defines the optional comment. <ul style="list-style-type: none"> ▪ 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.
<i><VLAN ID></i>	Configures the ID of the VLAN interface (integer between 2 and 4094).
<i><IPv4 Address></i>	Assigns the IPv4 address.
<i><IPv6 Address></i>	Assigns the IPv6 address. <p> Important - First, you must enable the IPv6 Support and reboot (see "System Configuration" on page 370).</p>
subnet-mask <i><Mask></i>	Configures the IPv4 subnet mask using the dotted decimal notation (X.X.X.X) - integer between 2 and 32..
mask-length <i><Mask Length></i>	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: <ul style="list-style-type: none"> ▪ 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) <p> Important - First, you must enable the IPv6 Support and reboot (see "System Configuration" on page 370).</p>

Parameter	Description
mtu <68-16000 1280-16000>	<p>Configures the Maximum Transmission Unit size for an interface.</p> <p>For IPv4:</p> <ul style="list-style-type: none"> ▪ Range: 68 - 16000 bytes ▪ Default: 1500 bytes <p>For IPv6:</p> <ul style="list-style-type: none"> ▪ Range: 1280 - 16000 bytes ▪ Default: 1500 bytes
state {on off}	<p>Configures interface's state:</p> <ul style="list-style-type: none"> ▪ 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.

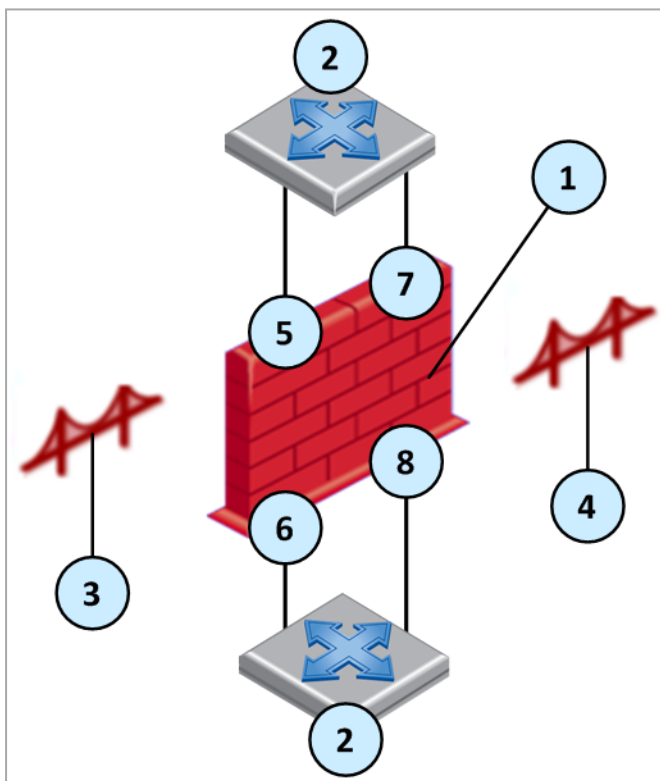
For **VLAN translation**, use different numbered VLAN interfaces to create the Bridge interface.

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 165](#)).

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 165](#)).

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

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




Note - VLAN translation is not supported in Trunk mode.

VXLAN Interfaces

In This Section:

Configuring VXLAN Interfaces in Gaia Portal	126
Configuring VXLAN Interfaces in Gaia Clish	128
Configuring VXLAN Interfaces on Cluster Members	130

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

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

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

Notes:

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




 **Warning** - By default, SecureXL does **not** accelerate traffic over a VXLAN tunnel.

- If you configure SecureXL to accelerate such traffic, the Firewall only inspects the payload of VXLAN packets (it does **not** inspect the VXLAN data).
- To configure SecureXL to accelerate such traffic, set the value of the SecureXL kernel parameter `sim_enable_vxlan` to 1 (one) in the `$PPKDIR/conf/simkern.conf` file and reboot.
For more information, see the [R81.20 Performance Tuning Administration Guide](#) > Chapter *Working with Kernel Parameters on Security Gateway* > Section *SecureXL Kernel Parameters*.

For additional information, see [sk170014](#).

Configuring VXLAN Interfaces in Gaia Portal

Adding a VXLAN interface

Step	Instructions
1	In the navigation tree, click Network Management > Network Interfaces .
2	Click Add > VXLAN .
3	In the Add VXLAN window, select the Enable option to set the VXLAN interface to UP.
4	On the IPv4 tab, enter the local IPv4 address and subnet mask for the VXLAN interface.
5	<p>Optional: On the IPv6 tab, enter the local IPv6 address and mask length for the VXLAN interface.</p> <p> Important - First, you must enable the IPv6 Support and reboot (see "System Configuration" on page 370).</p>
6	<p>On the VXLAN Tunnel tab:</p> <ol style="list-style-type: none"> In the VXLAN VNI field, enter or select the VXLAN Network Identifier (or VXLAN Segment ID) between 1 and 16,777,215. <p> Important - This value must be the same on the VXLAN peers.</p> In the Member Of field, select the physical interface related to this VXLAN. In the Remote Address field, enter the IPv4 address of the applicable physical interface on the remote VXLAN peer. In the DST Port field, enter or select the destination UDP port number between 1 and 65535 (default is 4789 - see IANA Service Name and Port Number Registry). <p> Best Practice - Use the default UDP port 4789.</p>
7	Click OK .

Example

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

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


<==> (Internet) <==>

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

The VXLAN interface configuration on these VXLAN peers:

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

Editing a VXLAN interface

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

Deleting a VXLAN interface

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

Configuring VXLAN Interfaces in Gaia Clish

Syntax

Adding a VXLAN interface

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

Viewing the configured VxLAN interface

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

Editing a VXLAN interface

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



Deleting a VXLAN interface

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

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

CLI Parameters

Parameter	Description
id <VXLAN VNI>	Configures the VXLAN Network Identifier (or VXLAN Segment ID) of the VXLAN interface (integer between 1 and 16,777,215). Important - This value must be the same on the VXLAN peers.
comments "Text"	Defines the optional comment. <ul style="list-style-type: none"> 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.
dev <Name of local physical interface>	Specifies a local physical interface.

Parameter	Description
<code>dstport <Destination UDP port></code>	<p>Specifies the destination UDP port number between 1 and 65535 (default is 4789 - see IANA Service Name and Port Number Registry).</p> <ul style="list-style-type: none">  Important - This value must be the same on the VXLAN peers.  Best Practice - Use the default UDP port 4789.
<code>remote <IPv4 address of physical interface on remote peer></code>	Specifies the IPv4 address of the applicable physical interface on the remote VXLAN peer.

Example

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

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

<==> (Internet) <===>

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

The VXLAN interface configuration on these VXLAN peers:

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

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

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

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

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

Configuring VXLAN Interfaces on Cluster Members

For more information, see the [R81.20 ClusterXL Administration Guide](#).

In Cluster, you have these options:

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

1. Configure a VXLAN interface on all the Cluster Members.
You must configure the *same* VXLAN VNI and **Remote Address** on each Cluster Member.
2. Connect with SmartConsole to the Management Server.
3. From the left navigation panel, click **Gateways & Servers**.
4. Double-click the cluster object.
5. From the left tree, click **Network Management**.
6. From the toolbar, click **Get Interfaces > Get Interfaces With Topology** and confirm.
Make sure you see the new VXLAN interface from each Cluster Member.
7. Select the new VXLAN interface and click **Edit**.
8. From the left tree, click the **General** page.
9. In the **General** section, in the **Network Type** field, select **Cluster**.
10. In the **IPv4** field, configure the applicable cluster Virtual IP address.
11. In the **Member IPs** section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.
12. Click **OK**.
13. Publish the SmartConsole session.
14. Install the Access Control Policy on this cluster object.

To use a VXLAN interface only on a specific Cluster Member

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

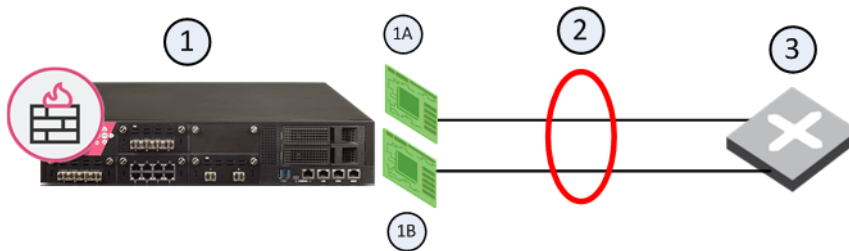
Make sure you see the new VXLAN interface from the specific Cluster Member, on which you configured it.

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

Bond Interfaces (Link Aggregation)

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

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



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

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

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

High Availability (Active/Backup)


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

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



Load Sharing (Active/Active)

All subordinate interfaces in the UP state are used simultaneously.

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

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

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

Mode	Description
Round Robin	Selects the Active subordinate interfaces sequentially.  Note - Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation MBS-4080).
802.3ad	Dynamically uses Active subordinate interfaces to share the traffic load. This mode uses the LACP protocol, which fully monitors the interface link between the Check Point Security Gateway and a switch.
XOR	All subordinate interfaces in the UP state are Active for Load Sharing. Traffic is assigned to Active subordinate interfaces based on one of these transmit hash policies: <ul style="list-style-type: none"> ▪ Layer 2 information (XOR of hardware MAC addresses) ▪ Layer 3+4 information (IP addresses and Ports)
ABXOR	Subordinate interfaces in the UP state are assigned to sub-groups called <i>bundles</i> . Only one bundle is Active at a time. All subordinate interfaces in the Active bundle share the traffic load. The system assigns traffic to all interfaces in the Active bundle based on the defined transmit hash policy.  Note - Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation MBS-1520).


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



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



See the [R81.20 Release Notes](#).


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

Configuring Bond Interfaces in Gaia Portal

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

Step	Instructions
1	In the navigation tree, click Network Management > Network Interfaces .
2	Make sure that the subordinate interfaces, which you wish to add to the Bond interface, do not have IP addresses.
3	For a new bond interface, select Add > Bond . 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.  Important - Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation MBS-3246).
5	On the IPv6 tab (optional), enter the IPv6 address and mask length. You can optionally select the Obtain IPv6 Address automatically option.  Important: <ul style="list-style-type: none"> ▪ First, you must enable the IPv6 Support and reboot (see "System Configuration" on page 370). ▪ Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation MBS-3246 and PMTR-47313). ▪ R81.20 does not support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313). Multi-Domain Server does not support IPv6 at all (Known Limitation PMTR-14989).

Step	Instructions
6	<p>On the Bond tab:</p> <ol style="list-style-type: none"> Select or enter a Bond Group ID. This parameter is an integer between 0 and 1024. Select the subordinate interfaces from the Available Interfaces list and then click Add. <ul style="list-style-type: none">  Note - Make sure that the subordinate interfaces do not have any IP addresses or aliases configured. Select an Operation Mode: <ul style="list-style-type: none"> ▪ Round Robin (default) Bond uses all subordinate interfaces sequentially (High Availability + Load Sharing). <ul style="list-style-type: none">  Note - Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation MBS-4080). ▪ 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).
7	<p>On the Advanced tab:</p> <ol style="list-style-type: none"> Configure the required MTU for your network (if not sure, leave the default value). 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. 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. Configure the Up Delay - How much time to wait, after sending a monitor request to a subordinate interface, before bringing up the subordinate interface. The valid range is 1-5000 ms. The default is 200 ms.

Step	Instructions
8	<p>Additional configuration settings are available depending on the selected Bond Operation Mode:</p> <ul style="list-style-type: none"> ▪ 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. <ul style="list-style-type: none">  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 R81.20 ClusterXL Administration Guide > Chapter <i>ClusterXL Requirements and Compatibility</i> > Section <i>Supported Topologies for Synchronization Network</i>. ▪ 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: <ol style="list-style-type: none"> 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 .

 **Notes:**

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

Configuring Bond Interfaces in Gaia Clish

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

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

Notes:

- You configure an IP address on a Bonding Group in the same way as you do on a physical interface (see ["Physical Interfaces" on page 102](#)).
- The name of a Bond interface in Gaia is "bond<Bond Group ID>".
For example, the name of a bond interface with a Bond Group ID of 5 is "bond5".
- To configure MTU on a Bond subordinate interface, you must configure MTU on the Bond interface.
This MTU applies to all subordinate interfaces assigned to this Bond interface.

Important:

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

Syntax


Adding a new Bonding Group

Syntax

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

Example


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

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

Adding a new subordinate interface to an existing Bonding Group

Syntax

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

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

Example

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

 **Notes:**

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

Configuring an existing Bonding Group

Syntax

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

Configuring the Bond Operating Mode

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

Syntax

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

Example

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

Notes:

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

Configuring the Up Delay Time


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

Syntax

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

Example

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

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

Configuring the Down Delay Time


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

Syntax

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

Example

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

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

Configuring the Media Monitoring Interval

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

Syntax

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

Example

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



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

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

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

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

Syntax

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

Example

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



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

Configuring an IP address on the existing Bonding Group

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

For more information, see "[Configuring Physical Interfaces in Gaia Clish](#)" on page 105.


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. <ul style="list-style-type: none"> ▪ Range: 0 - 1024 ▪ Default: No default value

Parameter	Description
<code><Name of Subordinate Interface></code>	<p>Specifies the name of the subordinate physical interface, which you add to (or remove from) the bond group.</p> <p>Make sure that the subordinate interfaces do not have any IP addresses or aliases configured.</p>
<code>mode <Mode></code>	<p>Configures the Bond operating mode (see "Bond Interfaces (Link Aggregation)" on page 132):</p> <ul style="list-style-type: none"> <p>■ <code>round-robin</code></p> <p>Bond uses all subordinate interfaces sequentially (High Availability + Load Sharing).</p> <p>This is the default mode.</p> <p> Note - Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation MBS-4080).</p> <p>■ <code>active-backup [primary <Name of Subordinate Interface>]</code></p> <p>Bond uses one subordinate interface at a time (High Availability)</p> <p>■ <code>xor xmit-hash-policy {layer2 layer3+4}</code></p> <p>Bond uses subordinate interfaces based on a hash function (High Availability + Load Sharing)</p> <p>■ <code>8023AD [lacp-rate {slow fast}]</code></p> <p>Dynamic bonding according to IEEE 802.3ad - LACP (Load Sharing)</p> <p>■ <code>ABXOR xmit-hash-policy ...</code></p> <p>Subordinate interfaces in the UP state are assigned to sub-groups called <i>bundles</i>.</p> <p>Only one bundle is Active at a time.</p> <p>All subordinate interfaces in the Active bundle share the traffic load.</p> <p>The system assigns traffic to all interfaces in the Active bundle based on the defined transmit hash policy.</p> <p> Note - Scalable Chassis 60000 / 40000 do not support this mode (Known Limitation MBS-1520).</p>

Parameter	Description
<pre>primary <Name of Subordinate Interface></pre>	<p>Specifies the name of the <i>primary</i> subordinate interface in the bond.</p> <p>By default, the first subordinate interface added to the bond group, becomes the primary.</p> <p> 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 R81.20 ClusterXL Administration Guide > Chapter <i>ClusterXL Requirements and Compatibility</i> > Section <i>Supported Topologies for Synchronization Network</i>.</p> <p> Note - Applies only to the Active-Backup bond mode.</p>
<pre>up-delay <0-5000></pre>	<p>Specifies the time in milliseconds to wait before enabling a subordinate interface after link recovery was detected.</p> <ul style="list-style-type: none"> ▪ Range: 0 - 5000 ms ▪ Default: 200 ms
<pre>down-delay <0-5000></pre>	<p>Specifies the time in milliseconds to wait before disabling a subordinate interface after link failure was detected.</p> <ul style="list-style-type: none"> ▪ Range: 0 - 5000 ms ▪ Default: 200 ms
<pre>lacp-rate {fast slow}</pre>	<p>Specifies the Link Aggregation Control Protocol (LACP) packet transmission rate:</p> <ul style="list-style-type: none"> ▪ <code>slow</code> - LACPDU packets are sent every 30 seconds ▪ <code>fast</code> - LACPDU packets are sent every second <p> Note - Applies only to the 802.3AD bond mode.</p>
<pre>mi-interval <1-5000></pre>	<p>Specifies the time in milliseconds to wait before checking the link on subordinate interfaces for a failure.</p> <ul style="list-style-type: none"> ▪ Range: 1 - 5000 ms ▪ Default: 100 ms

Parameter	Description
<pre>min-links <0-8></pre>	<p>Specifies the minimal number of required interface links for a bonding group in the 802.3AD mode.</p> <p>If fewer subordinate interfaces in a bonding group have their link in the "up" state, the Gaia changes the state of the bonding group to "down".</p> <ul style="list-style-type: none"> ▪ Range: 0 - 8 ▪ Default: 0 (Gaia does not count how many subordinate interfaces in a bonding group have their link in the "up" state) <p> Notes:</p> <ul style="list-style-type: none"> ▪ Applies only to the 802.3AD bond mode. ▪ In a cluster, also refer to the command "set interface <Bond Group ID> links". For more information, see the R81.20 ClusterXL Administration Guide > Chapter <i>ClusterXL Requirements and Compatibility</i> > Section <i>Configuring the Minimal Number of Required Subordinate Interfaces for Bond Load Sharing</i>.
<pre>xmit-hash-policy {layer2 layer3+4}</pre>	<p>Specifies the algorithm to use for assigning the traffic to Active subordinate interfaces:</p> <ul style="list-style-type: none"> ▪ <code>layer2</code> - Based on the XOR of hardware MAC addresses ▪ <code>layer3+4</code> - Based on the IP addresses and Ports <p> Note - Applies only to the XOR and the 802.3AD bond modes.</p>
<pre>abxor-threshold <Min number of UP subordinate interfaces></pre>	<p>Specifies the minimal number of subordinate interfaces that must be in the UP state for a bundle to be Active.</p> <p> Notes:</p> <ul style="list-style-type: none"> ▪ Applies only to the ABXOR and the 802.3AD bond modes. ▪ Scalable Chassis 60000 / 40000 do not support this mode (Known Limitation MBS-1520).

Examples

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

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

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

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

Making Sure that Bond Interface is Working

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


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

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

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

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

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

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

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

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

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

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

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

Example 3 - Output for Bond Operating Mode "XOR"

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

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

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

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

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

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

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

802.3ad info
LACP rate: slow

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

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

Configuring Bond High Availability in VRRP Cluster

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

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

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

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

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

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

Setting the value of the kernel parameter temporarily

Important - This change does not survive reboot.

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

Setting the value of the kernel parameter permanently

Step	Instructions
1	Connect to the command line on <i>each</i> Cluster Member.
2	Log in to the Expert mode.
3	Back up the current <code>\$FWDIR/boot/modules/fwkernel.conf</code> file: <pre>cp -v \$FWDIR/boot/modules/fwkernel.conf{, _BKP}</pre>
4	Edit the current <code>\$FWDIR/boot/modules/fwkernel.conf</code> file: <pre>vi \$FWDIR/boot/modules/fwkernel.conf</pre>
5	Add this line to the file (spaces and comments are not allowed): <pre>fwkernel_enhanced_enable=1</pre>
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 <code>fwkernel_enhanced_enable</code> was set to 1: <pre>fw ctl get int fwkernel_enhanced_enable</pre>

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

MAGG Interfaces

In This Section:

Configuring MAGG Interfaces in Gaia Portal	154
Configuring MAGG Interfaces in Gaia Clish	157

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

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

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



Notes:





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

Configuring MAGG Interfaces in Gaia Portal



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

Adding a MAGG interface

Step	Instructions
1	In the navigation tree, click Interface Management > Network Interfaces .
2	Click Add > Magg .
3	In the Comment field, enter the applicable comment text (up to 100 characters).
4	<p>On the IPv4 tab, do one of these:</p> <ul style="list-style-type: none"> ▪ Select Obtain IPv4 address automatically to get the IPv4 address from the DHCPv4 server. <ul style="list-style-type: none">  Important - Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation MBS-3246). ▪ Enter the IPv4 address and subnet mask in the applicable fields.
5	<p>Optional: On the IPv6 tab, do one of these:</p> <ul style="list-style-type: none"> ▪ Select Obtain IPv6 address automatically to get the IPv6 address from the DHCPv6 server. <ul style="list-style-type: none">  Important - Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation MBS-3246). ▪ Enter the IPv6 address and mask length in the applicable fields. <p> Important:</p> <ul style="list-style-type: none"> ▪ First, you must enable the IPv6 Support and reboot (see "System Configuration" on page 370). ▪ R81.20 does not support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313).
6	<p>On the Magg tab:</p> <ol style="list-style-type: none"> a. Select or enter a Bond Group ID. This parameter is an integer between 0 and 1024. b. Select the subordinate interface eth<X>-Mgmt<Y> interfaces from the Available Interfaces list and then click Add. <ul style="list-style-type: none">  Note - Make sure that the subordinate interfaces do not have any IP addresses or aliases configured.

Step	Instructions
7	<p>On the Advanced tab:</p> <ol style="list-style-type: none"> 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. 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. 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. 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).
8	Click OK .

Configuring a MAGG interface

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

Deleting a MAGG interface

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

Configuring MAGG Interfaces in Gaia Clish

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

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

Syntax

Adding a new management Bonding Group

Syntax

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

Example

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

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

Adding a new subordinate interface to an existing management Bonding Group

Syntax

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

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

Example

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

i Notes:

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

Configuring an existing management Bonding Group

Syntax

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

Configuring the Bond Operating Mode

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

Syntax

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

Example

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

Notes:

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

Configuring the Up Delay Time


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

Syntax

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

Example

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

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

Configuring the Down Delay Time


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

Syntax

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

Example

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

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

Configuring the Media Monitoring Interval


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

Syntax

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

Example

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

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


Deleting a subordinate interface from an existing Bonding Group

Syntax

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

Example

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

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

Deleting the bonding group

Syntax

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

Example

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

Notes:

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

Viewing the Bonding Group configuration


Syntax


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

Parameters

CLI Parameters

Parameter	Description
<Bond Group ID>	Configures the Bond Group ID. <ul style="list-style-type: none"> ▪ Range: 0 - 1024 ▪ Default: No default value

Parameter	Description
<code><Name of Subordinate Interface></code>	<p>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.</p>
<code>mode <Mode></code>	<p>Configures the Bond operating mode (see "Bond Interfaces (Link Aggregation)" on page 132). The MAGG interface only support the Active/Backup or the XOR mode:</p> <ul style="list-style-type: none"> ▪ <code>active-backup [primary <Name of Subordinate Interface>]</code> Bond uses one subordinate interface at a time (High Availability) ▪ <code>xor xmit-hash-policy {layer2 layer3+4}</code> Bond uses subordinate interfaces based on a hash function (High Availability + Load Sharing)
<code>primary <Name of Subordinate Interface></code>	<p>Specifies the name of the <i>primary</i> subordinate interface in the bond. By default, the first subordinate interface added to the bond group, becomes the primary.</p> <p> Note - Applies only to the Active-Backup bond mode.</p>
<code>up-delay <0-5000></code>	<p>Specifies the time in milliseconds to wait before enabling a subordinate interface after link recovery was detected.</p> <ul style="list-style-type: none"> ▪ Range: 0 - 5000 ms ▪ Default: 200 ms
<code>down-delay <0-5000></code>	<p>Specifies the time in milliseconds to wait before disabling a subordinate interface after link failure was detected.</p> <ul style="list-style-type: none"> ▪ Range: 0 - 5000 ms ▪ Default: 200 ms
<code>mii-interval <1-5000></code>	<p>Specifies the time in milliseconds to wait before checking the link on subordinate interfaces for a failure.</p> <ul style="list-style-type: none"> ▪ Range: 1 - 5000 ms ▪ Default: 100 ms

Parameter	Description
xmit-hash-policy {layer2 layer3+4}	<p>Specifies the algorithm to use for assigning the traffic to Active subordinate interfaces:</p> <ul style="list-style-type: none"> layer2 - Based on the XOR of hardware MAC addresses layer3+4 - Based on the IP addresses and Ports <p> Note - Applies only to the XOR bond mode.</p>

Examples

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

```

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

```


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

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

Bridge Interfaces

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

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

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


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

Notes:

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



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

Configuring Bridge Interfaces in Gaia Portal

 **Note** - For additional information:

- For Security Gateways or ClusterXL - see the [R81.20 Installation and Upgrade Guide](#) > Chapter *Special Scenarios for Security Gateways* > Section *Deploying a Security Gateway or a ClusterXL in Bridge Mode*.
- For Security Groups on Quantum Maestro - see the [R81.20 Quantum Maestro Administration Guide](#) > Chapter *Deploying a Security Group in Bridge Mode*.
- For Security Groups on Scalable Chassis - see the [R81.20 Quantum Scalable Chassis Administration Guide](#) > Chapter *Deploying a Security Group in Bridge Mode*.

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

Step	Instructions
1	In the left navigation tree, click Network Management > Network Interfaces .
2	Make sure that the subordinate interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned.
3	Click Add > Bridge . 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: <ul style="list-style-type: none"> ▪ 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 370).
8	Click OK .

**Notes:**


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

Configuring Bridge Interfaces in Gaia Clish

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





Notes:


- You configure an IP address on a Bridging Group in the same way as you do on a physical interface (see ["Physical Interfaces" on page 102](#)).
- The name of a Bridge interface in Gaia is "br<Bridge Group ID>".
For example, the name of a bridge interface with a Bridge Group ID of 5 is "br5".
- To configure MTU on a Bridge subordinate interface, you must configure MTU on the Bridge interface.
This MTU applies to all subordinate interfaces assigned to this Bridge interface.
- For additional information:
 - For Security Gateways or ClusterXL - see the [R81.20 Installation and Upgrade Guide](#) > Chapter *Special Scenarios for Security Gateways* > Section *Deploying a Security Gateway or a ClusterXL in Bridge Mode*.
 - For Security Groups on Quantum Maestro - see the [R81.20 Quantum Maestro Administration Guide](#) > Chapter *Deploying a Security Group in Bridge Mode*.
 - For Security Groups on Scalable Chassis - see the [R81.20 Quantum Scalable Chassis Administration Guide](#) > Chapter *Deploying a Security Group in Bridge Mode*.

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

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway, Cluster Member, or Security Group.
2	Log in to Gaia Clish.
3	<p>Make sure that the subordinate interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned:</p> <pre style="border: 1px solid black; padding: 10px;"> show interface <Name of Subordinate Interface> ipv4- address show interface <Name of Subordinate Interface> ipv6- address </pre>

Step	Instructions
4	<p>Add a new bridging group:</p> <pre data-bbox="316 264 1458 331">add bridging group <Bridge Group ID 0 - 1024></pre> <p> 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.</p>
5	<p>Add subordinate interfaces to the new bridging group:</p> <pre data-bbox="316 539 1458 719">add bridging group <Bridge Group ID> interface <Name of First Subordinate Interface> add bridging group <Bridge Group ID> interface <Name of Second Subordinate Interface></pre> <p> Notes:</p> <ul data-bbox="416 790 1445 987" style="list-style-type: none"> ▪ 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.
6	<p>Assign an IP address to the bridging group.</p> <p> 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 102).</p> <ul data-bbox="355 1182 839 1227" style="list-style-type: none"> ▪ To assign an IPv4 address, run: <pre data-bbox="395 1227 1458 1368">set interface <Name of Bridging Group> ipv4-address <IPv4 Address> {subnet-mask <Mask> mask-length <Mask Length>}</pre> <p>You can optionally configure the bridging group to obtain an IPv4 Address automatically.</p> <ul data-bbox="355 1458 839 1503" style="list-style-type: none"> ▪ To assign an IPv6 address, run: <pre data-bbox="395 1503 1458 1603">set interface <Name of Bridging Group> ipv6-address <IPv6 Address> mask-length <Mask Length></pre> <p>You can optionally configure the bridging group to obtain an IPv6 Address automatically.</p> <p> Important - First, you must enable the IPv6 Support and reboot (see "System Configuration" on page 370).</p>
7	<p>Save the configuration:</p> <pre data-bbox="316 1854 1458 1921">save config</pre>


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

Syntax

Adding a new bridging group

Syntax

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

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


Adding a new subordinate interface to an existing bridging group

Syntax

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

Example

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

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

Adding a fail-open interface to an existing bridging group

Syntax

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

Configuring an existing Bridging Group

Syntax

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

Example

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

Deleting a subordinate interface from an existing bridging group

Syntax

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

Example

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

Deleting a fail-open interface from the bridging group

Syntax

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

Deleting the bridging group

Syntax

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

Notes:

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

Example

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

Viewing the subordinate interfaces of an existing bridging group

Syntax

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

Viewing the configured bridging groups



Syntax

```
show bridging groups
```

Parameters

CLI Parameters

Parameter	Description
<i><Bridge Group ID></i>	Configures the Bridge Group ID. <ul style="list-style-type: none"> ▪ Range: 0 - 1024 ▪ Default: No default value
<i><Name of Bridge Interface></i>	Configures the name of the Bridge interface.

Parameter	Description
<code><Name of Subordinate Interface></code>	Specifies a physical subordinate interface.
<code>comments "Text"</code>	Configures an optional free text comment. <ul style="list-style-type: none"> 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.
<code>ipv4-address <IPv4 Address></code>	Configures the IPv4 address.
<code>ipv6-address <IPv6 Address></code>	Configures the IPv6 address. <p> Important - First, you must enable the IPv6 Support and reboot (see "System Configuration" on page 370).</p>
<code>subnet-mask <Mask></code>	Configures the IPv4 subnet mask using dotted decimal notation (X.X.X.X).
<code>mask-length <Mask Length></code>	Configures the IPv4 or IPv6 subnet mask length using the CIDR notation (integer between 2 and 32).
<code>ipv6-autoconfig {on off}</code>	Configures if this interface gets an IPv6 address from a DHCPv6 Server: <ul style="list-style-type: none"> <code>on</code> - Gets an IPv6 address from a DHCPv6 Server <code>off</code> - Does not get an IPv6 address from a DHCPv6 Server (you must assign it manually) <p> Important - First, you must enable the IPv6 Support and reboot (see "System Configuration" on page 370).</p>
<code>mac-addr <MAC Address></code>	Configures the hardware MAC address.

Parameter	Description
mtu <68-16000 1280-16000>	<p>Configures the Maximum Transmission Unit size for an interface.</p> <p>For IPv4:</p> <ul style="list-style-type: none"> ▪ Range: 68 - 16000 bytes ▪ Default: 1500 bytes <p>For IPv6:</p> <ul style="list-style-type: none"> ▪ Range: 1280 - 16000 bytes ▪ Default: 1500 bytes
rx-ringsize <0-4096>	<p>Configures the receive buffer size.</p> <ul style="list-style-type: none"> ▪ Range: 0 - 4096 bytes ▪ Default: Depends on the interface driver
tx-ringsize <0-4096>	<p>Configures the transmit buffer size.</p> <ul style="list-style-type: none"> ▪ Range: 0 - 4096 bytes ▪ Default: Depends on the interface driver

Example

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

Accept, or Drop Ethernet Frames with Specific Protocols

Important:

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

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

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

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

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

Step	Instructions
1	Connect to the command line on the Security Gateway, each Cluster Member, or Scalable Platform Security Group.
2	Log in to the Expert mode.
3	Backup the current <code>/etc/rc.d/init.d/network</code> file: <ul style="list-style-type: none"> ▪ On the Security Gateway / each Cluster Member: <pre>cp -v /etc/rc.d/init.d/network{,_BKP}</pre> ▪ On the Scalable Platform Security Group: <pre>g_cp -v /etc/rc.d/init.d/network{,_BKP}</pre>
4	Edit the current <code>/etc/rc.d/init.d/network</code> file: <pre>vi /etc/rc.d/init.d/network</pre>
5	After the line: <pre>./etc/init.d/functions</pre> Add this line: <pre>/sbin/sysctl -w net.bridge.bpdu_forwarding=0</pre>
6	Save the changes in the file and exit the Vi editor.

Step	Instructions
7	<p>On the Scalable Platform Security Group: Copy the modified file to other Security Group Members:</p> <pre data-bbox="316 309 1461 371">asg_cp2blades -b all /etc/rc.d/init.d/network</pre>
8	<p>Reboot.</p> <ul style="list-style-type: none"><li data-bbox="357 474 1461 577">▪ On the Security Gateway / each Cluster Member:<pre data-bbox="395 515 1461 577">reboot</pre><li data-bbox="357 586 1461 689">▪ On the Scalable Platform Security Group:<pre data-bbox="395 627 1461 689">g_reboot -a</pre>
9	<p>Make sure the new configuration is loaded:</p> <ul style="list-style-type: none"><li data-bbox="357 792 1461 896">▪ On the Security Gateway / each Cluster Member:<pre data-bbox="395 833 1461 896">sysctl net.bridge.bpdu_forwarding</pre><li data-bbox="357 904 1461 1008">▪ On the Scalable Platform Security Group:<pre data-bbox="395 945 1461 1008">g_all sysctl net.bridge.bpdu_forwarding</pre> <p>The output must show:</p> <pre data-bbox="316 1079 1461 1142">net.bridge.bpdu_forwarding = 0</pre>

Loopback Interfaces

In This Section:


Configuring Loopback Interfaces in Gaia Portal	177
Configuring Loopback Interfaces in Gaia Clish	180

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


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


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

Configuring Loopback Interfaces in Gaia Portal

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

Adding a loopback interface

Step	Instructions
1	In the navigation tree, click Interface Management > Network Interfaces .
2	Click Add > Loopback .
3	In the Add loopback window: <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> ▪ 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 370).
4	Click OK .

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

Configuring a loopback interface

Step	Instructions
1	In the navigation tree, click Interface Management > Network Interfaces .
2	Select a loopback interface and click Edit .
3	In the Edit loop<NN> window: <ol style="list-style-type: none"> a. If required, change the IPv4 address and subnet mask. b. If required, change the IPv6 address and mask length.
4	Click OK .

Deleting a loopback interface

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

Configuring Loopback Interfaces in Gaia Clish

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

Syntax

Adding a loopback interface

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

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

Configuring a loopback interface

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

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

Viewing a loopback interface

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

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

Deleting a loopback interface

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

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

Parameters

CLI Parameters

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

Parameter	Description
<i><IPv4 Address></i>	Specifies the IPv4 address These IPv4 addresses are not allowed: <ul style="list-style-type: none">▪ 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
<i><Mask Length></i>	Configures the IPv4 subnet mask length using the CIDR notation (integer between 2 and 32)
<i><Name of Loopback Interface></i>	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 [R81.20 Site to Site VPN Administration Guide](#) > Chapter *Route Based VPN*.

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

Procedure:

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

Configuring VPN community

You must configure the VPN Community and add the member Security Gateways to it before you configure a VPN Tunnel Interface. This section includes the basic procedure for defining a Site-to-Site VPN Community. To learn more about VPN communities and their definition procedures, see the [R81.20 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: <ol style="list-style-type: none"> Enter the VPN community name. From the left tree, click Gateways. Select the applicable Security Gateways. 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. Configure other settings as necessary.
6	Publish the SmartConsole session.

4. Make Route Based VPN the default option.

Do this procedure one time for each.

Configuring Route Based VPN

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

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

Configuring an empty group

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

Configuring the Route Based VPN as the default choice


Do these steps for each Security Gateway.

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

5. Configure the VTI.

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


Configuring VTI in Gaia Portal

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

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

Step	Instructions
3	<p>In the Add/Edit window, configure these parameters:</p> <ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> • 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

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

Syntax

- To add a VPN Tunnel Interface (VTI):

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

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

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

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

```
show vpn tunnels
```

- To delete a VPN Tunnel Interface (VTI):

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

i 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.
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 .

Step	Instructions
4	For each VPN member gateway: <ol style="list-style-type: none"> Double-click the Security Gateway object. From the left tree, click Network Management. Click Get Interfaces > Get Interfaces with Topology. This updates the topology to include the newly configured VTIs. Click Accept. 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 [R81.20 Gaia Advanced Routing Administration Guide](#).

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

Step	Instructions												
2	<p>In SmartConsole, add an Access Control rule that allows traffic to the VPN community (or all communities) that uses the OSPF service:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Source</th> <th>Destination</th> <th>VPN</th> <th>Service</th> <th>Action</th> </tr> </thead> <tbody> <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> </tbody> </table>	Name	Source	Destination	VPN	Service	Action	Allow OSPF for a VPN Community	Any	Any	MyIntranet	ospf	Accept
Name	Source	Destination	VPN	Service	Action								
Allow OSPF for a VPN Community	Any	Any	MyIntranet	ospf	Accept								

7. Install the policy and test.

Instructions


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

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

6in4 Tunnel Interfaces

In This Section:

Configuring 6in4 Tunnel Interfaces in Gaia Portal	192
Configuring 6in4 Tunnel Interfaces in Gaia Clish	194


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


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

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

To do this, 6in4 does these functions:

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

-  **Important** - Before you can configure 6in4 Tunnel interfaces, you must enable the IPv6 Support and reboot (see "[System Configuration](#)" on page 370).

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


Configuring 6in4 Tunnel Interfaces in Gaia Portal

Adding a 6in4 Tunnel interface

Step	Instructions
1	In the navigation tree, click Network Management > Network Interfaces .
2	Make sure that the physical interface, on which you add a 6in4 Tunnel interface, has an IPv4 address.
3	Click Add > 6in4 Tunnel .
4	In the Add 6in4 Tunnel window, select the Enable option to set the VLAN interface to UP.
5	Optional: On the IPv6 tab, enter the IPv6 address and mask length. You can optionally select the Obtain IPv6 address automatically option.
6	On the 6in4 Tunnel tab: <ul style="list-style-type: none"> ▪ In the Interface field, select the applicable physical interface. ▪ In the Tunnel ID field, enter or select the Tunnel ID between 2 and 999999. Note - The ID must be unique for every 6in4 tunnel that terminates on this Gaia. ▪ In the TTL field, enter or select the Time-to-Live for the 6in4 packets between 0 and 255. Note - This value must be the same on the peers. Default value is 0. ▪ In the Remote Address field, enter the IPv4 address at the remote end of the 6in4 tunnel.
7	Click OK .

Editing a VLAN interface

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

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

Deleting a 6in4 Tunnel interface

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

Configuring 6in4 Tunnel Interfaces in Gaia Clish

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

Syntax

Adding a new 6in4 Tunnel interface

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

Configuring a 6in4 Tunnel interface

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

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

Viewing the configuration of a specific 6in4 Tunnel interface

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

Deleting a 6in4 Tunnel interface

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

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

Parameters

CLI Parameters

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

Parameter	Description
<code><IPv4 Address on Remote Peer></code>	Specifies the IPv4 address at the remote end of the 6in4 tunnel.
<code>ttl <0-255></code>	Specifies the Time-to-Live for the 6in4 packets between 2 and 255. Note - This value must be the same on the peers. Default value is 0.
<code>comments "Text"</code>	Defines the optional comment. <ul style="list-style-type: none"> 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.
<code><IPv6 Address></code>	Assigns the IPv6 address.
<code>mask-length <Mask Length></code>	Configures the IPv6 subnet mask length using CIDR notation (/xx) - integer between 1 and 128.
<code>ipv6-autoconfig {on off}</code>	Configures if this interface gets an IPv6 address from a DHCPv6 Server: <ul style="list-style-type: none"> <code>on</code> - Gets an IPv6 address from a DHCPv6 Server <code>off</code> - Does not get an IPv6 address from a DHCPv6 Server (you must assign it manually)
<code>mtu <1280-16000></code>	Configures the Maximum Transmission Unit size for an interface. <ul style="list-style-type: none"> Range: 1280 - 16000 bytes Default: 1500 bytes
<code>state {on off}</code>	Configures interface's state: <ul style="list-style-type: none"> <code>on</code> - Enabled <code>off</code> - Disabled

Example

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

PPPoE Interfaces

In This Section:

Configuring PPPoE Interfaces in Gaia Portal	197
Configuring PPPoE Interfaces in Gaia Clish	199

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

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

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





Notes:

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

Configuring PPPoE Interfaces in Gaia Portal


Adding a PPPoE interface

Step	Instructions
1	In the navigation tree, click Network Management > Network Interfaces .
2	Make sure that the physical interface, on which you add a PPPoE interface, does not have an IP address.
3	Click Add > PPPoE .
4	In the Add PPPoE window, select the Enable option to set the PPPoE interface to UP.
5	On the PPPoE tab: <ul style="list-style-type: none"> ▪ In the PPPoE ID field, enter or select the ID between 0 and 999. Note - This ID must be unique for every PPPoE interface. ▪ In the Interface field, select the applicable physical interface. Gaia uses this interface to forward PPPoE frames. ▪ In the User Name field, enter the username needed to connect to the PPPoE server at the Internet Service Provider (ISP). Get it from the ISP. ▪ In the Password field, enter the password needed to connect to the PPPoE server at the Internet Service Provider (ISP). Get it from the ISP. ▪ Optional: Select Use Peer DNS to allow the ISP to define the IPv4 DNS server for the Gaia. The ISP supplies either one IPv4 DNS server (the Primary) or two (Primary and Secondary).  Important - If you select this option, the PPPoE Peer DNS servers overwrite the IPv4 DNS servers configured in Network Management > Hosts and DNS. ▪ Optional: Select Use Peer as Default Gateway to make the ISP server the Default Gateway for the Gaia.  Important - If you select this option, Gaia does not use anymore the Default Gateway configured in Network Management > IPv4 Static Routes.
9	Click OK .

Editing a PPPoE interface

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

Step	Instructions
3	Configure the applicable settings.
4	Click OK .

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

Deleting a PPPoE interface

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

Configuring PPPoE Interfaces in Gaia Clish

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

Syntax

Adding a new VLAN interface

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

Configuring a VLAN interface

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

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

Viewing the PPPoE configuration

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



Deleting a VLAN interface

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

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

Parameters

CLI Parameters

Parameter	Description
<code>id <PPPoE ID></code>	Specifies the ID between 0 and 999. Note - This ID must be unique for every PPPoE interface.
<code>interface <Name of Physical Interface></code>	Specifies a local physical interface. Gaia uses this interface to forward PPPoE frames.
<code>user-name <PPPoE Username></code>	Specifies the username needed to connect to the PPPoE server at the Internet Service Provider (ISP). Get it from the ISP.
<code>password <PPPoE Password></code>	Specifies the password needed to connect to the PPPoE server at the Internet Service Provider (ISP). Get it from the ISP.
<code>password_hash <PPPoE Password Hash></code>	Specifies the hash of the password needed to connect to the PPPoE server at the Internet Service Provider (ISP). Get it from the ISP.
<code>use-peer-dns {on off}</code>	Optional: Specifies whether to allow the ISP to define the IPv4 DNS server for the Gaia. The ISP supplies either one IPv4 DNS server (the Primary) or two (Primary and Secondary). <ul style="list-style-type: none"> ▪ on - Allow ▪ off - Do not allow  Important - If you enable this option, the PPPoE Peer DNS servers overwrite the IPv4 DNS servers configured with the "set dns" command.
<code>use-peer-as- default- gateway {on off}</code>	Optional: Specifies whether to make the ISP server the Default Gateway for the Gaia <ul style="list-style-type: none"> ▪ on - Allow ▪ off - Do not allow  Important - If you enable this option, Gaia does not use anymore the Default Gateway configured with the "set static-route default" command.

Parameter	Description
<code>fake-peer-address <IPv4 Address></code>	Optional. Configures the fake unicast peer IPv4 address (the default value is 0.0.0.0).
<code>use-fake-peer-address {on off}</code>	Optional. Configures whether to use the configured fake peer IPv4 address: <ul style="list-style-type: none"> ▪ on - Enabled ▪ off - Disabled


Example

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

GRE Interfaces

In This Section:

Configuring GRE Interfaces in Gaia Portal	203
Configuring GRE interfaces in Gaia Clish	205
Configuring GRE Interfaces on Cluster Members	208

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

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

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

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

Notes:

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

For additional information, see [sk169794](#).

Configuring GRE Interfaces in Gaia Portal

Adding a GRE interface

Step	Instructions
1	In the navigation tree, click Network Management > Network Interfaces .
2	Click Add > GRE .
3	On the IPv4 tab, enter the local IPv4 address and subnet mask for the GRE interface.
4	<p>On the GRE Tunnel tab:</p> <ol style="list-style-type: none"> In the GRE Interface ID field, enter or select the GRE Tunnel ID between 1 and 1024. In the Peer Address field, enter the IPv4 address for the GRE interface on the remote GRE peer. In the Local Address field, enter the IPv4 address of the applicable local physical interface. In the Remote Address field, enter the IPv4 address of the applicable physical interface on the remote GRE peer. In the TTL field, enter or select the Time-to-Live for the GRE packets between 0 and 255. Note - This value must be the same on the GRE peers.
5	Click OK .

Example


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

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

The GRE interface configuration on these GRE peers:

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

Editing a GRE interface

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

Deleting a GRE interface

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

Configuring GRE interfaces in Gaia Clish

Syntax

Adding a GRE interface


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

Viewing the configured GRE interface

```
show configuration gre
```


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

Editing a GRE interface

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

Deleting a GRE interface

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

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

CLI Parameters

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

Example

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

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

The GRE interface configuration on these GRE peers:

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

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

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

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

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

Configuring GRE Interfaces on Cluster Members

For more information, see the [R81.20 ClusterXL Administration Guide](#).

In Cluster, you have these options:

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

1. Configure a GRE interface on all the Cluster Members.
You must configure the *same* **GRE Interface ID** and **Remote Address** on each Cluster Member.
2. Connect with SmartConsole to the Management Server.
3. From the left navigation panel, click **Gateways & Servers**.
4. Double-click the cluster object.
5. From the left tree, click **Network Management**.
6. From the toolbar, click **Get Interfaces > Get Interfaces With Topology** and confirm.
Make sure you see the new GRE interface from each Cluster Member.
7. Select the new GRE interface and click **Edit**.
8. From the left tree, click the **General** page.
9. In the **General** section, in the **Network Type** field, select **Cluster**.
10. In the **IPv4** field, configure the applicable cluster Virtual IP address.
11. In the **Member IPs** section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.
12. Click **OK**.
13. Publish the SmartConsole session.
14. Install the Access Control Policy on this cluster object.

Using a GRE interface only on a specific Cluster Member

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


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

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


Gaia Management Interface

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

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

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

Selecting Management Interface in Gaia Portal

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

Procedure

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

Selecting Management Interface in Gaia Clish

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

Syntax

Viewing the current interface

```
show management interface
```

Selecting a new interface

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

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

Parameters

CLI Parameters

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

Example

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

Detection of IP Address Conflicts

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

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

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

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

Configuration in Gaia Clish

 **Important:**

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

Syntax

Viewing the current configuration


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

Configuring settings

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


Removing the current configuration

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

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

Parameters

CLI Parameters

Command	Description
<pre>set ip-conflicts-monitor interface {all <Name of Interface>}</pre>	<p>Specifies the interfaces, on which Gaia monitors for :</p> <ul style="list-style-type: none"> ■ all Detect IP address conflicts (duplicate IP addresses) on all supported interfaces ■ <Name of Interface> Detect IP address conflicts on the specified interface only You can run this command for each applicable interface <p> Best Practice - Enable this feature only for interfaces connected to your internal networks. If you enable this feature for all interfaces, or for interfaces connected to external networks, this feature generates too many log messages in the <code>/var/log/messages</code> file.</p>
<pre>set ip-conflicts-monitor state {off on}</pre>	<p>Enables (on) and disables (off) the feature.</p>
<pre>show ip-conflicts-monitor interfaces</pre>	<p>Shows the interfaces, on which Gaia detects IP address conflicts.</p>
<pre>show ip-conflicts-monitor state</pre>	<p>Shows the current state of the feature (off or on).</p>
<pre>delete ip-conflicts-monitor interfaces {all <Name of Interface>}</pre>	<p>Specifies the interfaces, on which Gaia stops to detect IP address conflicts:</p> <ul style="list-style-type: none"> ■ all Stop to detect IP address conflicts on all supported interfaces ■ <Name of Interface> Stop to detect IP address conflicts on the specified interfaces only

Example

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

Log Messages

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

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

To see the applicable log messages:

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

Example:

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

Additional Information

- The detection of IP address conflicts is based on the Linux [arpwatch](#) tool.
- When you enable this feature, Gaia runs the `/bin/arpwatch_launcher` daemon. This daemon is responsible to run the `/etc/rc.d/init.d/arpwatch` service.
- Gaia saves the applicable configuration in the Gaia database and in the `/etc/sysconfig/arpwatch` file.
Gaia generates the `/etc/sysconfig/arpwatch` file automatically.
- Gaia saves the MAC-to-IP address binding information in the `/var/lib/arpwatch/arp.dat.<Name of Interface>` file.

The information includes:

- The detected MAC address
- The IP address assigned to that MAC address
- The time of detection (in Unix epoch format)

It can take several minutes for Gaia to populate this database.

Interface Link Status

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

Important:

- On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.
- On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

To see interface status in Gaia Portal:

1. In the navigation tree, click **Network Management > Network Interfaces**.
2. Double-click an interface to see its parameters.

Link Status	Description
Down (gray)	The physical interface is disabled (down).
No link (red)	The physical interface is enabled (up), but Gaia cannot find a network connection.
Up (green)	The physical interface is enabled (up) and connected to the network.

To see interface status in Gaia Clish:


Run one of these commands:

```
show interfaces all
```

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

CLI Reference (interface)

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

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

 **Important:**

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

Description

Add, configure, and delete interfaces and interface properties.

Syntax

Adding an interface

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

Configuring an interface

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

Viewing an interface configuration

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

```
show interfaces all
```

Deleting an interface, or interface configuration

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

Working with Gaia Management Interface

```
show management interface
```

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

Working with Gaia IP Conflict Detection

```
show ip-collisions-monitor
```

```
set ip-collisions-monitor
```

```
delete ip-collisions-monitor
```


ARP

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

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

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

Configuring ARP in Gaia Portal

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


Viewing dynamic ARP entries

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

Viewing static ARP entries

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

Changing static and dynamic ARP parameters

Step	Instructions
1	In the navigation tree, click Network Management > ARP .
2	In the upper right corner, click the Configuration tab.
3	<p>In the ARP Table Settings section:</p> <ol style="list-style-type: none"> Enter the Maximum Entries. This is the maximal number of entries in the ARP cache. Range: 1024 - 131072 entries Default: 4096 entries <p> 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.</p> <ol style="list-style-type: none"> 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

Adding a static ARP entry

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

Deleting a static ARP entry

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

Deleting all dynamic ARP entries

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

Configuring ARP in Gaia Clish

- i** **Important** - On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- i** **Note** - For Scalable Platforms (Maestro and Chassis), also refer to the "asg_arp" command in Gaia gClish.
See the [R81.20 Quantum Maestro Administration Guide](#).
See the [R81.20 Quantum Scalable Chassis Administration Guide](#).

Syntax

Adding a static ARP entry

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

Deleting static and dynamic ARP entries

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

Configuring ARP table parameters

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

Viewing ARP table parameters


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

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

Parameters

CLI Parameters

Parameter	Description
static	Configures static ARP entries.
dynamic	Configures dynamic ARP entries.

Parameter	Description
<pre>ipv4-address <IPv4 Address></pre>	<p>Configures IPv4 Address for a static ARP entry.</p> <ul style="list-style-type: none"> ▪ Range: Dotted-quad ([0-255].[0-255].[0-255].[0-255]) ▪ Default: No default value
<pre>macaddress</pre>	<p>Configures the hardware MAC address (six hexadecimal octets separated by colons) for a static ARP entry.</p> <ul style="list-style-type: none"> ▪ Range: 00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF ▪ Default: No default value
<pre>table validity- timeout <Seconds></pre>	<p>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.</p> <ul style="list-style-type: none"> ▪ Range: 60 - 86400 seconds (24 hours) ▪ Default: 60 seconds
<pre>table cache-size <Number of Entries></pre>	<p>Configures the maximal number of entries in the ARP cache table.</p> <ul style="list-style-type: none"> ▪ Range: 1024 - 131072 ▪ Default: 4096 <p> 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.</p>

DHCP Server

i Important - Scalable Platforms (Maestro and Chassis) do **not** support this feature (Known Limitation MBS-3246).

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

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

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

You configure DHCP server subnets on the Gaia device interfaces.

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

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

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

Workflow


Step	Instructions
1	To define a DHCP subnet on a Gaia interface: <ol style="list-style-type: none"> 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

Important:

- Scalable Platforms (Maestro and Chassis) do **not** support this feature (Known Limitation MBS-3246).
- Starting in R81.20, you can configure DHCP Server setting in the context of a VSX Virtual System. See "[Configuring a DHCP Server in Gaia Clish](#)" on [page 228](#).

Allocating DHCP parameters to hosts

Step	Instructions
1	In the navigation tree, click Network Management > DHCP Server .
2	In the DHCP Server Subnet Configuration section, click Add . 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. <ol style="list-style-type: none"> 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 or 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.

Step	Instructions
	<p>Optional: In the Lease Configuration section, configure the DHCP lease settings:</p> <ol style="list-style-type: none"> 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.
5	<p>Optional: On the Routing & DNS tab, define routing and DNS parameters for DHCP clients:</p> <ul style="list-style-type: none"> ▪ 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, <code>example.com</code>). ▪ 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.

Changing the DHCP parameters in a subnet


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

Disabling DHCP server on all interfaces

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

Deleting DHCP subnet

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

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

Configuring a DHCP Server in Gaia Clish

Important:

- Scalable Platforms (Maestro and Chassis) do **not** support this feature (Known Limitation MBS-3246).
- On a VSX Gateway / each VSX Cluster Member, you must run these commands in the context of the applicable Virtual System (`set virtual-system <VS ID>`).

Syntax

Adding 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>
```

Configuring 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>
```

Deleting 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>
```

Enabling or disabling the DHCP Server process

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

Viewing the DHCP Server configuration

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

i 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).

Parameter	Description
disable	Disables the DHCP Server subnet, or the DHCP Server process (depending on the context).
default-lease <Lease in Seconds>	Specifies the default DHCP lease in seconds, for host IPv4 addresses. Applies only if DHCP clients do not request a unique lease time. If you do not enter a value, the default is 43,200 seconds.
max-lease <Maximal Lease in Seconds>	Specifies the maximal DHCP lease in seconds, for host IPv4 addresses. This is the longest lease available. If you do not enter a value, the configuration default is 86,400 seconds.
default-gateway <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: <code>example.com</code>
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: <code>192.0.2.101, 192.0.2.102, 192.0.2.103</code>
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 235](#))
- Hosts (see ["Hosts" on page 237](#))
- DNS settings (see ["DNS" on page 241](#))

System Name

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

Configuring Host Name and Domain Name in Gaia Portal

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

Step	Instructions
1	In the navigation tree, click Network Management > Host and DNS .
2	In the System Name section: <ol style="list-style-type: none"> In the Host Name field, enter the network name of the Gaia device. Optional: In the Domain Name field, enter the domain. For example, <code>example.com</code>. Click Apply.

Configuring Host Name and Domain Name in Gaia Clish

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

Description

Configure the host name of your platform.

Syntax

- To configure a hostname:

```
set hostname <Name of Host>
```

- To show the configured hostname:


```
show hostname
```

- To configure a domain name (optional):

```
set domainname <Domain>
```

- To show the configured domain name:

```
show domainname
```

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


Hosts

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

You can:

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

Configuring Hosts in Gaia Portal

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

Adding a static host entry

Step	Instructions
1	In the navigation tree, click Network Management > Hosts and DNS .
2	In the Hosts section, click Add .
3	Enter: <ul style="list-style-type: none"> ▪ 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

Editing the static host entry

Step	Instructions
1	In the navigation tree, click Network Management > Hosts and DNS .
2	In the Hosts section, select a host entry and click Edit .
3	Edit: <ul style="list-style-type: none"> ▪ Host Name ▪ IPv4 address ▪ IPv6 address

Deleting the static host entry

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

Configuring Hosts in Gaia Clish

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

Description

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

Syntax

Adding a static host entry

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

Editing the static host entry

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

Deleting the static host entry

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

Viewing the configured static host entry

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

Viewing all configured IP addresses of all hosts

```
show host names [ipv4 | ipv6]
```

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

Parameters

CLI Parameters

Parameter	Description
<code>name <Name of Host></code>	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.
<code>ipv4-address <IPv4 Address of Host></code>	The IPv4 address of the host.
<code>ipv6-address <IPv6 Address of Host></code>	The IPv6 address of the host.


DNS

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


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

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

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


 **Note** - From R81, you can configure specific DNS settings in each Virtual System. See the [R81.20 VSX Administration Guide](#).

Configuring DNS in Gaia Portal

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

Configuring the DNS Servers

Step	Instructions
1	In the navigation tree, click Network Management > Hosts and DNS .
2	In the System Name section: In the Domain Name field, enter the domain name (for example, <code>example.com</code>).

Step	Instructions
3	<p>In the DNS section:</p> <ol style="list-style-type: none">In the DNS Suffix field, enter the domain name suffix. 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 1223). <p> Note - Domain names that are also valid numeric IP addresses (for example: 10.19.76.100), although syntactically correct, are not permitted.</p> <p>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".</p> <ol style="list-style-type: none">In the Primary DNS Server field, enter the IPv4 or IPv6 address of the Primary DNS server.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).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).Click Apply.

Configuring DNS in Gaia Clish

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

Description

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

Syntax

Configuring the DNS servers and the DNS suffix

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

Viewing the configured DNS servers and the DNS suffix

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

Deleting the DNS servers and the DNS suffix


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

i 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>	<p>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 1223).</p> <p> Note - Domain names that are also valid numeric IP addresses (for example: 10.19.76.100), although syntactically correct, are not permitted.</p> <p>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".</p>

IPv4 Static Routes

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

You define static routes manually in the Gaia Portal, or in Gaia Clish (in Gaia gClish on Security Groups) with the `"set static-route"` command.

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

Static route definitions include these parameters:

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


Configuring IPv4 Static Routes in Gaia Portal

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

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

Configuring One IPv4 Static Route at a Time

Step	Instructions
1	In the navigation tree, click Network Management > IPv4 Static Routes .
2	In the IPv4 Static Routes section, click Add . 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: <ul style="list-style-type: none"> ▪ Normal - To accept and forward packets ▪ Blackhole - To drop packets, and not send ICMP <i>unreachable</i> packet to the traffic source ▪ Reject - To drop packets, and send ICMP <i>unreachable</i> 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 <code>scope_local</code> attribute is set correctly, run the <code>"cat /etc/routed.conf"</code> command. For more information, see sk92799 .
8	In the Comment field, enter the applicable comment text (up to 100 characters).

Step	Instructions
9	<p>Click Add Gateway and select one of these options:</p> <ul style="list-style-type: none"> ▪ Option 1: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. <p> Notes:</p> <ul style="list-style-type: none"> ▪ <i>Priority</i> 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	<p>If you defined a next hop gateway by IP Address, you can select the Ping option, if you need to monitor next hops for the IPv4 static route with the <code>ping</code>. The Ping feature sends ICMP Echo Requests to make sure the next hop gateway for a static route is working.</p> <p>Gaia includes in the kernel forwarding table only next hop gateways, which are verified as working.</p> <p>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.</p>

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 : <ul style="list-style-type: none"> ▪ Normal - To accept and forward packets ▪ Blackhole - To drop packets, and not send ICMP <i>unreachable</i> packet to the traffic source ▪ Reject - To drop packets, and send ICMP <i>unreachable</i> packet to the traffic source
4	<p>Add the routes in the text box, using this syntax:</p> <pre style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <Destination IPv4 Address>/<Mask Length> <IPv4 Address of Next Hop Gateway> ["<Comment>"] </pre> <p>Where:</p> <ul style="list-style-type: none"> ▪ <i><Destination IPv4 Address>/<Mask Length></i> - 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 <code>default</code> keyword instead of an IPv4 address when referring to the default route. ▪ <i><IPv4 Address of Next Hop Gateway></i> - Specifies the IPv4 address of the next hop gateway ▪ <i>"<Comment>"</i> - Optional. Free text comment for the static route. Write the text in double quotes. Maximal length of the text string is 100 characters. <p>Example:</p> <pre style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> default 192.0.2.100 192.0.2.1 "Default Route" 192.0.2.200/24 192.0.2.18 "My Backup Route" </pre>
5	<p>Click Apply.</p> <p>The newly configured static routes show in the IPv4 Static Routes section.</p> <p>Note - The text box shows entries that contain errors with messages at the top of the page.</p>

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.

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

Syntax

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

Adding or configuring a default static IPv4 route

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

Adding or configuring a specific static IPv4 route

```
set static-route <Destination IPv4 Address>
  comment {"Text" | off}
  nexthop
    gateway
      address <IPv4 Address of Next Hop Gateway>
        {on | off}
      monitored-ip <Monitored IP Address> {on | off}
      monitored-ip-option {fail-all | fail-any | force-if-symmetry {on |
off}}
      [priority <Priority>]
      logical <Name of Local Interface>
        {on | off}
        [priority <Priority>]
    blackhole
    reject
  off
  ping {on | off}
  rank <Rank>
  scopelocal {on | off}
```

Viewing all configured static IPv4 routes

```
show route static all
```

Removing a default static IPv4 route

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

Removing a specific static IPv4 route

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

Removing a specific path only, when multiple next hop gateways are configured

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

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

i 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 <code>default</code> 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. <ul style="list-style-type: none"> 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 <i>unreachable</i> packet to the traffic source.
reject	Specifies that this next hop drops packets and sends ICMP <i>unreachable</i> packet to the traffic source.

Parameter	Description
<pre>address <IPv4 Address of Next Hop Gateway></pre>	<p>Specifies the IPv4 address of the next hop gateway.</p>
<pre>logical <Name of Local Interface></pre>	<p>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.</p>
<pre>monitored-ip <Monitored IP Address> {on off}</pre>	<p>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".</p>
<pre>monitored-ip-option {fail-all fail-any force-if-symmetry {on off}}</pre>	<p>Set failure condition and flavor for the configured monitored IP address(es).</p> <ul style="list-style-type: none"> ■ <code>fail-all</code> 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: <code>off</code> ■ <code>fail-any</code> 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: <code>on</code> ■ <code>force-if-symmetry</code> Ignores IP reachability reports from IP addresses with asymmetric traffic. Default: <code>off</code>

Parameter	Description
<pre>priority <Priority></pre>	<p>Defines which gateway to select as the next hop when multiple gateways are configured.</p> <p>The lower the priority, the higher the preference - priority 1 means the highest preference, and priority 8 means the lowest preference.</p> <p>You can define two or more paths with the same priority to specify a backup path with equal priority.</p> <p>A next hop gateway with no priority configured is preferred over a next hop gateway with priority configured</p>
<pre>nexthop ... on</pre>	<p>Adds the specified next hop gateway.</p>
<pre>nexthop ... off</pre>	<p>Deletes the specified next hop gateway.</p> <p>If you specify a next hop gateway, only the specified path is deleted.</p> <p>If you do not specify a next hop gateway, the route and all related paths are deleted.</p>
<pre>off</pre>	<p>Removes the static route.</p>
<pre>ping {on off}</pre>	<p>Enables (on) or disables (off) the ping of specified next hop gateways for IPv4 static routes.</p> <p>The Ping feature sends ICMP Echo Requests to make sure the next hop gateway for a static route is working.</p> <p>Gaia includes in the kernel forwarding table only next hop gateways, which are verified as working.</p> <p>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.</p> <p>To configure the ping behavior, run:</p> <pre style="border: 1px solid black; padding: 5px;">set ping count <value> set ping interval <value></pre>

Parameter	Description
<pre>rank <Rank></pre>	<p>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 <code>rank</code> keyword in place of the <code>next-hop</code> keyword with no other parameters. Accepted values are: <code>default (60)</code>, integer numbers from 0 to 255. In addition, see this command: "<code>set protocol-rank protocol <Rank></code>"</p>
<pre>scopelocal {on off}</pre>	<p>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 <code>scopelocal</code> attribute is set correctly, run the "<code>cat /etc/routed.conf</code>" command. For more information, see sk92799.</p>

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	256
Configuring IPv6 Static Routes in Gaia Clish	258
Troubleshooting	262

i Important - First, you must enable the IPv6 Support and reboot (see "[System Configuration](#)" on page 370).

Configuring IPv6 Static Routes in Gaia Portal

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

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

Procedure

Step	Instructions
1	In the navigation tree, click Network Management > IPv6 Static Routes .
2	In the IPv6 Static Routes section, click Add .
3	In the Destination / Mask Length field, enter the IPv6 address and prefix (default prefix is 64).
4	Select the Next Hop Type field select: <ul style="list-style-type: none"> ▪ Normal - To accept and forward packets ▪ Blackhole - To drop packets, and not send ICMP <i>unreachable</i> packet to the traffic source ▪ Reject - To drop packets, and send ICMP <i>unreachable</i> 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).

Step	Instructions
7	In the Add Gateway section, click Add .
8	In the Gateway Address field, enter the IPv6 address of the next hop gateway.
9	<p>In the Priority field, either do not enter anything, or select an integer between 1 and 8.</p> <p><i>Priority</i> defines the order for selecting the next hop gateway when multiple next hop gateways are configured.</p> <p>The lower the priority, the higher the preference - priority 1 means the highest preference, and priority 8 means the lowest preference.</p> <p>A next hop gateway with no priority configured is preferred over a next hop gateway with priority configured.</p> <p>You cannot configure two next hop gateways with the same priority, because IPv6 Equal Cost Multipath Routes are not supported.</p>
10	Click OK .
11	<p>Select the Ping6 option, if you need to monitor next hops for the IPv6 static route using <code>ping6</code>.</p> <p>The Ping6 feature sends ICMPv6 Echo Requests to make sure the next hop gateway for a static route is working.</p>
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.



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

Adding or configuring the default static IPv6 route

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

Adding or configuring the specific static IPv6 route

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

Viewing all configured static IPv6 routes

```
show ipv6 route static all
```

Removing the default static IPv6 route

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

Removing the specific static IPv6 route

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

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

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

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



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

Parameters

CLI Parameters

Parameter	Description
default	Defines the default static IPv6 route.
<i><Destination IPv6 Address></i>	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. <ul style="list-style-type: none"> 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 <i>unreachable</i> packet to the traffic source.
reject	Specifies that this next hop drops packets and sends ICMP <i>unreachable</i> packet to the traffic source.
address <i><IPv6 Address of Next Hop Gateway></i>	Defines the IPv6 address of the next hop gateway.
interface <i><Name of Local Interface></i>	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
<code>priority</code> <code><Priority></code>	<p>Defines the order for selecting the next hop gateway when multiple next hop gateways are configured.</p> <p>The lower the priority, the higher the preference - priority 1 means the highest preference, and priority 8 means the lowest preference.</p> <p>A next hop gateway with no priority configured is preferred over a next hop gateway with priority configured.</p> <p>You cannot configure two next hop gateways with the same priority, because IPv6 Equal Cost Multipath Routes are not supported.</p>
<code>nexthop ... on</code>	Adds the specified next hop gateway.
<code>nexthop ... off</code>	<p>Deletes the specified next hop gateway.</p> <p>If you specify a next hop, only the specified path is deleted.</p> <p>If you do not specify a next hop, the route and all related paths are deleted.</p>
<code>off</code>	Removes the static route.
<code>ping6 {on off}</code>	<p>Enables (<code>on</code>) or disables (<code>off</code>) the ping of specified next hop gateways for IPv6 static routes.</p> <p>The Ping6 feature sends ICMPv6 Echo Requests to make sure the next hop gateway for a static route is working.</p> <p>Gaia includes in the kernel forwarding table only next hop gateways, which are verified as working.</p> <p>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.</p> <p>To configure the ping6 behavior, run:</p> <pre style="border: 1px solid black; padding: 5px;">set ping count <value> set ping interval <value></pre>
<code>rank <Rank></code>	<p>Selects a route, if there are many routes to a destination that use different routing protocols.</p> <p>The route with the lowest rank value is selected.</p> <p>Use the <code>rank</code> keyword in place of the <code>nexthop</code> keyword with no other parameters.</p> <p>Accepted values are: <code>default</code> (60), integer numbers from 0 to 255.</p> <p>In addition, see this command: <code>set protocol-rank protocol <Rank></code></p>

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 370).
- On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

Syntax

- To add an IPv6 neighbor entry:

```
add neighbor-entry ipv6-address <IPv6 Address of Neighbor>
macaddress <MAC Address of Neighbor> interface <Name of Local
Interface>
```


- To show an IPv6 neighbor entry:

```
show neighbor<SPACE><TAB>
```

```
show neighbor TABLE
```

- To delete an IPv6 neighbor entry:

```
delete neighbor-entry ipv6-address <IPv6 Address of Neighbor>
interface <Name of Local Interface>
```

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

Parameters

Parameter	Description
<i><IPv6 Address of Neighbor></i>	Specifies the IPv6 address of a new static Neighbor Discovery entry

Parameter	Description
<i><MAC Address of Neighbor></i>	Specifies the MAC address for respective IPv6 address
<i><Name of Local Interface></i>	Name of the local interface that connects to the Neighbor

NetFlow Export

In This Section:

Introduction	265
Configuration Procedure	267
Available Commands in Gaia Clish	272

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 maximum of three NetFlow Collectors. Gaia sends the NetFlow records 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 send the records.

For more information, see [sk102041](#).

Configuration Procedure

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

1. Configure the NetFlow Export settings in Gaia

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

Configuring the NetFlow settings in Gaia Portal

- a. In the left navigation tree, click **Network Management > NetFlow Export**.
- b. **Optional:** In the **Global Options** section, configure when the NetFlow starts to send the data after a connection opens, and click **Apply**.

This configures how frequently the NetFlow sends the number of ongoing connections.

Enter a value between 10 and 60 seconds, or enter the value 0 to disable.


- c. In the **Collectors** section, click **Add**.

d. Enter the required data for each collector:

Parameter	Description
IP Address	The destination IPv4 address, to which Gaia sends the NetFlow packets. 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: <ul style="list-style-type: none"> ▪ 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.

e. Click **OK**.

- f. In the **Advanced Options** section, the **NetFlow Fw rule** option controls for which traffic to enable the NetFlow export:

Scenario	Instructions
You performed a Clean Install of R81.20	<ul style="list-style-type: none"> ■ By default (this option is cleared) the NetFlow export is enabled for traffic accepted by all Access Control rules. ■ You can select this option to enable the NetFlow export only for traffic accepted by Access Control rules with the Track option Log and Accounting you configured in SmartConsole. <ul style="list-style-type: none">  Important - If you selected this option, you must configure the applicable Access Control rules in SmartConsole.
You upgraded to R81.20 from R80.40 or lower version	<p>You must:</p> <ol style="list-style-type: none"> i. Configure select this option in Gaia Portal and click Apply. ii. Configure the applicable Access Control rules with the Track option Log and Accounting in SmartConsole.

Configuring the NetFlow settings in Gaia Clish

- a. **Optional:** Configure when the NetFlow starts to send the data after a connection opens.

```
set netflow liveconn_interval {<10-60> | 0}
```


Enter a value between 10 and 60 seconds, or enter the value 0 to disable.


- b. Configure a new NetFlow collector:

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


c. Configure for which traffic to enable the NetFlow export:

```
set netflow fwrule {1 | 0}
```

Scenario	Instructions
You performed a Clean Install of R81.20	<ul style="list-style-type: none"> ■ By default (value 0) the NetFlow export is enabled for traffic accepted by all Access Control rules. ■ You can configure the value 1 to enable the NetFlow export only for traffic accepted by Access Control rules with the Track option Log and Accounting you configured in SmartConsole. <ul style="list-style-type: none">  Important - If you configure the value 1, you must configure the applicable Access Control rules in SmartConsole.
You upgraded to R81.20 from R80.40 or lower version	<p>You must:</p> <ol style="list-style-type: none"> i. Configure the value 0 in Gaia Clish. ii. Configure the applicable Access Control rules with the Track option Log and Accounting in SmartConsole.

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

2. In SmartConsole, configure the explicit Access Control rules

-  **Important** - This step is necessary only in these cases:
- In Gaia Portal you selected the option "NetFlow Fw rule"
 - In Gaia Clish you ran the command "set netflow fwrule 0".
- a. From the left navigation panel, click **Security Policies**.
 - b. Open the applicable policy.
 - c. In the top left corner, click **Access Control > Policy**.

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

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

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

- e. Publish the SmartConsole session.
- f. Install the Access Control policy on the Security Gateway or Cluster object.

Available Commands in Gaia Clish

Syntax

- Configure when the NetFlow starts to send the data after a connection opens.

```
set netflow liveconn_interval {<10-60> | 0}
```

- To configure a new NetFlow collector:

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

- To change settings of an existing NetFlow collector:

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

- To configure for which traffic the NetFlow exports its records:

```
set netflow fwrule {1 | 0}
```


- To show the configured NetFlow collectors:

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

- To show when the NetFlow starts to send the data after a connection opens:

```
show netflow liveconn_interval
```

- To show for which traffic the NetFlow exports its records:


```
show netflow fwrule
```




- To delete a configured NetFlow collector:

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

CLI Parameters

Parameter	Description
<code>ip <IPv4 Address of Collector></code>	Specifies the destination IPv4 address of the NetFlow Collector, to which Gaia sends the NetFlow packets. This parameter is mandatory.
<code>port <Destination Port on Collector></code>	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.

Parameter	Description
<pre>srcaddr <Source IPv4 Address></pre>	<p>Optional: Specifies the source IPv4 address of the NetFlow packets.</p> <p>This must be an IPv4 address of the local host.</p> <p>The default is an IPv4 address of the network interface, from which Gaia sends the NetFlow packets.</p> <p>We recommend the default.</p>
<pre>export-format {Netflow_V5 Netflow_V9 IPFIX}</pre>	<p>The NetFlow protocol version to use:</p> <ul style="list-style-type: none"> ▪ Netflow_V5 - Protocol NetFlow v5 ▪ Netflow_V9 - Protocol NetFlow v9 (default) ▪ IPFIX - Known as protocol "NetFlow v10" <p>Each NetFlow protocol version has a different packet format.</p>
<pre>for-ip <IPv4 Address of Collector> for-port <Destination Port on Collector></pre>	<p>These parameters specify the configured NetFlow Collector.</p> <p> Notes:</p> <ul style="list-style-type: none"> ▪ 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.

Parameter	Description						
<pre>set netflow fwrule {1 0}</pre>	<p>Specifies for which traffic to enable the NetFlow export:</p> <table border="1" data-bbox="593 277 1463 1218"> <thead> <tr> <th data-bbox="593 277 810 353">Scenario</th> <th data-bbox="817 277 1463 353">Instructions</th> </tr> </thead> <tbody> <tr> <td data-bbox="593 358 810 913"> <p>You performed a Clean Install of R81.20</p> </td> <td data-bbox="817 358 1463 913"> <ul style="list-style-type: none"> ■ By default (value 0) the NetFlow export is enabled for traffic accepted by all Access Control rules. ■ You can configure the value 1 to enable the NetFlow export only for traffic accepted by Access Control rules with the Track option Log and Accounting you configured in SmartConsole. <p> Important - If you configure the value 1, you must configure the applicable Access Control rules in SmartConsole.</p> </td> </tr> <tr> <td data-bbox="593 918 810 1218"> <p>You upgraded to R81.20 from R80.40 or lower version</p> </td> <td data-bbox="817 918 1463 1218"> <p>You must:</p> <ol style="list-style-type: none"> 1. Configure the value 0 in Gaia Clish. 2. Configure the applicable Access Control rules with the Track option Log and Accounting in SmartConsole. </td> </tr> </tbody> </table>	Scenario	Instructions	<p>You performed a Clean Install of R81.20</p>	<ul style="list-style-type: none"> ■ By default (value 0) the NetFlow export is enabled for traffic accepted by all Access Control rules. ■ You can configure the value 1 to enable the NetFlow export only for traffic accepted by Access Control rules with the Track option Log and Accounting you configured in SmartConsole. <p> Important - If you configure the value 1, you must configure the applicable Access Control rules in SmartConsole.</p>	<p>You upgraded to R81.20 from R80.40 or lower version</p>	<p>You must:</p> <ol style="list-style-type: none"> 1. Configure the value 0 in Gaia Clish. 2. Configure the applicable Access Control rules with the Track option Log and Accounting in SmartConsole.
Scenario	Instructions						
<p>You performed a Clean Install of R81.20</p>	<ul style="list-style-type: none"> ■ By default (value 0) the NetFlow export is enabled for traffic accepted by all Access Control rules. ■ You can configure the value 1 to enable the NetFlow export only for traffic accepted by Access Control rules with the Track option Log and Accounting you configured in SmartConsole. <p> Important - If you configure the value 1, you must configure the applicable Access Control rules in SmartConsole.</p>						
<p>You upgraded to R81.20 from R80.40 or lower version</p>	<p>You must:</p> <ol style="list-style-type: none"> 1. Configure the value 0 in Gaia Clish. 2. Configure the applicable Access Control rules with the Track option Log and Accounting in SmartConsole. 						
<pre>set netflow liveconn_interval {<10-60> 0}</pre>	<p>Configures when the NetFlow starts to send the data after a connection opens. Enter a value between 10 and 60 seconds, or enter the value 0 to disable</p>						
<pre>show netflow fwrule</pre>	<p>Shows for which traffic the NetFlow exports its records:</p> <ul style="list-style-type: none"> ■ 1 The NetFlow export is enabled only for traffic accepted by Access Control rules with the Track option Log and Accounting you configured in SmartConsole. ■ 0 The NetFlow export is enabled for traffic accepted by all Access Control rules. 						

System Management

This chapter includes procedures and reference information for:



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

System Passwords

In this section, you can configure these passwords in Gaia OS:

- A password for the Expert mode
- A password for the Gaia GRUB (boot loader)
- ★ **Best Practice** - For security reasons, configure different passwords for the Expert mode and for GRUB.

Configuring System Passwords in Gaia Portal

-  **Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.
-  **Best Practice** - For security reasons, configure different passwords for the Expert mode and for GRUB.

Configuring the Expert mode password

Description



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

The default Gaia shell is called `clish`.

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

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

For low-level configuration, use the more permissive Expert mode shell. In addition, see [sk144112](#).

- To enter the Expert shell, run in Gaia Clish: `expert`
- To exit from the Expert shell and go back to Gaia Clish, run: `exit`
-  **Note** - If a command is supported in Gaia Clish, it is **not** supported to run the corresponding command in Expert mode.
For example, to work with interfaces, Gaia Clish provides the commands "`show interface`" and "`set interface`".
Therefore, it is **not** supported to run the `ifconfig` command in the Expert mode.
-  **Note** - There is **no** default password for the Expert mode. You must configure a password for the Expert mode before you can use it.

Procedure

Step	Instructions
1	With a web browser, connect to Gaia Portal at: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <code>https://<IP address of Gaia Management Interface></code> </div>
2	Click System Management > System Passwords .
3	In the section Change Expert Password , enter the required password. The password must contain at least 6 characters.
4	Click Apply .

Configuring the GRUB password**Description**

The GRUB password protects the GRUB menu and GRUB terminal.

Gaia asks for this password when you boot into the Maintenance Mode and revert Gaia snapshots.



**Important:**

- You must configure a GRUB password before you boot into the Maintenance Mode or revert a Gaia snapshot.
- If do not know your GRUB password, and Gaia does not boot into the Normal Mode, you must contact [Check Point Support](#).

Procedure

Step	Instructions
1	With a web browser, connect to Gaia Portal at: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <code>https://<IP address of Gaia Management Interface></code> </div>
2	Click System Management > System Passwords .
3	In the section Change GRUB Password , enter the required password. The password must contain at least 6 characters.
4	Click Apply .

Configuring System Passwords in Gaia Clish

-  **Important** - On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
-  **Best Practice** - For security reasons, configure different passwords for the Expert mode and for GRUB.

Configuring the Expert mode password

Description

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



The default Gaia shell is called `clish`.

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

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

For low-level configuration, use the more permissive Expert mode shell. In addition, see [sk144112](#).

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

-  **Note** - If a command is supported in Gaia Clish, it is **not** supported to run the corresponding command in Expert mode.
For example, to work with interfaces, Gaia Clish provides the commands "`show interface`" and "`set interface`".
Therefore, it is **not** supported to run the `ifconfig` command in the Expert mode.
-  **Note** - There is **no** default password for the Expert mode. You must configure a password for the Expert mode before you can use it.

Syntax to configure an Expert mode password in plain text

```
set expert-password
```



The password must contain at least 6 characters.

Syntax to configure an Expert mode password as a salted hash

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

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

Parameters

Parameter	Description
<code>hash <Hash String></code>	<p>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 "copenssl" command (run: <code>copenssl passwd -help</code>). To configure the default hash algorithm, see:</p> <ul style="list-style-type: none"> ▪ "Password Hashing Algorithm" on page 459 (in Gaia Portal) ▪ "Configuring Hashing Algorithm" on page 468 (in Gaia Clish) <p> Best Practice - Do not use MD5 hash because it is not secure.</p> <p> Notes:</p> <ul style="list-style-type: none"> ▪ Format: <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <code>\$<Hash Standard>\$<Salt>\$<Encrypted></code> </div> ▪ The length of this hash string must be less than 128 characters. ▪ <code><Hash Standard></code> <p>One of these digits:</p> <ul style="list-style-type: none"> • 1 = MD5 • 5 = SHA256 • 6 = SHA512 ▪ <code><Salt></code> <p>A string of these characters: <code>a-z A-Z 0-9 . / [] _ ` ^</code></p> <p>The length of this string must be between 2 and 16 characters.</p> ▪ <code><Encrypted></code> <p>A string of these characters: <code>a-z A-Z 0-9 . / [] _ ` ^</code></p> <p>The length of this string must be:</p> <ul style="list-style-type: none"> • 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
```

Configuring the GRUB password

Description

The GRUB password protects the GRUB menu and GRUB terminal.

Gaia asks for this password when you boot into the Maintenance Mode and revert Gaia snapshots.

Important:

- You must configure a GRUB password before you boot into the Maintenance Mode or revert a Gaia snapshot.
- If do not know your GRUB password, and Gaia does not boot into the Normal Mode, you must contact [Check Point Support](#).

Syntax to configure a GRUB password in plain text

```
set grub2-password
```

The password must contain at least 6 characters.


Syntax to configure a GRUB password as a SHA512 salted hash

```
set grub2-password-hash <Hash String>
```

Use the slated hash configuration when you upgrade or restore with user-defined shell scripts.

 **Important** - Gaia saves the new GRUB password automatically.

Parameters

Parameter	Description
hash <Hash String>	<p>The password as a SHA512 salted hash instead of plain text.</p> <p> Notes:</p> <ul style="list-style-type: none"> ■ To get a hash string for a password, run this command in the Expert mode: <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">grub2-mkpasswd-pbkdf2</div> ■ Format of the hash string: <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">grub.pbkdf2.sha512.<Rounds>.<Salt>.<Checksum></div> ■ The length of this hash string must be between 282 and 512 characters. ■ grub.pbkdf2.sha512 A constant string. ■ <Rounds> The number of iterations stored in the decimal format. In Gaia OS, this number is always 10000. ■ <Salt> The salt string that is encoded using upper-case hexadecimal digits. The length of this string must be 128 characters. ■ <Checksum> The resulting derived key that is encoded using upper-case hexadecimal digits. The length of this string must be 128 characters.

Example 1 - Plain text

```

gaia> set grub2-password
Enter new grub2 password: *
Enter new grub2 password (again): *
Password is only 1 characters long; it must be at least 6 characters in length.
Enter new grub2 password: *****
Enter new grub2 password (again): *****
Password is not complex enough; try mixing more different kinds of characters (upper case, lower case, digits, and punctuation).
Enter new grub2 password: *****
Enter new grub2 password (again): *****
gaia>

gaia> show configuration grub2-password
set grub2-password-hash grub.pbkdf2.sha512.10000.B8A(---truncated---)7D0.017(---truncated---)623
gaia>

```

Example 2 - Salted SHA512 hash

```
[Expert@gaia:0]# grub2-mkpasswd-pbkdf2
Enter password: *****
Reenter password: *****
PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.B8A(---truncated---)7D0.017(---truncated---)623
[Expert@gaia:0]#

[Expert@gaia:0]# clish


gaia> set grub2-password-hash grub.pbkdf2.sha512.10000.B8A(---truncated---)7D0.017(---truncated---)623
gaia>

gaia> show configuration grub2-password
set grub2-password-hash grub.pbkdf2.sha512.10000.B8A(---truncated---)7D0.017(---truncated---)623
gaia>
```

Proxy

Proxy for Gaia Operating System


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

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

Proxy for Check Point Servers

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

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

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

Security Gateway as an HTTP/HTTPS Proxy

You can configure a Security Gateway or Cluster as an HTTP/HTTPS Proxy. See the [R81.20 Quantum Security Gateway Guide](#) > Chapter "HTTP/HTTPS Proxy".

Configuring Proxy in Gaia Portal

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

Configuring a proxy server

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

Editing the existing proxy server configuration

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

Removing the existing proxy server configuration

Step	Instructions
1	With a web browser, connect to Gaia Portal at: <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"><code>https://<IP address of Gaia Management Interface></code></div>
2	Click System Management > Proxy .
3	Clear Use a Proxy server .
4	Click Apply .

Configuring Proxy in Gaia Clish

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

Syntax

Configuring a proxy server or editing the existing proxy server configuration

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

Removing the existing proxy server configuration

```
delete proxy  
    address  
    all  
    port
```

Viewing the existing proxy server configuration

```
show proxy  
    address  
    port
```

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

Time

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

This is important for these reasons:

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

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

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

Network Time Protocol (NTP)

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

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

Configuring the Time and Date manually

Step	Instructions
1	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:

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

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
<i><date></i>	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 an NTP interface:

By default, Gaia uses all interfaces to work with the configured NTP servers (based on the routing table).

You can configure Gaia to use only a specific interface to work with NTP.

To configure such an interface, it must have an IP address assigned.

```
add ntp interface <Name of Interface>
```

- To 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
    interface
    servers
```

- To delete an NTP server:



```
delete ntp server <IPv4 address or Hostname of NTP Server>
```

- To delete an NTP interface:

If you delete all specific NTP interfaces, then by default, Gaia uses all interfaces to work with the configured NTP servers (based on the routing table).

```
delete ntp interface <Name of Interface>
```


Parameters

Parameter	Description
active	Shows the NTP status: <ul style="list-style-type: none"> ▪ Yes - enabled ▪ No - disabled
current	Shows the IP address or Host name of the NTP server that Gaia uses right now.
interface	Shows the specific NTP interfaces.
servers	Shows the configured NTP servers.
active {on off}	Enables (on) or disables (off) NTP.
server	Keyword that identifies the NTP server - time server, from which Gaia synchronizes its clock. The specified time server does not synchronize to the local clock of Gaia.
primary	Configures the IP address or Host name of the primary NTP server.
secondary	Configures the IP address or Host name of the secondary NTP server.  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.
<Name of Interface>	Press the TAB key to see the available interfaces.

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.

-  **Important** - Scalable Platforms (Maestro and Chassis) do **not** support this feature (Known Limitation MBS-4756).

Configuring Cloning Groups in Gaia Portal

Important:

- Scalable Platforms (Maestro and Chassis) do **not** support this feature (Known Limitation MBS-4756).
- If you change the members of a Gaia Cloning Group with many members down, you are logged out of the Gaia Portal with an incorrect error message:
Unable to connect to server.

The correct message is:

An error occurred while applying configuration change to all cloning group members- the operation was successful only for online members.

This is the normal behavior of the cloning group. This error does not indicate a critical failure.

Creating a new Cloning Group

Step	Instructions
1	With a web browser, connect to Gaia Portal at: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"><code>https://<IP address of Gaia Management Interface></code></div>
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. <ol style="list-style-type: none"> 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 (<i>admin</i>). This password is necessary to: <ul style="list-style-type: none"> ▪ 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.

Step	Instructions
5	<p>In the Shared Features screen, select features to clone to other members of the Cloning Group.</p> <p>Pay attention to the features you want to clone.</p> <p>For example, you might not want to clone static routes to Security Gateways that are members of a cluster.</p>
6	Click Next for the Wizard Summary .
7	Click Finish .

List of Shared Features

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

Table: Shared Features in Gaia Portal

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


Table: Shared Features in Gaia Portal (continued)


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

Table: Shared Features in Gaia Portal (continued)

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

Managing a Cloning Group

Step	Instructions
1	Sign out of the Gaia Portal.
2	Sign in <i>to the same Gaia Portal</i> using the <i>admin</i> account and password. (Alternatively, log in to the Gaia Portal on the Security Gateway using the <i>admin</i> 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.

Managing a Cloning Group as an assigned administrator

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

Joining an existing Cloning Group


Step	Instructions
1	<p>Connect to the Gaia Portal on a Security Gateway. With a web browser, connect to Gaia Portal at:</p> <pre>https://<IP address of Gaia Management Interface></pre>
2	<p>In System Management > Cloning Group, click Start Cloning Group Creation Wizard. The Cloning Group Wizard opens.</p>
3	<p>Select Join an existing Cloning Group.</p>
4	<p>The Join Existing Cloning Group window opens.</p> <ul style="list-style-type: none"> ▪ 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 (<i>cadmin</i>). (The same password you entered when you created the Cloning Group, to which you wish to join.) The <i>cadmin</i> password: <ul style="list-style-type: none"> • Lets you log in to the <i>cadmin</i> account • Is used to create authentication credentials for members during synchronization
5	<p>Click Finish.</p>

Creating a Cloning Group that follows ClusterXL

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

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




Step	Instructions
1	Connect to the Gaia Portal on a Security Gateway. With a web browser, connect to Gaia Portal at: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <code>https://<IP address of Gaia Management Interface></code> </div>
2	In System Management > Cloning Group , click Start Cloning Group Creation Wizard . The Cloning Group Creation Wizard opens.
3	Select Cloning group follows ClusterXL . <ul style="list-style-type: none"> ▪ Enter the Cloning Group name. ▪ Enter a password for the Cloning Group administration account (<i>cadmin</i>).
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	306
CLI Syntax	307

-  **Note** - When run from the *admin* account, these commands apply to all members of the Gaia group.
-  **Important** - After you add, configure, or delete features, run the "save config" command to save the settings permanently.
-  **Important** - Scalable Platforms (Maestro and Chassis) do **not** support this feature (Known Limitation MBS-4756).

Cloning Group Modes

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

Creating the first Cloning Group member in Manual mode

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

Adding other Security Gateways to the Cloning Group in Manual mode

Perform these steps on each of the Security Gateways.

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

Creating Cloning Group members in ClusterXL mode

Perform these steps on all member Security Gateways.

Step	Instructions
1	Set the cloning group mode to <code>ClusterXL</code> .
2	Set the cloning group password.
3	Set the cloning group state to <code>on</code> .


CLI Syntax

Creating and configuring a Cloning Group

Syntax

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

Parameters

Parameter	Description
<code>local-ip</code> <IPv4 address>	The IPv4 address used to synchronize shared features between members of the Cloning Group.
<code>mode</code> {manual cluster-xl}	The mode determines whether the Cloning Group is defined manually, or through ClusterXL.
<code>name</code> <Name of Cloning Group>	Name of the Cloning Group.
<code>password</code> <Password>	Password for the administrator's (admin) account, used to access the Cloning Group configuration in the Gaia Portal, or Gaia Clish. When prompted, enter and confirm the password.
<code>state</code> {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.

Adding Shared Features

Syntax

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

Parameters

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

List of Shared Features

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

Table: Shared Features in Gaia Clish

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

Table: Shared Features in Gaia Clish (continued)

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

Table: Shared Features in Gaia Clish (continued)

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

Deleting Shared Features

Syntax

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

Parameters


Parameter	Description
<Feature>	<p>The name of the feature to be deleted from the list of shared features. To see the list of the enabled Shared Features:</p> <ol style="list-style-type: none"> Enter: <pre>delete cloning-group shared-feature</pre> Press <SPACE> and <TAB>.

Joining an existing Cloning Group

Syntax

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

Parameters

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

Removing a member from a Cloning Group

```
leave cloning-group
```

Removing an inaccessible Cloning Group member

Syntax

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

Parameters

Parameter	Description
<i><IPv4 address of Member></i>	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.

i **Notes:**


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

Viewing the Cloning Group configuration

Syntax

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


Parameters

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

Synchronizing a member in the Cloning Group

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

Enabling or disabling the Cloning Group management mode

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

Syntax

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

Parameters

Parameter	Description
<code>on</code>	Enables the Cloning Group management mode.
<code>off</code>	Disables the Cloning Group management mode.

SNMP

In This Section:

Introduction	314
SNMP v3 - User-Based Security Model (USM)	316
Enabling SNMP	316
SNMP Agent Address	316
SNMP Traps	317

Introduction

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

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

Notes:

- The Check Point implementation also supports the User-based Security model (USM) portion of SNMPv3.
- The Gaia implementation of SNMP is built on NET-SNMP.
Changes were made to the first version to address security and other fixes.
For more information, see [Net-SNMP](#).
- Scalable Platform Security Groups support only this SNMP OID branch:
OID 1.3.6.1.4.1.2620.1.48
`iso.org.dod.internet.private.enterprise.checkpoint.products.asg`
To see VPN status, you can use the `tunnelTable` branch (OID 1.3.6.1.4.1.2620.500.9002.1).
- Scalable Platform Security Groups support only this SNMP trap:
OID 1.3.6.1.4.1.2620.1.2001
`iso.org.dod.internet.private.enterprise.checkpoint.products.asg`
Trap

Warning - If you use SNMP, we recommend that you change the community strings for security purposes. If you do not use SNMP, disable SNMP or the community strings.

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

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

SNMP, as implemented on Check Point platforms, enables an SNMP manager to monitor the device using `GetRequest`, `GetNextRequest`, `GetBulkRequest`, and a select number of traps.

The Check Point implementation also supports using `SetRequest` to change these attributes: `sysContact`, `sysLocation`, and `sysName`. You must configure read-write permissions for set operations to work.

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


Use Gaia to run these tasks:

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

SNMP v3 - User-Based Security Model (USM)

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

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

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

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


Enabling SNMP


The SNMP daemon is disabled by default.

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

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

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

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

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

SNMP Agent Address

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

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

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

SNMP Traps

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

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

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


Gaia supports these types of SNMP traps:

Table: SNMP Traps in Gaia

Type of Trap	Description
<code>coldStart</code>	Notifies when the SNMPv2 agent is re-initialized.
<code>linkUpLinkDown</code>	Notifies when one of the links changes state to up or down.
<code>authorizationError</code>	Notifies when an SNMP operation is not properly authenticated.
<code>configurationChange</code>	Notifies when a change to the system configuration is applied.
<code>configurationSave</code>	Notifies when a permanent change to the system configuration occurs.
<code>lowDiskSpace</code>	Notifies when space on the system disk is low. Sent if the disk space utilization in the <code>/</code> partition has reached 80 percent or more of its capacity.
<code>powerSupplyFailure</code>	Notifies when a power supply for the system fails. This trap is supported only on platforms with two power supplies installed and running.
<code>fanFailure</code>	Notifies when a CPU or chassis fan fails.
<code>overTemperature</code>	Notifies when the temperature rises above the threshold.
<code>highVoltage</code>	Notifies if one of the voltage sensors exceeds its maximum value.
<code>lowVoltage</code>	Notifies if one of the voltage sensors falls below its minimum value.

Table: SNMP Traps in Gaia (continued)

Type of Trap	Description
<code>raidVolumeState</code>	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 <code>raid_diagnostic</code> and confirm that it shows the RAID status.
<code>biosFailure</code>	Notifies when the Primary BIOS failure is detected. Sent once the event occurs. Applies to computers with Dual BIOS.
<code>vrrpv2AuthFailure</code>	Notifies when the VRRP Cluster Member has packet an authentication failure in VRRPv2 (IPv4) and VRRPv3 (IPv6). Sent each polling interval.
<code>vrrpv2NewMaster</code>	Notifies when the VRRP Cluster Member transitioned to VRRP Master state in VRRPv2 (IPv4). Sent each polling interval.
<code>vrrpv3NewMaster</code>	Notifies when the VRRP Cluster Member transitioned to VRRP Master state in VRRPv3 (IPv6). Sent each polling interval.
<code>vrrpv3ProtoError</code>	Notifies when the VRRP Cluster Member has a protocol error in VRRPv2 (IPv4) and VRRPv3 (IPv6). Sent each polling interval.

 **Important** - For Scalable Platforms, see the:

- [R81.20 Quantum Maestro Administration Guide](#) > Chapter *Logging and Monitoring* > Section *System Monitoring* > Section *Working with SNMP*.
- [R81.20 Quantum Scalable Chassis Administration Guide](#) > Chapter *Logging and Monitoring* > Section *System Monitoring* > Section *Working with SNMP*.

Configuring SNMP in Gaia Portal

For detailed information, see [sk90860: How to configure SNMP on Gaia OS](#).


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

Enabling SNMP


Step	Instructions
1	In the navigation tree, click System Management > SNMP .
2	Select Enable SNMP Agent .
3	In the Version drop down list, select the version of SNMP to run: <ul style="list-style-type: none"> ▪ 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 .

Configuring 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.


Configuring the SNMP community strings

Step	Instructions
1	In the V1/V2 Settings section, in Read Only Community String , set a string other than public . You must always use this as 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

Adding a USM user

Step	Instructions
1	In the navigation tree, click System Management > SNMP .
2	In the V3 - User-Based Security Model (USM) section, click Add . The Add New USM User window opens.
3	<p>In the User Name, enter the applicable user name. This can be the same as a user name for system access.</p> <p> Notes:</p> <ul style="list-style-type: none"> ▪ 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	<p>In the Security Level, select one of these options from the drop-down list:</p> <ul style="list-style-type: none"> ▪ 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	<p>In the User Permissions, select one of these options from the drop-down list:</p> <ul style="list-style-type: none"> ▪ read-only ▪ read-write
6	<p>In the Authentication Protocol, select one of these options from the drop-down list:</p> <ul style="list-style-type: none"> ▪ SHA256 ▪ SHA512 <p>The default is SHA512.</p> <p> Note - When you change the configured Authentication Protocol of an existing SNMPv3 USM user, Gaia OS requires you to change the Authentication Pass Phrase because the previous password is not valid anymore.</p>

Step	Instructions
7	In the Authentication Pass Phrase , enter a password for the user that is between 8 and 128 characters in length.
8	In the Privacy Protocol , select: <ul style="list-style-type: none"> ▪ DES ▪ AES ▪ AES256 <p>The default is DES.</p> <p> Note - When you change the configured Privacy Protocol of an existing SNMPv3 USM user, Gaia OS requires you to change the Privacy Pass Phrase because the previous password is not valid anymore.</p>
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.

Editing a USM user

Step	Instructions
1	In the navigation tree, click System Management > SNMP .
2	In the V3 - User-Based Security Model (USM) section, select the user and click Edit . The Edit USM User window opens.
3	You can change the Security Level , User Permissions , the Authentication Protocol , the Authentication Passphrase , or the Privacy Protocol .
4	Click Save .

Deleting a USM user

Step	Instructions
1	In the navigation tree, click System Management > SNMP .
2	In the V3 - User-Based Security Model (USM) section, select the user and click Remove . The Deleting USM User Entry window opens.
3	The window shows this message: Are you sure you want to delete "username" entry? Click Yes .

Enabling or disabling SNMP trap types

Step	Instructions
1	In the navigation tree, click System Management > SNMP .
2	In the Enabled Traps section, click Set . The Add New Trap Receiver window opens. <ul style="list-style-type: none"> ▪ To enable a trap: Select it from the Disabled Traps list, and click Add> ▪ To disable a trap: Select it 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

Adding an SNMP trap receiver

Step	Instructions
1	In the navigation tree, click System Management > SNMP .
2	In the Trap Receivers Settings section, click Add . The Add New Trap Receiver window opens.
3	In the IPv4 Address , enter the IP address of an SNMP receiver.
4	In the Version , select the SNMP Version for the specified receiver.
5	In the Community String , enter the SNMP community string for the specified receiver.
6	Click Save .

Editing an SNMP trap receiver

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

Deleting an SNMP trap receiver

Step	Instructions
1	In the navigation tree, click System Management > SNMP .
2	In the Trap Receivers Settings section, select the SNMP trap receiver and click Remove . 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	<p>In the OID, enter the SNMP OID to query.</p> <ul style="list-style-type: none"> ▪ 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 $x.x.x$. (124 sub-identifiers more) ▪ Number range of each sub-identifier: 0 - 4294967295. ▪ The first sub-identifier must be one of these numbers: <ul style="list-style-type: none"> • 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	<p>In the Operator field, select the applicable operator to examine the value the SNMP OID to query returns:</p> <ul style="list-style-type: none"> ▪ 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	<p>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.</p>

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 .

Working with SNMP Traps on Scalable Platforms

See the:

- [R81.20 Quantum Maestro Administration Guide](#) > Chapter *Logging and Monitoring* > Section *System Monitoring* > Section *Working with SNMP*.
- [R81.20 Quantum Scalable Chassis Administration Guide](#) > Chapter *Logging and Monitoring* > Section *System Monitoring* > Section *Working with SNMP*.

Configuring SNMP in Gaia Clish

For detailed information, see [sk90860: How to configure SNMP on Gaia OS](#).

Important:


- On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- Scalable Platforms do **not** support the "set snmp traps" command. You must use the "asg alert" configuration wizard to configure SNMP traps in Gaia gClish.
- After you add, configure, or delete features, run the "save config" command to save the settings permanently.

Best Practice:

For commands that include "auth-pass-phrase", "privacy-pass-phrase", or both, use the hashed commands.

To get the hashed password, run the "show configuration snmp" command.

Syntax for the 'add' commands

 **Note** - To see all available commands:

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

Syntax

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

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

Description of commands

Command	Description
<pre>add snmp custom-trap ...</pre>	<p>Adds a custom SNMP trap:</p> <ul style="list-style-type: none"> ■ <i><Custom Trap Name></i> Specifies the name of the custom trap. Range: 1 - 128 characters. ■ <i>oid <Value></i> Specifies the SNMP OID to query. <ul style="list-style-type: none"> • 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 <i>X.X</i> to <i>X.X</i>. (124 sub-identifiers more) • Number range of each sub-identifier: 0 - 4294967295. • The first sub-identifier must be one of these numbers: <ul style="list-style-type: none"> ◦ 0 In this case, the second sub-identifier must be between 0-39: <i>0.<0-39></i>. (other applicable sub-identifiers) ◦ 1 In this case, the second sub-identifier must be between 0-39: <i>1.<0-39></i>. (other applicable sub-identifiers) ◦ 2 <i>2.X</i>. (other applicable sub-identifiers) ■ <i>operator <Logical Operator></i> Specifies the operator to examine the value the SNMP OID to query returns: <ul style="list-style-type: none"> • <i>Equal</i> - The returned value is equal to the value in the "threshold" parameter. • <i>Not_Equal</i> - The returned value is not equal to the value in the "threshold" parameter. • <i>Less_Than</i> - The returned value is less than the value in the "threshold" parameter. • <i>Greater_Than</i> - The returned value is greater than the value in the "threshold" parameter. • <i>Changed</i> - The returned value is different than the returned value in the previous SNMP OID query. ■ <i>threshold <Value></i> Specifies an integer value to which Gaia operating system compares the value returned in the SNMP OID query. Range: 1 - 128 characters. ■ <i>frequency <Value></i>

Command	Description
	<p>Specifies the interval (in seconds) between the SNMP OID queries. Range: 1 - 4294967295.</p> <ul style="list-style-type: none"> 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 ...	<p>Adds an SNMPv3 USM user.</p> <p>Notes:</p> <ul style="list-style-type: none"> 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 | AES256} authentication-protocol
{SHA256 | SHA512}
set snmp usm user <UserName> security-level authPriv auth-pass-
phrase-hashed <Hashed Pass Phrase> privacy-pass-phrase <Privacy
Pass Phrase> privacy-protocol {DES | AES | AES256}
authentication-protocol {SHA256 | SHA512}
set snmp usm user <UserName> security-level authNoPriv auth-
pass-phrase <Pass Phrase> authentication-protocol {SHA256 |
SHA512}
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
<code>set snmp agent-version {any v3-Only}</code>	Configures the supported SNMP version: <ul style="list-style-type: none"> ▪ <code>all</code> - Support SNMP v1, v2 and v3. ▪ <code>v3-Only</code> - Support SNMP v3 only.
<code>set snmp agent {on off}</code>	Enables (<code>on</code>) or disables (<code>off</code>) the SNMP Agent.
<code>set snmp clear-trap ...</code>	Configures the indication of a custom SNMP trap termination.
<code>set snmp community <String> {read-only read-write}</code>	Configures the SNMP community password and if this password lets you only read the values of SNMP objects (<code>read-only</code>), or set the values as well (<code>read-write</code>).
<code>set snmp contact ...</code>	Configures the contact name for the SNMP community.
<code>set snmp custom-trap ...</code>	Configures the settings of an existing custom SNMP trap. See the explanations in the "add snmp custom-trap" command.
<code>set snmp location ...</code>	Configures the contact location for the SNMP community.
<code>set snmp mode {default vs}</code>	Configures how to run the SNMP daemon: <ul style="list-style-type: none"> ▪ <code>default</code> <ul style="list-style-type: none"> • On non-VSX Gateway, this is the only supported mode. • On VSX Gateway, SNMP daemon runs only in the context of VS0. ▪ <code>vs</code> <ul style="list-style-type: none"> • For VSX Gateway only. • Each Virtual Device has a separate SNMP daemon running in the context of that Virtual Device.
<code>set snmp traps coldStart-threshold <Seconds></code>	Configures the threshold for the SNMP <code>coldStart</code> trap.

Command	Description
<pre>set snmp traps polling-frequency <Seconds></pre>	Configures the polling interval for the SNMP traps.
<pre>set snmp traps receiver ...</pre>	Configures the IPv4 address of the SNMP Trap Sink.
<pre>set snmp traps trap-user <UserName></pre>	Configures the user, which will generate the SNMP traps.
<pre>set snmp traps trap ...</pre>	Configures the Gaia built-in SNMP traps.
<pre>set snmp usm user <UserName> ...</pre>	<p>Configures the SNMPv3 USM user.</p> <p> Notes:</p> <ul style="list-style-type: none"> ▪ When you change the configured Authentication Protocol of an existing SNMPv3 USM user, Gaia OS requires you to change the Authentication Pass Phrase because the previous password is not valid anymore. ▪ When you change the configured Privacy Protocol of an existing SNMPv3 USM user, Gaia OS requires you to change the Privacy Pass Phrase because the previous password is not valid anymore.
<pre>set snmp vs- direct-access {on off}</pre>	<p>Enables (<code>on</code>) and disables (<code>off</code>) the SNMP direct queries on the IP address of a Virtual System (not only VS0), or Virtual Router.</p> <p>This mode works only when SNMP <code>vs</code> mode is enabled. See the R81.20 VSX Administration Guide.</p>

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.

Command	Description
<code>delete snmp traps trap-user <UserName></code>	Removes the user, which will generate the SNMP traps.
<code>delete snmp usm user <UserName></code>	Removes the SNMPv3 USM user.

Working with SNMP Traps on Scalable Platforms

See the:

- [R81.20 Quantum Maestro Administration Guide](#) > Chapter *Logging and Monitoring* > Section *System Monitoring* > Section *Working with SNMP*.
- [R81.20 Quantum Scalable Chassis Administration Guide](#) > Chapter *Logging and Monitoring* > Section *System Monitoring* > Section *Working with SNMP*.

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`, `noSuchObject`, `noSuchInstance`, or `EndOfMibView`.

This table describes the elements:

Variable-bindings element	Description
<code>value</code>	Value that is associated with each object instance. This value is specified in a PDU request.
<code>unSpecified</code>	A NULL value is used in retrieval requests.
<code>noSuchObject</code>	Indicates that the agent does not implement the object, to which it refers by this object identifier.
<code>noSuchInstance</code>	Indicates that this object does not exist for this operation.
<code>endOfMIBView</code>	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
<code>noSuchObject</code>	If a variable does not have an <code>OBJECT IDENTIFIER</code> prefix that exactly matches the prefix of any variable accessible by this request, its value field is set to <code>noSuchObject</code> .
<code>noSuchInstance</code>	If the variable's name does not exactly match the name of a variable, its value field is set to <code>noSuchInstance</code> .
<code>genErr</code>	If the processing of a variable fails for any other reason, the responding entity returns <code>genErr</code> and a value in the error-index field that is the index of the problem object in the variable-bindings field.
<code>tooBig</code>	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 <code>tooBig</code> , an error-index of zero, and an empty variable-bindings field.

GetNextRequest

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

GetBulkRequest

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

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

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

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

Job Scheduler


You can schedule regular jobs.


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

Configuring Job Scheduler in Gaia Portal

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

Scheduling new jobs

Step	Instructions
1	In the navigation tree, click System Management > Job Scheduler .
2	Click Add . 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	<p>In the Command to Run, enter the name of the command.</p> <p> Important:</p> <ul style="list-style-type: none"> ▪ 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 651): <ul style="list-style-type: none"> • On a Security Management Server / Log Server / SmartEvent Server: <div data-bbox="576 954 1458 1057" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>source /etc/profile.d/CP.sh ; <Applicable Check Point Command></pre> </div> • On a Multi-Domain Server / Multi-Domain Log Server: <div data-bbox="576 1106 1458 1330" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>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></pre> </div> • On a Security Gateway / Cluster Members (non-VSX): <div data-bbox="576 1379 1458 1482" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>source /etc/profile.d/CP.sh ; <Applicable Check Point Command></pre> </div> • On a VSX Gateway / VSX Cluster Members: <div data-bbox="576 1532 1458 1671" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>source /etc/profile.d/CP.sh ; source /etc/profile.d/vsenv.sh ; <Applicable Check Point Command></pre> </div>
5	Below the Schedule , select the frequency (Minute Interval, Hourly, Daily, Weekly, Monthly, During Boot) 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 353).
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:

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

Syntax

Adding new scheduled jobs

```
add cron job <Job Name> command "<Command>" recurrence
    daily time <HH:MM>
    hourly hours {all | <0-23> | <HH1>,<HH2>,...,<HHn>} at <1-
59>
    interval <1-59>
    monthly month <1-12> days <1-31> time <HH:MM>
    weekly days <0-6> time <HH:MM>
    system-startup
```

Editing the existing scheduled jobs

```
set cron job <Job Name>
    command "<Command>"
    recurrence
        daily time <HH:MM>
        hourly hours {all | <0-23> | <HH1>,<HH2>,...,<HHn>}
at <1-59>
    interval <1-59>
    monthly month <1-12> days <1-31> time <HH:MM>
    weekly days <0-6> time <HH:MM>
    system-startup

set cron mailto <Email Address>
```

Viewing the existing scheduled jobs

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


Deleting the existing scheduled jobs

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

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

Parameters**CLI Parameters**

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

Parameter	Description
"<Command>"	<p>The command to run.</p> <p> Important:</p> <ul style="list-style-type: none"> ▪ The command must be a Linux command. ▪ You must enclose the syntax in quotes: <ul style="list-style-type: none"> • 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 651): <ul style="list-style-type: none"> • On a Security Management Server / Log Server / SmartEvent Server: <pre data-bbox="767 835 1457 936" style="border: 1px solid #ccc; padding: 5px;">source /etc/profile.d/CP.sh ; <Applicable Check Point Command></pre> • On a Multi-Domain Server / Multi-Domain Log Server: <pre data-bbox="767 1025 1457 1361" style="border: 1px solid #ccc; padding: 5px;">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></pre> • On a Security Gateway / Cluster Members (non-VSX): <pre data-bbox="767 1458 1457 1559" style="border: 1px solid #ccc; padding: 5px;">source /etc/profile.d/CP.sh ; <Applicable Check Point Command></pre> • On a VSX Gateway / VSX Cluster Members: <pre data-bbox="767 1608 1457 1749" style="border: 1px solid #ccc; padding: 5px;">source /etc/profile.d/CP.sh ; source /etc/profile.d/vsenv.sh ; <Applicable Check Point Command></pre>

Parameter	Description
<pre>recurrence daily time <HH:MM></pre>	<p>Specifies that the job should run once a day - every day, at specified time.</p> <p>Enter the time of day in the 24-hour clock format - <Hours>:<Minutes>.</p> <p>Example: 14:35</p>
<pre>recurrence hourly hours {all <0-23> < HH1 >,< HH2>,...,<HHn>} at <1-59></pre>	<p>Specifies that the job should run every day at a specified hour and minute:</p> <ul style="list-style-type: none"> ■ all at <1-59> Run each hour at the specified minute Example (run every day at <HH>:15): all at 15 ■ <0-23> at <1-59> Run at a specific hour and at the specified minute Example (run every day at 14:15): 14 at 15 ■ <HH1>,<HH2>,...,<HHn> at <1-59> Run at specific hours and at the specified minute Example (run every day at 10:15, 12:15, and 14:15): 10,12,14 at 15
<pre>recurrence interval <1-59></pre>	<p>Specifies that the job should run every number of minutes.</p> <p>Example (run every 15 minutes): 15</p>
<pre>recurrence monthly month <1-12> days <1-31> time <HH:MM></pre>	<p>Specifies that the job should run once a month - on specified months, on specified dates, and at specified time.</p> <p>Months are specified by numbers from 1 to 12:</p> <ul style="list-style-type: none"> ■ January = 1 ■ February = 2 ■ ... ■ December = 12 <p>Dates of month are specified by numbers from 1 to 31.</p> <p>To specify several consequent months, enter their numbers separate by commas.</p> <p>Example: For January, February, and March, enter 1, 2, 3</p> <p>To specify several consequent dates, enter their numbers separate by commas.</p> <p>Example: For 1st, 2nd and 3rd day of the month, enter 1, 2, 3</p>

Parameter	Description
<pre>recurrence weekly days <0-6> time <HH:MM></pre>	<p>Specifies that the job should run once a week - on specified days of week, and at specified time.</p> <p>Days of week are specified by numbers from 0 to 6:</p> <ul style="list-style-type: none"> ▪ Sunday = 0 ▪ Monday = 1 ▪ Tuesday = 2 ▪ Wednesday = 3 ▪ Thursday = 4 ▪ Friday = 5 ▪ Saturday = 6 <p>To specify several consequent days of a week, enter their numbers separate by commas. Example: For Sunday, Monday, and Tuesday, enter 0, 1, 2</p>
<pre>recurrence system-startup</pre>	<p>Specifies that the job should at every system startup.</p>
<pre>mailto <Email Address></pre>	<p>Specifies the email address, to which Gaia sends the jobs' results.</p> <p>Enter one email address for each command. You must also configure a mail server (see "Mail Notification" on page 353).</p>

Mail Notification

In This Section:

Introduction	353
Configuring Mail Notification in Gaia Portal	354
Configuring Mail Notification in Gaia Clish	355

Introduction

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

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

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


Gaia supports these mail notification features:

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

Gaia does not support these mail notification features:

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

Configuring Mail Notification in Gaia Portal

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

Step	Instructions
1	In the navigation tree, click System Management > Mail Notification .
2	In the Mail Server field, enter the IPv4 Address or Hostname of the mail server. For example: <code>mail.example.com</code>
3	In the User Name field, enter the user name. For example: <code>user@mail.example.com</code>
4	Click Apply .

Configuring Mail Notification in Gaia Clish

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

Description

Use this group of commands to configure mail notifications.

Syntax

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

```
set mail-notification server <IPv4 Address or Hostname>
```

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

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

- To show the configured mail server and user:

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

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

Parameters

Parameter	Description
<code>server <IPv4 Address or Hostname></code>	The IPv4 address or Hostname of the mail server, to which Gaia sends mail notifications. Example: mail.company.com
<code>username <User Name></code>	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	357
Configuring Messages in Gaia Portal	357
Configuring Messages in Gaia Clish	358
Limits	361

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

Comparison

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

Configuring Messages in Gaia Portal

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

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

Configuring Messages in Gaia Clish

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

Syntax for Banner message

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

```
show message banner status
```

```
show message all status
```

- To show the configured banner message:

```
show message banner
```

```
show message all
```

- To define a new single-line banner message:

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

See the **Limits** section below.

Example:

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

- To define a new multi-line banner message:

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

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

- To enable or disable the configured banner message:


```
set message banner on
```

```
set message banner off
```

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

1. Delete the user-defined banner message:

```
delete message banner
```

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

2. Disable the default banner:

```
set message banner off
```

Syntax for Message of the Day

- To show the configured message of the day:

```
show message motd
```

```
show message all
```

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

```
show message motd status
```

```
show message all status
```

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

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

See the **Limits** section below.

Example:

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

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

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

See the **Limits** section below.

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


```
set message motd on
```

```
set message motd off
```

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


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

```
delete message motd
```

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

2. Disable the default message of the day:

```
set message motd off
```

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

Limits

Message type	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	362
Configuring Display Format in Gaia Clish	363

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: <ul style="list-style-type: none"> ▪ 12-hour ▪ 24-hour
3	In Date , select one of these options: <ul style="list-style-type: none"> ▪ dd/mm/yyyy ▪ mm/dd/yyyy ▪ yyyy/mm/dd ▪ dd-mmm-yyyy
4	In IPv4 netmask , select one of these options: <ul style="list-style-type: none"> ▪ 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

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

Step	Instructions
1	In the navigation tree, click System Management > Session .
2	In the Command Line Shell section, configure the inactivity timeout for the Gaia Clish.
3	In the Web UI section, configure the inactivity timeout for the Gaia Portal. <ul style="list-style-type: none"> ▪ Range: 1 - 720 minutes ▪ Default: 10 minutes

Configuring the Session in Gaia Clish

i **Important:**

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

Syntax

- To configure the timeout:

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

- To show the configured timeout:

```
show inactivity-timeout
```

Parameters

Parameter	Description
<i><Timeout></i>	The inactivity timeout (in minutes) for the Gaia Clish. <ul style="list-style-type: none">▪ Range: 1 - 720 minutes▪ Default: 10 minutes

Crash Data

In This Section:


Introduction	366
Configuring Core Dumps in Gaia Portal	366
Configuring Core Dumps in Gaia Clish	368

Introduction


A process core dump file contains the recorded status of the working memory of the Gaia computer at the time that a Gaia process terminated abnormally.

When a process terminates abnormally, it produces a core dump file in the `/var/log/dump/usermode/` directory.

If the `/log` partition has less than 200 MB, Gaia OS does not create new core dump files and deletes the existing core dump files to get more free space. This prevents the core dump files from filling the `/log` partition.

 **Warning** - The core dump files may contain personal data. For more information, see [sk175504](#).

Configuring Core Dumps in Gaia Portal

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

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

Procedure

Step	Instructions
1	In the navigation tree, click System Management > Crash Data .
2	Select Enable Core Dumps and configure the parameters.
3	<p>In the Total space limit field, configure the maximum disk space to keep all core dump files.</p> <p>Gaia OS deletes the oldest core dump file if it requires disk space for a new core dump file.</p> <p>Gaia OS enforces the process limit before the space limit.</p> <ul style="list-style-type: none"> ▪ Range: 1 - 99999 MB ▪ Default: <ul style="list-style-type: none"> ◦ Management Server- 1000 MB ◦ Security Gateway in the Kernel Space Firewall (KSF) mode - 1000 MB ◦ Security Gateway in the User Space Firewall (USFW) mode - 10000 MB
4	<p>In the Dumps per process field, configure the maximum number of core dump files to keep for each process executable file.</p> <p>A new core dump file overwrites the oldest core dump file.</p> <p>Gaia OS enforces the process limit before the space limit.</p> <ul style="list-style-type: none"> ▪ Range: 1 - 99999 ▪ Default: 2 <p>Example</p> <p>There are two user space processes "A" and "B", and the limit is 2 core dump files for each process.</p> <p>Process "A" terminates 1 time, and process "B" terminates 3 times.</p> <p>Gaia OS keeps these core dumps:</p> <ul style="list-style-type: none"> ▪ 1 core dump for process "A" ▪ 2 core dumps for process "B" <p>Gaia OS deletes the core dump #3 for process "B" because of the process limit.</p>
5	Click Apply .

Configuring Core Dumps in Gaia Clish

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

Syntax

- To enable or disable core dump files:

```
set core-dump {enable | disable}
```

- To configure the total disk space limit for all core dump files (in MB):

```
set core-dump total <0-99999>
```

- To configure the number of core dump files for each process:

```
set core-dump per_process <0-99999>
```

- To show the status of this feature:

```
show core-dump status
```

- To show the configured total disk space limit:

```
show core-dump total
```

- To show the configured limit of core dump files for each process:

```
show core-dump per_process
```

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

Parameters

Parameter	Description
total <0-99999>	<p>The maximum disk space to keep all core dump files. Gaia OS deletes the oldest core dump file if it requires disk space for a new core dump file. Gaia OS enforces the process limit before the space limit.</p> <ul style="list-style-type: none"> ▪ Range: 1 - 99999 MB ▪ Default: <ul style="list-style-type: none"> ◦ Management Server - 1000 MB ◦ Security Gateway in the Kernel Space Firewall (KSF) mode - 1000 MB ◦ Security Gateway in the User Space Firewall (USFW) mode - 10000 MB
per_process <0-99999>	<p>The maximum number of core dump files to keep for each process executable file. A new core dump file overwrites the oldest core dump file. Gaia OS enforces the process limit before the space limit.</p> <ul style="list-style-type: none"> ▪ Range: 1 - 99999 ▪ Default: 2 <p>Example</p> <p>There are two user space processes "A" and "B", and the limit is 2 core dump files for each process. Process "A" terminates 1 time, and process "B" terminates 3 times. Gaia OS keeps these core dumps:</p> <ul style="list-style-type: none"> ▪ 1 core dump for process "A" ▪ 2 core dumps for process "B" <p>Gaia OS deletes the core dump #3 for process "B" because of the process limit.</p>

System Configuration

In This Section:

Configuring IPv6 Support in Gaia Portal	371
Configuring IPv6 Support in Gaia Clish	371

Important:

- R81.20 does **not** support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313).
- Multi-Domain Server 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 101 . To configure IPv6 static routes, see "IPv6 Static Routes" on page 256 .

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

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

Step	Instructions
1	With a web browser, connect to Gaia Portal at: <pre>https://<IP address of Gaia Management Interface></pre>
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. i Important - IPv6 support is not available until you reboot.

Configuring IPv6 Support in Gaia Clish

i Important:

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

- To configure IPv6 support:

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


i Important - This change requires reboot.

- To show the state of IPv6 support:

```
show ipv6-state
```

Procedure

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

Step	Instructions
3	On Scalable Platforms, go to Gaia gClish: Type <code>gclish</code> and press Enter.
4	Enable the IPv6 support: <pre>set ipv6-state on</pre>
5	Save the changes: <pre>save config</pre>
6	Reboot: <pre>reboot</pre>  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.



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

Configuring the System Logging

Step	Instructions
1	In the navigation tree, click System Management > System Logging .
2	In the System Logging section, select the applicable options: <ul style="list-style-type: none"> ▪ 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 "<code>set syslog cplogs {on off}</code>" 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 "<code>set syslog mgmtauditlogs {on off}</code>" command.

Step	Instructions
	<ul style="list-style-type: none"> ▪ 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 <code>/var/log/messages</code> file. Default: Selected To specify a Gaia configuration audit log file, run this command: <pre>set syslog filename /<Path>/<File></pre> <p>Note - This option is configured in the Gaia Clish with the "set syslog auditlog {disable permanent}" command.</p>
3	Click Apply .

Configuring the Remote System Logging

Step	Instructions
1	In the navigation tree, click System Management > System Logging .
2	In the Remote System Logging section, click Add .
3	In the IP Address field, enter the IPv4 address of the remote syslog server.
4	<p>In the Priority field, select the severity level of the logs that are sent to the remote server.</p> <p>These are the accepted values (as defined by the RFC 5424 - Section-6.2.1):</p> <ul style="list-style-type: none"> ▪ 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.

Editing the Remote System Logging settings

Step	Instructions
1	In the navigation tree, click System Management > System Logging .
2	In the Remote System Logging section, select the remote server.
3	Click Edit .
4	In the IP Address field, enter the IPv4 address of the remote syslog server.
5	In the Priority field, select the severity level of the logs that are sent to the remote server.
6	Click OK .

Deleting the Remote System Logging settings

Step	Instructions
1	In the navigation tree, click System Management > System Logging .
2	In the Remote System Logging section, select the remote syslog server.
3	Click Delete .
4	In the confirmation window, click Yes .

Syslog configuration files

By default, Gaia Operating System saves the Syslog configuration in these files:

- `/etc/rsyslog.conf`
- `/etc/sysconfig/rsyslog`

If it is necessary to add specific settings manually in these files (that Gaia OS does not have), then it is necessary to make these files immutable, so Gaia OS does not overwrite them:

1. Connect to the command line on Gaia OS.
2. Log in to the Expert mode.
3. Edit the applicable Syslog configuration file as required in your environment.
4. Examine the current attributes on the applicable configuration file you edited:

- `lsattr /etc/rsyslog.conf`
- `lsattr /etc/sysconfig/rsyslog`

5. Add the immutable attribute on the applicable configuration file you edited:


- `chattr +i /etc/rsyslog.conf`
- `chattr +i /etc/sysconfig/rsyslog`

6. Examine the current attributes on the applicable configuration file you edited:

- `lsattr /etc/rsyslog.conf`
- `lsattr /etc/sysconfig/rsyslog`

7. Restart the Syslog service:

```
service rsyslog restart
```

 **Warning** - While the Syslog configuration files are immutable:

- Gaia OS cannot save the changes in the Syslog configuration you make in Gaia Portal or Gaia Clish.
- Gaia OS cannot restore a Gaia Backup.

To remove the immutable attribute from a file, use this command:

```
chattr -i <file>
```

Configuring System Logging in Gaia Clish


Description

You can configure the System Logging and Remote System Logging.

System Logging configures the Gaia to send these logs:

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

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

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

 **Important:**

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

Syntax for System Logging configuration

- To send the Gaia system logs to a Check Point Management Server:

```
set syslog cplogs {on | off}
```

- To send the Gaia configuration audit logs to a Check Point Management Server:

```
set syslog mgmtauditlogs {on | off}
```

- To save the Gaia configuration audit logs:

```
set syslog auditlog {disable | permanent}
```

- To configure the file name of the Gaia configuration audit log:

```
set syslog filename /<Path>/<File>
```

- To show the Gaia system logging configuration:

```
show syslog
  all
  auditlog
  cplogs
  filename
  mgmtauditlogs
```

Syntax for Remote System Logging configuration

- To send Gaia system logs to a remote syslog server:

```
add syslog log-remote-address <IPv4 Address> level
<Severity>
```





- To show the Gaia system logging configuration:




```
show syslog
  all
  log-remote-address <IPv4 Address>
  log-remote-addresses
```

- To stop sending Gaia system logs to the specific remote server:

```
delete syslog log-remote-address <IPv4 Address> [level
<Severity>]
```

CLI Parameters

Parameter	Description
<code>cplogs {on off}</code>	<p>Specifies if the Gaia sends the Gaia system logs to a Check Point Management Server:</p> <ul style="list-style-type: none"> ▪ <code>on</code> - Send Gaia system syslogs ▪ <code>off</code> - Do not send Gaia syslogs <p>Default: <code>off</code></p> <p> Note - This command corresponds to the Send Syslog messages to management server option in the Gaia Portal > System Management > System Logging.</p>
<code>mgmtauditlogs {on off}</code>	<p>Specifies if the Gaia sends the Gaia audit logs (for configuration changes that authorized users make) to a Check Point Management Server:</p> <ul style="list-style-type: none"> ▪ <code>on</code> - Send Gaia audit logs ▪ <code>off</code> - Do not send Gaia audit logs <p>Default: <code>on</code></p> <p> Note - This command corresponds to the Send audit logs to management server upon successful configuration option in the Gaia Portal > System Management > System Logging.</p>
<code>auditlog {disable permanent}</code>	<p>Specifies if the Gaia saves the logs for configuration changes that authorized users make:</p> <ul style="list-style-type: none"> ▪ <code>disable</code> - Disables the Gaia audit log facility ▪ <code>permanent</code> - Enables the Gaia audit log facility to save information about all successful changes in the Gaia configuration. To specify a destination file, run the <code>set syslog filename </Path/File></code> command (otherwise, Gaia uses the default <code>/var/log/messages</code> file). <p>Default: <code>permanent</code></p> <p> Note - This command corresponds to the Send audit logs to syslog upon successful configuration option in the Gaia Portal > System Management > System Logging.</p>
<code></Path>/<File></code>	<p>Configures the full path and file name of the system log.</p> <p>Default: <code>/var/log/messages</code></p> <p> Note in Gaia Portal does not let you configure this setting.</p>

Parameter	Description
log-remote-address	<p>Configures Gaia to send system logs to a remote syslog server.</p> <ul style="list-style-type: none">  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>	<p>IPv4 address of the remote syslog server, to which Gaia sends its system logs.</p> <ul style="list-style-type: none"> ▪ Range: Dotted-quad ([0-255].[0-255].[0-255].[0-255]) ▪ Default: No default value
<Severity>	<p>Syslog severity level for the system logging. These are the accepted values (as defined by the RFC 5424 - Section-6.2.1):</p> <ul style="list-style-type: none"> ▪ <code>emerg</code> - System is unusable ▪ <code>alert</code> - Action must be taken immediately ▪ <code>crit</code> - Critical conditions ▪ <code>err</code> - Error conditions ▪ <code>warning</code> - Warning conditions ▪ <code>notice</code> - Normal but significant condition ▪ <code>info</code> - Informational messages ▪ <code>debug</code> - Debug-level messages ▪ <code>all</code> - All messages <p> Notes:</p> <ul style="list-style-type: none"> ▪ 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 Operating System saves the Syslog configuration in these files:

- /etc/rsyslog.conf
- /etc/sysconfig/rsyslog

If it is necessary to add specific settings manually in these files (that Gaia OS does not have), then it is necessary to make these files immutable, so Gaia OS does not overwrite them:

1. Connect to the command line on Gaia OS.
2. Log in to the Expert mode.
3. Edit the applicable Syslog configuration file as required in your environment.
4. Examine the current attributes on the applicable configuration file you edited:
 - `lsattr /etc/rsyslog.conf`
 - `lsattr /etc/sysconfig/rsyslog`
5. Add the immutable attribute on the applicable configuration file you edited:


- `chattr +i /etc/rsyslog.conf`
- `chattr +i /etc/sysconfig/rsyslog`

6. Examine the current attributes on the applicable configuration file you edited:

- `lsattr /etc/rsyslog.conf`
- `lsattr /etc/sysconfig/rsyslog`

7. Restart the Syslog service:

```
service rsyslog restart
```

 **Warning** - While the Syslog configuration files are immutable:


- Gaia OS cannot save the changes in the Syslog configuration you make in Gaia Portal or Gaia Clish.
- Gaia OS cannot restore a Gaia Backup.

To remove the immutable attribute from a file, use this command:

```
chattr -i <file>
```

Redirecting Routed System Logging Messages

It is possible to configure the Routed daemon to write its log messages (for example, OSPF or BGP errors) to one of these log files:

Log File	Description
<code>/var/log/routed_messages</code>	Dedicated file that contains only the Routed log messages. In Gaia versions R80 and higher, the Routed writes to this file by default.
<code>/var/log/messages</code>	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.  Best Practice - Configure the Routed to write its log messages to the <code>/var/log/routed_messages</code> 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

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

Step	Instructions
1	From the left navigation tree, click Advanced Routing > Routing Options .
2	In the Routing Process Message Logging Options section, select Log Routed Separately .
3	<p>In the Maximum File Size field, enter the size (in megabytes) for each log file. The default size is 1 MB.</p> <p>When the active log file <code>/var/log/routed_messages</code> reaches the maximal configured size, the Gaia OS rotates it and creates the new <code>/var/log/routed_messages</code> file.</p>
4	<p>In the Maximum Number of Files field, enter the maximal number of log files to keep.</p> <p>The default is to keep 10 log files:</p> <ul style="list-style-type: none"> ■ <code>/var/log/routed_messages</code> ■ <code>/var/log/routed_messages.0</code> ■ <code>/var/log/routed_messages.1</code> ■ ... ■ <code>/var/log/routed_messages.9</code> <p>If the number of all log files reaches the maximal configured number, the Gaia OS deletes the oldest file, and rotates the existing files.</p> <p>The file names end with a number suffix. The greater the suffix number, the older the file.</p>
5	Click Apply .

Configuration in Gaia Clish

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

Step	Instructions
1	Connect to the command line on Gaia.
2	Log in to Gaia Clish.
3	On Scalable Platforms, go to Gaia gClish: Type <code>gclish</code> and press Enter.
4	Enable the logging of RoutedD messages to a dedicated log file: <pre>set routedsyslog on</pre>
5	Configure the size (in megabytes) for each log file: <pre>set routedsyslog size <Number of MB between 1 and 2047></pre> The default size is 1 MB. When the active log file <code>/var/log/routed_messages</code> reaches the maximal configured size, the Gaia OS rotates it and creates the new <code>/var/log/routed_messages</code> file.
6	Configure the maximal number of log files to keep: <pre>set routedsyslog maxnum <Number of Files between 1 and 4294967295></pre> The default is to keep 10 log files: <ul style="list-style-type: none"> ■ <code>/var/log/routed_messages</code> ■ <code>/var/log/routed_messages.0</code> ■ <code>/var/log/routed_messages.1</code> ■ ... ■ <code>/var/log/routed_messages.9</code> 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.
7	Save the configuration: <pre>save config</pre>

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	<ul style="list-style-type: none"> ▪ If default values were used for "maxnum" and "size": <pre>set routedsyslog on</pre> ▪ If custom values were configured for "maxnum" and "size": <pre>set routedsyslog on set routedsyslog maxnum <Configured_Value> set routedsyslog size <Configured_Value></pre>
Expert mode	grep routedsyslog /config/active	<ul style="list-style-type: none"> ▪ If default values were used for "maxnum" and "size": <pre>routed:instance:default:routedsyslog t</pre> ▪ If custom values were configured for "maxnum" and "size": <pre>routed:instance:default:routedsyslog t routed:instance:default:routedsyslog:size e <Configured_Value> routed:instance:default:routedsyslog:fil es <Configured_Value></pre>

Important:

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

Configuring Log Volume

If there is enough available disk space, you can increase the size of the log partition.


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

 **Important:**

Before you change the size of the log partition, take the Gaia snapshot and export it to an external storage. See "[Snapshot Management](#)" on page 545.

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

Use the `lvm_manager` tool in the Expert mode.

Step	Instructions
1	Connect to the Gaia system through the console port .
2	Reboot: <input type="text" value="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 <code>lvm_manager</code> tool as described in the sk95566 : <input type="text" value="lvm_manager"/>
7	Reboot: <input type="text" value="reboot"/>

Related information

See "[LVM Overview](#)" on page 624.

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

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

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

Configuring Telnet Access in Gaia Clish

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

Syntax

- To configure Telnet access:

```
set net-access telnet {on | off}
```

- To show the configured Telnet access:


```
show net-access telnet
```

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

Host Access

You can configure hosts or networks that are allowed to connect to the Gaia Portal or Gaia Clish.

Configuring Allowed Gaia Clients in Gaia Portal

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

Step	Instructions
1	In the navigation tree, click System Management > Host Access .
2	Click Add . The Add a New Allowed Client window opens.
3	Select one of these options: <ul style="list-style-type: none">▪ 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

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

Syntax

- To add an allowed client:

```
add allowed-client
    host
        any-host
            ipv4-address <Host IPv4 Address>
        network ipv4-address <Network IPv4 Address> mask-length
            <1-31>
```

- To show the configured allowed clients:

```
show allowed-client all
```

- To delete an allowed client:

```
delete allowed-client
    host
        any-host
            host ipv4-address <Host IPv4 Address>
        network ipv4-address <Network IPv4 Address>
```

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


Parameters

Parameter	Description
<Host IPv4 Address>	The IPv4 address of the allowed host in dotted decimal format (X.X.X.X)
<Network IPv4 Address>	The IPv4 address of the allowed network in dotted decimal format (X.X.X.X)

Example

```
gaia> add allowed-client host any-host
gaia> show allowed-client all
Type                Address
Mask Length
Host                Any
gaia>
```


LLDP

 **Important** - Scalable Platforms (Maestro and Chassis) do **not** support this feature (Known Limitation MBS-10753).

You can configure Gaia to advertise and receive information from other network devices over the Link Layer Discovery Protocol (LLDP) protocol.

The LLDP is a vendor-neutral link layer protocol that network devices use to advertise their identity, capabilities (and so on) and to receive information about their neighbors on a local area network based on IEEE 802 standard.


The gathered information may include:

- System Name
- System Description
- System Capabilities (switching, routing, etc.)
- Port Description
- Management Address

 **Important** - By default, LLDP is *disabled* in the Gaia operating system.

Configuring LLDP in Gaia Portal

Step	Instructions
1	In the navigation tree, click System Management > LLDP .

Step	Instructions
2	<p>In the Type Length Value (TLV) section, select which information to send in the LLDP packets, and click Apply:</p> <ul style="list-style-type: none"> ▪ System Name To send the Gaia "<i><Hostname>.<Domainname></i>". Note - To configure the domain name, see "System Name" on page 235. ▪ System Description To send the formatted output of the "<code>uname -msr</code>" command (which contains kernel name, kernel release, and kernel machine hardware name). ▪ System Capabilities To send the string "<code>station</code>" (regardless of the Check Point configuration). ▪ Port Description To send the name of the interface. ▪ Management Address <ul style="list-style-type: none"> • Select Send Management interface IP to send the IP address of the Gaia Management interface only. • Send Configured interface IP to send the IP address of each selected interface.
3	<p>In the Timers section, configure the applicable values, and click Apply:</p> <ul style="list-style-type: none"> ▪ Transmit Interval This interval controls how frequently Gaia To send LLDP packets on the selected interfaces. Enter a value between 8 and 32768 (default is 30) seconds. ▪ Hold Time Multiplier This multiplier controls the Time-to Live (TTL) of the LLDP packets: TTL = (Transmit Interval) x (Hold Time Multiplier). This TTL is the duration, for which the receiving neighbor stores the LLDP information in its database. Enter a value between 2 and 10 (default is 4). <p> Note - These values are global and apply to all selected interfaces.</p>


Step	Instructions
4	<p>In the Interfaces section, add the applicable interfaces.</p> <ul style="list-style-type: none"> ■ To add all configured interfaces: <ul style="list-style-type: none"> a. Click Add All. b. Click Yes to confirm. c. The default LLDP mode for all interfaces is Transmit and Receive. To change the LLDP mode: <ul style="list-style-type: none"> i. Select an interface. ii. Click Edit. iii. Select the applicable LLDP mode. iv. Click Save. ■ To add a specific interface: <ul style="list-style-type: none"> a. Click Add. b. In the Interface Name field, select an interface. c. In the Mode field, select the applicable LLDP mode. d. Click Save. <p>The available LLDP modes are:</p> <ul style="list-style-type: none"> ■ Transmit and Receive - The interface transmits and receives the LLDP packets. ■ Transmit only - The interface only transmits the LLDP packets, but does not receive the LLDP packets. ■ Receive only - The interface only receives the LLDP packets, but does not transmit the LLDP packets.
5	<p>In the LLDP Configuration section, select Enable LLDP, and click Apply.</p>

Configuring LLDP in Gaia Clish

Syntax

- To configure LLDP:

```
set lldp
  hold-time-multiplier <2-10>
  interface <Name of Interface>
    receive {on | off}
    transmit {on | off}
    transmit-and-receive {on | off}
  state {on | off}
  tlv
    port-description {on | off}
    system-name {on | off}
    system-description {on | off}
    system-capabilities {on | off}
    management-address {on from {configured-interface
| mgmt-interface} | off}
    transmit-interval <8-32768>
```

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

- To show the LLDP configuration:

```
show lldp status
  interface <Name of Interface>
  timers
  tlv
```

Parameters

Parameter	Description
<code>hold-time-multiplier</code>	This multiplier controls the Time-to Live (TTL) of the LLDP packets: TTL = (Transmit Interval) x (Hold Time Multiplier). This TTL is the duration, for which the receiving neighbor stores the LLDP information in its database. Enter a value between 2 and 10 (default is 4).
<code>interface <Name of Interface></code>	Specifies the name of an interface, which sends or receives the LLDP packets.
<code>interface <Name of Interface> receive {on off}</code>	Enables (<code>on</code>) and disables (<code>off</code>) the LLDP mode on the interface as "receive only". The interface only receives the LLDP packets, but does not transmit the LLDP packets.
<code>interface <Name of Interface> transmit {on off}</code>	Enables (<code>on</code>) and disables (<code>off</code>) the LLDP mode on the interface as "transmit only". The interface only transmits the LLDP packets, but does not receive the LLDP packets.
<code>interface <Name of Interface> transmit-and-receive {on off}</code>	Enables (<code>on</code>) and disables (<code>off</code>) the LLDP mode on the interface as "transmit and receive". The interface transmits and receives the LLDP packets.
<code>state {on off}</code>	Enables (<code>on</code>) and disables (<code>off</code>) the LLDP on the specified interface.
<code>tlv port-description {on off}</code>	Enables (<code>on</code>) and disables (<code>off</code>) the LLDP-enabled interface to send the Port Description information in the LLDP packets. Sends the name of the interface.
<code>tlv system-name {on off}</code>	Enables (<code>on</code>) and disables (<code>off</code>) the LLDP-enabled interface to send the System Name information in the LLDP packets. Sends the Gaia " <code><Hostname>.<Domainname></code> ". Note - To configure the domain name, see " System Name " on page 235.

Parameter	Description
<pre>tlv system-description {on off}</pre>	<p>Enables (on) and disables (off) the LLDP-enabled interface to send the System Description information in the LLDP packets.</p> <p>Sends the formatted output of the "uname -msr" command (which contains kernel name, kernel release, and kernel machine hardware name).</p>
<pre>tlv system-capabilities {on off}</pre>	<p>Enables (on) and disables (off) the LLDP-enabled interface to send the System Capabilities information in the LLDP packets.</p> <p>Sends the string "station" (regardless of the Check Point configuration).</p>
<pre>tlv management-address {on off}</pre>	<p>Enables (on) and disables (off) the LLDP-enabled interface to send the Management Address information in the LLDP packets.</p> <ul style="list-style-type: none"> ▪ from <code>mgmt-interface</code> - Sends the IP address of the Gaia Management interface only. ▪ from <code>configured-interface</code> - Sends the IP address of each LLDP-enabled interface.
<pre>transmit-interval <8-32768></pre>	<p>This interval controls how frequently the LLDP-enabled interface sends the LLDP packets. Enter a value between 8 and 32768 (default is 30) seconds.</p>
<pre>timers</pre>	<p>Shows the configured LLDP timers:</p> <ul style="list-style-type: none"> ▪ Hold Time Multiplier ▪ Transmit Interval

Example - Viewing the LLDP status

```
MyGaia> show lldp status
LLDP server  enabled
Interfaces
eth0 - receive
eth1 - receive and transmit
eth2 - transmit
Optional Information
port-description off
system-name on
system-description off
system-capabilities on
management-address on
Timers
Hold time multiplier 5
Transmit interval 20
MyGaia>
```

Viewing the LLDP neighbors in the Expert mode

1. Connect to the command line on Gaia.
2. Log in to the Expert mode.
3. Run:

```
lldpneighbors
```

Example output

```
[Expert@MyGaia:0]# lldpneighbors
Read 512 bytes. Total size is now: 512
Buffer is: 0xFFADB704 and Temporary Buffer is 0xFFADB700.
Read 282 bytes. Total size is now: 794
Buffer is: 0xFFADB704 and Temporary Buffer is 0xFFADB700.

OpenLLDP Neighbor Info:

Interface 'eth0' has 0 LLDP Neighbors:

Interface 'eth1' has 2 LLDP Neighbors:

Neighbor 1:
    Chassis ID:          MA
    Port ID:             Interface Name - eth0
    Time To Live:       120 seconds
    End Of LLDPDU:

Neighbor 2:
    Chassis ID:          MA
    Port ID:             Locally Assigned - Eth1/37
    Time To Live:       120 seconds
    Port Description:   Ethernet1/37
    System Name:        SecureOsLabFL6ApplianceSwitch.SecreOS_LAB6
    System Description: Cisco Nexus Operating System (NX-OS) Software
                        TAC support: http://www.cisco.com/tac
                        Copyright (c) 2002-20XX, Cisco Systems, Inc. All rights
reserved.
    System Capabiltiies: Bridge/Switch (disabled)
                        Router (enabled)
    Management Address: IPv4 - 172.23.95.1 (ifIndex - 83886080) (OID: Standard LLDP
MIB)
    Organizationally Specific:
    End Of LLDPDU:

[Expert@MyGaia:0]#
```


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 [R81.20 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

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

Step	Instructions
1	In the navigation tree, click User Management > 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

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

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 / Gaia gClish by default.


You must assign one or more roles before the new users can log in.




Notes:

- You can assign permissions to all Gaia features or a subset of the features without assigning a user ID of 0.
If you assign a user ID of 0 to a user account (you can do this only in the Gaia Clish), the user is equivalent to the Admin user and the roles assigned to that account cannot be modified.
- Do not define a new user for external users.
An external user is one that is defined on an authentication server (such as RADIUS or TACACS), and not on the local Gaia system.

When you create a user, you can add pre-defined roles (privileges) to the user. For more information, see ["Roles" on page 415](#).

 **Warning** - A user with read and write permission to the Users feature can change the password of another user, or an admin user. Therefore, write permission to the Users feature should be assigned with caution.

Managing User Accounts in Gaia Portal


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


Viewing the list of all configured users

In the navigation tree, click **User Management > Users**.

You can also see your username in the top right corner of the Gaia Portal.

Adding a new user

Step	Instructions
1	In the navigation tree, click User Management > Users .
2	Click Add .
3	In the Login Name field, enter the username. 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.

Step	Instructions
9	<p>Select User must change password at next logon, if you wish to force the user to change the configured password during the next login.</p> <p> 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.</p>
10	<p>Optional: In the UID field, enter or select the applicable User ID:</p> <ul style="list-style-type: none"> ▪ 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 <code>/usr/bin/scponly</code> - see sk88981)
11*	<p>In the Access Mechanisms section:</p> <ul style="list-style-type: none"> ▪ Select Web to allow this user to access Gaia Portal. ▪ Select Clish Access to allow this user to access Gaia Clish. ▪ Select Gaia API to allow this user to access Gaia RESTful API (see Check Point Gaia API Reference).
12*	<p>In the Available Roles list:</p> <ol style="list-style-type: none"> a. Select the roles you wish to assign to this user. To select several roles: <ol style="list-style-type: none"> 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 420](#).


Login Shells

Shell	Description
/etc/cli.sh	<p>This is the default option.</p> <p>Lets the user work with the full Gaia Clish.</p> <p>By default, some basic networking commands (such as <code>ping</code>) are also available.</p> <p>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 446).</p> <p>User can run the <code>expert</code> command to enter the Bash shell (Expert mode).</p>
/bin/bash	<p>BASH Linux shell.</p> <p>Lets the user work with the Expert mode.</p> <p>User can run the <code>clish</code> command to enter the Gaia Clish.</p>
/bin/csh	<p>CSH Linux shell.</p> <p>User can run the <code>clish</code> command to enter the Gaia Clish.</p>
/bin/sh	<p>SH Linux shell.</p> <p>User can run the <code>clish</code> command to enter the Gaia Clish.</p>
/bin/tcsh	<p>TCSH Linux shell.</p> <p>User can run the <code>clish</code> command to enter the Gaia Clish.</p>
/usr/bin/scponly	<p>User is not allowed to log in to Gaia.</p> <p>User can only connect to Gaia over SCP and transfer files to and from the system.</p> <p>Other commands are forbidden.</p>
/sbin/nologin	<p>User is not allowed to log in to Gaia.</p>

Changing the user configuration

Step	Instructions
1	In the navigation tree, click User Management > Users .
2	Select the user.
3	Click Edit .
4	In the Real Name field, enter the user's real name or other informative text.

Step	Instructions
5	In the Home Directory field, enter the user's home directory.
6	In the Shell field, select the user's default login shell.
7	Select User must change password at next logon , if you wish to force the user to change the configured password during the next login.
8	In the Available Roles list, select the roles you wish to assign to this user and click Add > .
9	In the Assigned Roles list, select the roles you wish to remove from this user and click Remove > .
10	Click OK .

 **Note** - For the default users **admin** and **monitor**, you can only change the Shell and Roles.

Deleting a user


Step	Instructions
1	In the navigation tree, click User Management > Users .
2	Select the user.
3	Click Delete .
4	Click OK to confirm.

 **Note** - You cannot delete the default users **admin** and **monitor**.

Managing User Accounts in Gaia Clish

Important:

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

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

Syntax

Adding a local user account


```
add user <UserName> uid <User ID> homedir <Path>
```

Adding a RADIUS user account

```
add user <UserName> uid 0 homedir <Path>
```

Editing a user account

```
set user <UserName>
    force-password-change {yes | no}
    gid <System Group ID>
    homedir <Path>
    lock-out off
    newpass <Password>
    password
    password-hash <Password Hash>
    realname <Name>
    shell <Login Shell>
    uid <User ID>
```

 **Note** - For the default users **admin** and **monitor**, you can only change the Shell and Roles.

Viewing the summary information about all users

```
show users
```

Viewing information about a specific user

```
show user <UserName>
    [force-password-change]
    [gid]
    [homedir]
    [lock-out]
    [realname]
    [shell]
    [uid]
```

Deleting a configured user


```
delete user <User ID>
```





Note - You cannot delete the default users **admin** and **monitor**.

Parameters**CLI Parameters**

Parameter	Description
<pre>user <UserName></pre>	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 - _
<pre>uid <User ID></pre>	<p>Optional. Configures unique User ID to identify permissions of the user:</p> <ul style="list-style-type: none"> ▪ 0 for administrator users and RADIUS user account (this is the default option) ▪ An integer between 103 and 65533 for non-administrator user <p> Notes:</p> <ul style="list-style-type: none"> • Configure this UID for users with the default shell <code>/usr/bin/scponly</code> - see sk88981. • If you do not enter a value, Gaia OS automatically assigns the next free sequential number.
<pre>homedir <Path></pre>	<p>Configures user's home directory.</p> <p>This is the full Linux path name of a directory, to which the user will log in.</p> <p>Must be a sub-directory of the <code>/home/</code> directory.</p> <p>If the sub-directory does not already exist, it is created.</p>

Parameter	Description
force- password- change {yes no}	<p>If you wish to force the user to change the configured password during the next login, use the value "yes".</p> <p> 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.</p>
gid <System Group ID>	<p>Configures System Group ID (0-65535) for the primary group, to which a user belongs.</p> <p>The default is 100.</p> <p>You can add the user to several groups.</p> <p>Use the "add group" and "set group" commands to manage the groups.</p>
lock-out off	<p>Unlocks the user, if the user was locked out.</p> <p>The password expiration date is adjusted, if necessary.</p>
newpass <Password>	<p>Configures a new password for the user.</p> <p>Gaia does not ask to verify the new password.</p> <p>The password you enter shows on the terminal command line in plain text, and is stored in the command history as plain text.</p>
password	<p>Configures a password for the new user.</p> <p>The command runs in interactive mode.</p> <p>You must enter the password twice, to verify it.</p> <p>The password you enter is not visible on the terminal command line.</p>

Parameter	Description
password-hash <Password Hash>	<p>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: <code>cpopenssl passwd -help</code>). To configure the default hash algorithm, see:</p> <ul style="list-style-type: none"> ▪ "Password Hashing Algorithm" on page 459 (in Gaia Portal) ▪ "Configuring Hashing Algorithm" on page 468 (in Gaia Clish) <p> Best Practice - Do not use MD5 hash because it is not secure.</p> <p> Notes:</p> <ul style="list-style-type: none"> ▪ Format: <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <code>\$<Hash Standard>\$<Salt>\$<Encrypted></code> </div> ▪ The length of this hash string must be less than 128 characters. ▪ <Hash Standard> One of these digits: <ul style="list-style-type: none"> • 1 = MD5 • 5 = SHA256 • 6 = SHA512 ▪ <Salt> A string of these characters: <code>a-z A-Z 0-9 . / [] _ ` ^</code> The length of this string must be between 2 and 16 characters. ▪ <Encrypted> A string of these characters: <code>a-z A-Z 0-9 . / [] _ ` ^</code> The length of this string must be: <ul style="list-style-type: none"> • For MD5, less than 22 characters. • For SHA256, less than 43 characters. • For SHA512, less than 86 characters.
realname <Name>	<p>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.</p>
shell <Login Shell>	<p>Configures the user's default login shell. See the explanations in the "Login Shells" section below.</p>


Login Shells

Shell	Description
/etc/cli.sh	<p>This is the default option.</p> <p>Lets the user work with the full Gaia Clish.</p> <p>By default, some basic networking commands (such as <code>ping</code>) are also available.</p> <p>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 446).</p> <p>User can run the <code>expert</code> command to enter the Bash shell (Expert mode).</p>
/bin/bash	<p>BASH Linux shell.</p> <p>Lets the user work with the Expert mode.</p> <p>User can run the <code>clish</code> command to enter the Gaia Clish.</p>
/bin/csh	<p>CSH Linux shell.</p> <p>User can run the <code>clish</code> command to enter the Gaia Clish.</p>
/bin/sh	<p>SH Linux shell.</p> <p>User can run the <code>clish</code> command to enter the Gaia Clish.</p>
/bin/tcsh	<p>TCSH Linux shell.</p> <p>User can run the <code>clish</code> command to enter the Gaia Clish.</p>
/usr/bin/scponly	<p>User is not allowed to log in to Gaia.</p> <p>User can only connect to Gaia over SCP and transfer files to and from the system.</p> <p>Other commands are forbidden.</p>
/sbin/nologin	<p>User is not allowed to log in to Gaia.</p>

Roles

Role-based administration (RBA) lets you create administrative roles for users. With RBA, an administrator can allow Gaia users to access specified features by including those features in a role and assigning that role to users. Each role can include a combination of administrative (read/write) access to some features, monitoring (read-only) access to other features, and no access to other features.

You can also specify which access mechanisms (Gaia Portal, or Gaia Clish) are available to the user.

 **Note** - When users log in to the Gaia Portal, they see only those features to which they have read-only or read/write access. If they have read-only access to a feature, they can see the settings pages, but cannot change the settings.

Gaia includes these predefined roles:

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


 **Notes:**

- You **cannot** delete or change the predefined roles.
- Do **not** define a new user for external users.
An external user is one that is defined on an authentication server (such as RADIUS or TACACS), and not on the local Gaia system.


Configuring Roles in Gaia Portal

You define roles on the **User Management > Roles** page of the Gaia Portal.

This page also shows a list of existing roles.


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

Adding a new role

Step	Instructions
1	In the navigation tree, click User Management > Roles .
2	Click Add .
3	In the Role Name field, enter the applicable name. 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 425.
5	On the Extended Commands tab: Select the commands you wish to configure in this role. <ul style="list-style-type: none"> ▪ To select several commands: <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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 446.

Step	Instructions
6	Click OK .

Changing features and commands in the existing role

Step	Instructions
1	In the navigation tree, click User Management > Roles .
2	Select the role.
3	Click Edit .
4	<p>On the Features tab:</p> <p>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.</p> <p> 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!</p>
5	<p>On the Extended Commands tab:</p> <p>Select the commands you wish to configure in this role.</p> <ul style="list-style-type: none"> ▪ To select several commands: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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 .

Deleting a role

Step	Instructions
1	In the navigation tree, click User Management > Roles .
2	Select the role.
3	Click Delete .
4	Click OK to confirm.




Note - You cannot delete the default roles **adminRole** and **monitorRole**.

Assigning users to a role

Step	Instructions
1	In the navigation tree, click User Management > Roles .
2	Select the role.
3	Click Assign Members .
4	In the Available Users list, left-click the user you wish to add to the role. To select several users: <ol style="list-style-type: none"> 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 .

Removing users from a role

Step	Instructions
1	In the navigation tree, click User Management > Roles .
2	Select the role.
3	Click Assign Members .
4	In the Users with Role list, left-click the user you wish to remove from the role. To select several users: <ol style="list-style-type: none">Press and hold the CTRL key on the keyboard.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 404](#)).

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.

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

Syntax

Adding an RBA role

```
add rba role <New Role Name> domain-type System
    all-features
    readonly-features <List of RO Features>
    readwrite-features <List of RW Features>}
```

i **Note** - You can add "readonly-features" and "readwrite-features" in the same command.

Choosing which VSX Virtual Systems this role can access

```
add rba role <Existing Role Name>
    virtual-system-access 0
    virtual-system-access all
    virtual-system-access VSID1, VSID2, ..., VSIDn
```

Assigning Gaia access mechanisms to a user

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

Assigning an RBA role to a user

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

Viewing the RBA roles information


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

Deleting an entire RBA role

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

Deleting features from an RBA role

```
delete rba role <Role Name>
  readonly-features <List of RO Features>
  readwrite-features <List of RW Features>
```


 **Note** - You can delete "readonly-features" and "readwrite-features" in the same command.

Removing Gaia access mechanisms from a user

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

Removing an RBA role from a user

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



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



Notes:

- There are no "set" commands for configured roles.
- You cannot delete the default roles **adminRole** or **monitorRole**.

Parameters

CLI Parameters

Parameter	Description
<code>role <Role Name></code>	Role name as a character string that contains letters, numbers or the underscore (_) character. The role name must start with a letter.
<code>domain-type System</code>	Reserved for future use.
<code>virtual-system-access {0 all VSID1, VSID2, ..., VSIDn}</code>	Specifies which VSX Virtual Systems this role can access: <ul style="list-style-type: none"> 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).
<code>all-features</code>	Grants read-write permissions to all features. <p> Important - This is equivalent to the admin role!</p>
<code>readonly-features <List of RO Features></code>	A comma-separated list of Gaia features that have read-only permissions in the specified role. See: <ul style="list-style-type: none"> "List of Available Features in Roles" on page 425 "List of Available Extended Commands in Roles" on page 446 <p> Notes:</p> <ul style="list-style-type: none"> 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
<pre>readwrite-features <List of RW Features></pre>	<p>A comma-separated list of Gaia features that have read-write permissions in the specified role.</p> <p>See:</p> <ul style="list-style-type: none"> ▪ "List of Available Features in Roles" on page 425 ▪ "List of Available Extended Commands in Roles" on page 446 <p> Notes:</p> <ul style="list-style-type: none"> ▪ 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. <p> 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!</p>
<pre>user <User Name></pre>	<p>User, to which access mechanism permissions and roles are assigned.*</p>
<pre>roles < Role1 ,Role2, ..., RoleN></pre>	<p>Comma-separated list of role names that are assigned to or removed from the specified user (spaces are not allowed in this syntax).*</p>
<pre>access-mechanisms {Web-UI CLI Web- UI,CLI Gaia-API}</pre>	<p>Defines the access mechanisms that users can work with to manage Gaia:*</p> <ul style="list-style-type: none"> ▪ 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) ▪ Gaia-API - Access only to Gaia RESTful API (see Check Point Gaia API Reference)

* To configure these settings in Gaia Portal, see ["Managing User Accounts in Gaia Portal" on page 406](#).

Example

```
gaia> add rba role NewRole domain-type System readonly-features vpn,ospf,rba readwrite-features snmp

gaia> show rba role NewRole
Role
  NewRole
  domain-type System
  read-write-feature snmp
  read-only-feature vpn,ospf,rba
gaia>

gaia> add rba user John roles NewRole

gaia> add rba user John access-mechanisms Web-UI,CLI

gaia> show rba user John
User
  John
  access-mechanism CLI
  access-mechanism Web-UI
  role NewRole
gaia>

gaia> delete rba user John roles NewRole

gaia> delete rba role NewRole
```


List of Available Features in Roles

Important:

- Read the Known Limitations for R81.20 in [sk174965](#).
- Read the Known Limitations for Scalable Platforms in [sk148074](#).

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.	<pre>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 *</pre>
Advanced VRRP	adv-vrrp	Configure the Advanced Virtual Router Redundancy Protocol (VRRP)	<pre>set vrrp * show vrrp *</pre>
Appliance Maintenance	prod-maintain	Overview page for Appliance Maintenance.	
ARP	arp	Control static ARP entries and proxy ARP entries. Control dynamic ARP entries.	<pre>add arp * delete arp * set arp * show arp *</pre>

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
Banner Messages	message	Control Banner Message and Message of the Day.	set message * delete message * show message *
BGP	bgp	Configure dynamic routing through the Border Gateway Protocol (BGP).	set as * set router-id * set bgp * show route bgp * show as * show router-id * show bgp *
Blades Summary	blades	Show summary for enabled Software Blades.	
cdt	cdt	Central Deployment Tool	show cdt * set cdt * start cdt *
Certificate Authority	certificate_authority	Control Certificate Authority.	cpca_client
Change My Password	selfpasswd	Change your user account password.	set selfpasswd *
Cloning Group	CloningGroup	Control Gaia Cloning Groups.	set cloning-group * add cloning-group * delete cloning-group * join cloning-group * re-synch cloning-group * leave cloning-group * show cloning-group *

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
Cloning Group Management	CloningGroupManagement	Control management of Gaia Cloning Groups.	set cloning-group-management *
Cloud Config	cloud-config	Control of Zero Touch.	show cloud-config * set cloud-config * delete cloud-config *
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 *

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
DHCP Server	dhcp	Control DHCP Server on Gaia.	<pre> 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 *</pre>
DHCPv6 Relay	dhcp6relay	Control Relay of DHCPv6 messages between DHCP clients and DHCP servers on different IPv6 Network.	<pre> set ipv6 dhcp6relay * show ipv6 dhcp6relay *</pre>
Display Configuration	configuration	Save and show Gaia configuration.	<pre> save configuration * show configuration *</pre>
Display Format	format	Control how the system displays time, date and netmask.	<pre> set format * show format *</pre>
DNS	dns	Control DNS servers on Gaia.	<pre> set dns * delete dns * show dns *</pre>

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
Domain Name	domainname	Control the domain name on Gaia.	set domainname * delete domainname show domainname
Download SmartConsole	smart-console	Download SmartConsole from Gaia Portal.	N/A
Expert Mode	expert	Access to the Expert mode shell.	expert
Expert Password	expert-password	Change the Expert mode password (interactive).	set expert-password
Expert Password Hash	expert-password-hash	Change the Expert mode password using password hash.	set expert-password-hash *
Extended Commands	command	Control the ability to define additional Extended Commands for the Gaia Clish.	add command * delete command * show command * show commands show extended *
Factory Defaults	fcd	Restore Gaia OS to Factory Defaults.	set fcd * show fcd *

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
Firewall Management	firewall_management	Control Login and Logout from Management Server.	mgmt *
Front Panel	lcd	Control the front panel LCD display available on some Check Point appliances.	set lcd * show lcd *
Hardware Health	hw-monitor	Hardware sensor monitoring.	show sysenv all cpstat -f sensors os
High Availability	high-avail-group	Overview page for High Availability.	
Host Access	host-access	Control which hosts are allowed to connect to Gaia.	add allowed-client * 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 *

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
IGMP	igmp	Control multicast group memberships through the Internet Group Management Protocol (IGMP).	set igmp * show igmp *
Inactivity timeout	inactto	Control inactivity timeout for Gaia Portal and Gaia Clish.	set inactivity-timeout * show inactivity-timeout *
Inbound Route Filters	import	Configure IPv4 Inbound Route Filters for RIP, OSPFv2, and BGP IPv4.	set inbound-route-filter *
Inbound Route Filters	import6	Configure IPv6 Inbound Route Filters for RIPng, OSPFv3, and BGP IPv6.	set ipv6 inbound-route-filter *
Installation	ftw	Run the Gaia First Time Configuration Wizard.	

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
Interface Naming	interface-name	Set a different name for an existing interface (requires a reboot and reconfiguration of the interface)	set interface-name *
IP Broadcast Helper	iphelper	Control forwarding of UDP broadcast traffic to other interfaces.	set iphelper * 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 *

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
IPv6 VRRP	vrrp6	Control the IPv6 Virtual Router Redundancy Protocol (VRRPv3).	set ipv6 vrrp6 * show ipv6 vrrp6 *
Job Scheduler	cron	Control scheduled automated tasks that perform actions at a specific time.	add cron * set cron * delete cron * show cron *
License Activation	license_activation	Access to "Activate Licenses".	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 *
Maintenance	maintenance-group	Overview page for Maintenance.	N/A

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
Management Interface	management_interface	Control which interface is used for management (main interface).	set management * show management *
NDP	neighbor	Control IPv6 Neighbor Discovery Protocol.	add neighbor-entry * set neighbor * delete neighbor-entry * show neighbor *
NetFlow Export	netflow	Control NetFlow Export on Gaia.	add netflow * set netflow * delete netflow * show netflow *
Network Access	netaccess	Control TELNET access to Gaia.	set net-access * show net-access *

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
Network Interfaces	interface	Control Physical interfaces, Aliases, Bridges, Bonds, VLANs, PPPoE.	<pre> 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 *</pre>
Network Management	interface-group	Overview page for Network Management.	<pre> show interface * show interfaces * set interface *</pre>
NTP	ntp	Control Network Time Protocol for synchronizing the Gaia clock.	<pre> add ntp * set ntp * delete ntp * show ntp *</pre>

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).	<pre>set ospf * show ospf * show route ospf *</pre>
OSPF v3	ospf3	Control IPv6 dynamic routing through the Open Shortest-Path First protocol v3 (OSPFv3).	<pre>set ipv6 ospf3 * set router-id * show ipv6 ospf3 * show ipv6 route ospf3 * show router-id *</pre>
Password Policy	password-controls	Control password and account policies on Gaia.	<pre>set password-controls * show password-controls *</pre>
Performance Optimization	perf	Control Multi-Queue on Security Gateway.	<pre>set multi-queue * show multi-queue *</pre>
PIM	pim	Control Protocol-Independent Multicast (PIM).	<pre>set pim * show pim * show mfc *</pre>

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 *
Router Service	router-service-group	Overview page for Routing Services.	

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
Routing Monitor	show-route-all	View summary information about routes on Gaia.	show route *
Routing Options	route-options	Configure protocol ranks and trace (debug) options on Gaia.	set routedsyslog * 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 or Card)	sam	Deprecated - SAM card is not supported. Monitor Security Acceleration Module for information on usage and connections.	show sam *
Scheduled Backup	scheduled_backup	Create scheduled backups of the Gaia for events of data loss.	add backup-scheduled * 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 Management	system-group	Overview page for System Management.	
System Status	sysenv	Hardware sensor monitoring.	show sysenv *

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
TACACS_ Enable	tacacs_enable	Control TACACS+ mechanism on Gaia.	tacacs_enable * show tacacs_enable *
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 *

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
User Management	<code>security-access-group</code>	Overview page for User Management.	
Users	<code>user</code>	Control user accounts on Gaia.	<pre>add user * set user * delete user * show user * show users *</pre>
Version	<code>version</code>	Shows the version of the installed Check Point product, and Gaia build and kernel.	<pre>show version *</pre>
Virtual-System	<code>virtual-system</code>	Control VSX Virtual Systems (CLI only). You must configure all Virtual Systems in SmartConsole only.	<pre>add virtual-system * set virtual-system * delete virtual-system * show virtual-system *</pre>
VPNT	<code>vpnt</code>	Control VPN Tunneling on Gaia.	<pre>add vpn * set vpn * delete vpn *</pre>

Table: List of Available Features in Roles (continued)

Feature name in Gaia Portal	Feature name in Gaia Clish	Description	Affected commands in Gaia Clish
VRRP	vrrp	Control the IPv4 Virtual Router Redundancy Protocol (VRRPv2) - Monitored Circuit/Simplified VRRP.	<pre> set vrrp * add mcvr * set mcvr * delete mcvr * show vrrp * show mcvr * </pre>
VSX	vsx	Enable or Disable the VSX mode (to be used only by Check Point Support only).	<pre> set vsx * show vsx * </pre>
Web configuration	web	Control Gaia Portal.	<pre> set web * generate web * show web * </pre>

List of Available Extended Commands in Roles

Important:

- Read the Known Limitations for R81.20 in [sk174965](#).
- Read the Known Limitations for Scalable Platforms in [sk148074](#).

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_cpcapca	Runs the Check Point Internal Certificate Authority (ICA).
cpca_client	ext_cpcapca_client	Controls the Check Point Internal Certificate Authority (ICA).
cpca_create	ext_cpcapca_create	Creates the Check Point Internal Certificate Authority (ICA) database.
cpca_dbutil	ext_cpcapca_dbutil	Controls the Check Point Internal Certificate Authority (ICA) database.
cpconfig	ext_cpconfig	Runs the Check Point Configuration Tool for Security Management Server and Security Gateway.
cphaprob	ext_cphaprob	Access to clustering commands.
cphastart	ext_cphastart	Enables the clustering feature on Security Gateway.
cphastop	ext_cphastop	Disables the clustering feature on Security Gateway.
cpinfo	ext_cpinfo	Collects the Check Point diagnostics information.
cplic	ext_cplic	Controls the Check Point licenses.

Command name in Gaia Portal	Command name in Gaia Clish / Gaia gClish	Description
cpshared_ver	ext_cpshared_ver	Shows the Check Point SVN Foundation version.
cpstart	ext_cpstart	Starts the installed Check Point products.
cpstat	ext_cpstat	Shows the Check Point statistics history information for Software Blades and Gaia.
cpstop	ext_cpstop	Stops the installed Check Point products.
cpview	ext_cpview	Shows the advanced Check Point statistics information for Software Blades and Gaia in real-time.
cpwd_admin	ext_cpwd_admin	Controls the Check Point WatchDog administration tool.
diag	ext_diag	Sends the system diagnostics information.
dtps	ext_dtps	Controls the Endpoint Policy Server commands.
etmstart	ext_etmstart	Starts the QoS Software Blade.
etmstop	ext_etmstop	Stops the QoS Software Blade.
fgate	ext_fgate	Controls the QoS Software Blade.
fips	ext_fips	Controls the FIPS mode.
fw	ext_fw	Access to Security Gateway commands for IPv4.
fw6	ext_fw6	Access to Security Gateway commands for IPv6.
fwaccel	ext_fwaccel	Access to SecureXL commands for IPv4.
fwaccel6	ext_fwaccel6	Access to SecureXL commands for IPv6.
fwm	ext_fwm	Access to Security Management commands.
ifconfig	ext_ifconfig	Deprecated. Use "show interface", or "set interface" commands instead.

Command name in Gaia Portal	Command name in Gaia Clish / Gaia gClish	Description
ips	ext_ips	Controls the IPS Software Blade.
lomipset	ext_lomipset	Configures the LOM Card IP address.
LSMcli	ext_LSMcli	Access to SmartProvisioning command line.
LSMenabler	ext_LSMenabler	Enables the SmartProvisioning.
mds_backup	ext_mds_backup	Creates backup of the Multi-Domain Server.
mds_restore	ext_mds_restore	Restores the backup of the Multi-Domain Server.
mdscmd	ext_mdscmd	Access to Multi-Domain Server command line.
mdsconfig	ext_mdsconfig	Runs the Check Point Configuration Tool for Multi-Domain Server.
mdsstart	ext_mdsstart	Starts the Multi-Domain Server.
mdsstart_customer	ext_mdsstart_customer	Starts a specific Domain Management Server.
mdsstat	ext_mdsstat	Shows the status of the Multi-Domain Server and all Domain Management Servers.
mdsstop	ext_mdsstop	Stops the Multi-Domain Server.
mdsstop_customer	ext_mdsstop_customer	Stops a specific Domain Management Server.
netstat	ext_netstat	Shows network connections, routing tables, and interface statistics.
ping	ext_ping	Sends pings to a host using IPv4.
ping6	ext_ping6	Sends pings to a host using IPv6.
raid_diagnostic	ext_raid_diagnostic	Access to RAID Monitoring tool.


Command name in Gaia Portal	Command name in Gaia Clish / Gaia gClish	Description
raidconfig	ext_raidconfig	Access to RAID Configuration and Monitoring tool.
rtm	ext_rtm	Controls the Monitoring Software Blade.
rtmstart	ext_rtmstart	Starts the Monitoring Software Blade.
rtmstop	ext_rtmstop	Stops the Monitoring Software Blade.
rtmtopsvc	ext_rtmtopsvc	Monitors top services using the Monitoring Software Blade.
SDSUtil	ext_SDSUtil	Access to Software Distribution Server utility.
sim	ext_sim	Access to SecureXL SIM device commands for IPv4.
SnortConvertor	ext_SnortConvertor	Access to the IPS Snort conversion tool.
tecli	ext_tecli	Access to the Threat Emulation Software Blade shell.
top	ext_top	Shows the most active system processes.
traceroute	ext_traceroute	Runs the trace tool.
vpn	ext_vpn	Controls the VPN kernel module for IPv4.
vpn6	ext_vpn6	Controls the VPN kernel module for IPv6.
vsx_util	ext_vsx_util	Controls the managed VSX Gateways and VSX Clusters on a Management Server.

Password Policy

This section explains how to configure your platform:

- To enforce creation of strong passwords.
- To monitor and prevent use of already used passwords.
- To force users to change passwords at regular intervals.

One of the important elements of securing your Check Point cyber security platform is to set user passwords and create a good *password policy*.

 **Note** - The password policy does not apply to non-local users that authentication servers such as RADIUS manage their login information and passwords. In addition, it does not apply to non-password authentication, such as the public key authentication supported by SSH.

To set and change user passwords, see ["Users" on page 404](#) and ["User Management" on page 402](#).

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	453
Password Strength	454
Password History	455
Mandatory Password Change	456
Denying Access to Unused Accounts	457
Denying Access After Failed Login Attempts	458
Password Hashing Algorithm	459

Procedure

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

Step	Instructions
1	In the navigation tree, click User Management > Password Policy .
2	Configure the password policy options: <ul style="list-style-type: none"> ▪ Password Strength (see "Password Strength" on the next page) ▪ Password History (see "Password History" on page 455) ▪ Mandatory Password Change (see "Mandatory Password Change" on page 456) ▪ Deny Access to Unused Accounts (see "Denying Access to Unused Accounts" on page 457) ▪ Deny Access After Failed Login Attempts (see "Denying Access After Failed Login Attempts" on page 458) ▪ Password hashing algorithm (see "Password Hashing Algorithm" on page 459)
3	Click Apply .

Password Strength

Parameter	Description
Minimum Password Length	<p>The minimum number of characters in a Gaia user, or an SNMP user password.</p> <p>Does not apply to passwords that were already configured.</p> <ul style="list-style-type: none"> ▪ Range: 6 - 128 ▪ Default: 6
Disallow Palindromes	<p>A palindrome is a sequence of letters, numbers, or characters that can be read the same in each direction.</p> <ul style="list-style-type: none"> ▪ Default: Selected
Password Complexity	<p>The required number of character types:</p> <ul style="list-style-type: none"> ▪ 1 - Don't check ▪ 2 - Require two character types (default) ▪ 3 - Require three character types ▪ 4 - Require four character types <p>Character types are:</p> <ul style="list-style-type: none"> ▪ Upper case alphabetic (A-Z) ▪ Lower case alphabetic (a-z) ▪ Digits (0-9) ▪ Other (everything else) <p>Changes to this setting do not affect existing passwords.</p>

Password History

Parameter	Description
Check for Password Reuse	<p>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.</p> <ul style="list-style-type: none">▪ Default: Selected
History Length	<p>The number of former passwords to keep and check against when a new password is configured for a user.</p> <ul style="list-style-type: none">▪ Range: 1 - 1000▪ Default: 10


Mandatory Password Change

Parameter	Description
Password Expiration	<p>The number of days, for which a password is valid. After that time, the password expires.</p> <p>The count starts when the user changes the password.</p> <p>Users are required to change an expired password the next time they log in.</p> <p>Does not apply to SNMP users.</p> <ul style="list-style-type: none"> ▪ Range: 1 - 1827, or Passwords never expires ▪ Default: Passwords never expires
Warn users before password expiration	<p>How many days before the user's password expires to start generating warnings to the user that user must change the password.</p> <p>A user that does not log in, does not see this warning.</p> <ul style="list-style-type: none"> ▪ Range: 1 - 366 ▪ Default: 7
Lockout users after password expiration	<p>Lockout users after password expiration.</p> <p>After a user's password has expired, user has this number of days to log in and change it.</p> <p>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.</p> <p>The administrator can unlock a user that is locked out from the User Management > Users page.</p> <ul style="list-style-type: none"> ▪ 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	<p>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.</p> <ul style="list-style-type: none"> ▪ Default: Not selected

Denying Access to Unused Accounts

Parameter	Description
Deny access to unused accounts	<p>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.</p> <ul style="list-style-type: none">▪ Default: Not selected
Days of non-use before lock-out	<p>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.</p> <ul style="list-style-type: none">▪ Range: 30 - 1827▪ Default: 365

Denying Access After Failed Login Attempts

Parameter	Description
Deny access after failed login attempts	<p>If the configured limit is reached, the user is locked out (unable to log in) for a configured time.</p> <p> 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.</p> <ul style="list-style-type: none"> ▪ Default: Not selected
Block admin user	<p>This option is available only if Deny access after failed login attempts is enabled.</p> <p>If the configured limit of failed login attempts for the <code>admin</code> user is reached, the <code>admin</code> user is locked out (unable to log in) for a configured time.</p>
Maximum number of failed attempts allowed	<p>This only takes effect if Deny access after failed attempts is enabled.</p> <p>The number of failed login attempts that a user is allowed before being locked out.</p> <p>After making that many successive failed attempts, future attempts fail.</p> <p>When one login attempt succeeds, counting of failed attempts stops, and the count is reset to zero.</p> <ul style="list-style-type: none"> ▪ Range: 2 - 1000 ▪ Default: 10

Parameter	Description
Allow access again after time	<p>This only takes effect, if Deny access after failed login attempts is enabled.</p> <p>Allow access again after a user was locked out (due to failed login attempts).</p> <p>The user is allowed access after the configured time, if there were no login attempts during that time.</p> <ul style="list-style-type: none"> ▪ Range: 60 - 604800 seconds ▪ Default: 1200 seconds (20 minutes) <p>Examples:</p> <ul style="list-style-type: none"> ▪ 60 = 1 minute ▪ 300 = 5 minutes ▪ 3600 = 1 hour ▪ 86400 = 1 day ▪ 604800 = 1 week

Password Hashing Algorithm

Parameter	Description
Password hashing algorithm	<p>Configures the hashing algorithm to store new passwords in the Gaia database.</p> <ul style="list-style-type: none"> ▪ Range: SHA256, or SHA512 ▪ Default: SHA512

Configuring Password Policy in Gaia Clish

In This Section:

Password Strength	460
Password History	462
Mandatory Password Change	463
Denying Access to Unused Accounts	465
Denying Access After Failed Login Attempts	466
Configuring Hashing Algorithm	468

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

Important:

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

Password Strength

Syntax

- To configure the password strength:

```
set password-controls
    complexity <1-4>
    min-password-length <6-128>
    palindrome-check {on |off}
```

- To show the configured password strength:

```
show password-controls
    complexity
    min-password-length
    palindrome-check

show password-controls all
```

Parameters

Parameter	Description
<code>complexity <1-4></code>	<p>The required number of character types:</p> <ul style="list-style-type: none"> ▪ 1 - Don't check ▪ 2 - Require two character types (default) ▪ 3 - Require three character types ▪ 4 - Require four character types <p>Character types are:</p> <ul style="list-style-type: none"> ▪ Upper case alphabetic (A-Z) ▪ Lower case alphabetic (a-z) ▪ Digits (0-9) ▪ Other (everything else) <p>Changes to this setting do not affect existing passwords.</p> <ul style="list-style-type: none"> ▪ Range: 1 - 4 ▪ Default: 2
<code>min-password-length <6-128></code>	<p>The minimum number of characters in a Gaia user, or an SNMP user password.</p> <p>Does not apply to passwords that were already configured.</p> <ul style="list-style-type: none"> ▪ Range: 6 - 128 ▪ Default: 2
<code>palindrome-check {on off}</code>	<p>A palindrome is a sequence of letters, numbers, or characters that can be read the same in each direction.</p> <ul style="list-style-type: none"> ▪ Range: <code>on</code>, or <code>off</code> ▪ Default: <code>on</code>

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}	<p>Check for reuse of passwords for all users.</p> <p>Enables or disables password history checking and password history recording.</p> <p>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 <code>history-length</code>.</p> <p>Does not apply to SNMP passwords.</p> <ul style="list-style-type: none"> ▪ Range: on, or off ▪ Default: on
history-length <1-1000>	<p>The number of former passwords to keep and check against when a new password is configured for a user.</p> <ul style="list-style-type: none"> ▪ 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>	<p>Lockout users after password expiration.</p> <p>After a user's password has expired, user has this number of days to log in and change it.</p> <p>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.</p> <p>The administrator can unlock a user that is locked out from the User Management > Users page.</p> <ul style="list-style-type: none"> ▪ Range: 1 - 1827, or never ▪ Default: never
expiration-warning-days <1-366>	<p>How many days before the user's password expires to start generating warnings to the user that user must change the password.</p> <p>A user that does not log in, does not see this warning.</p> <ul style="list-style-type: none"> ▪ Range: 1 - 366 ▪ Default: 7

Parameter	Description
force-change-when {no password}	<p>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.</p> <ul style="list-style-type: none"> ▪ Range: <ul style="list-style-type: none"> • no - Disables this functionality. • password - Forces users to change their password after their password was changed. ▪ Default: no
password-expiration <1-1827 never>	<p>The number of days, for which a password is valid. After that time, the password expires.</p> <p>The count starts when the user changes the password.</p> <p>Users are required to change an expired password the next time they log in.</p> <p>Does not apply to SNMP users.</p> <ul style="list-style-type: none"> ▪ 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>	<p>Configures the number of days of non-use before locking out the unused account.</p> <p>This only takes effect, if the "set password-controls deny-on-nonuse enable" is set to "on".</p> <ul style="list-style-type: none"> ▪ Range: 30 - 1827 ▪ Default: 365
deny-on-nonuse enable {on off}	<p>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.</p> <ul style="list-style-type: none"> ▪ 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
<pre>allow-after <60-604800></pre>	<p>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.</p> <ul style="list-style-type: none"> ■ Range: 60 - 604800 seconds ■ Default: 1200 seconds (20 minutes) <p>Examples:</p> <ul style="list-style-type: none"> ■ 60 = 1 minute ■ 300 = 5 minutes ■ 3600 = 1 hour ■ 86400 = 1 day ■ 604800 = 1 week
<pre>block-admin {on off}</pre>	<p>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 <code>admin</code> user is reached, the <code>admin</code> user is locked out (unable to log in) for a configured time.</p> <ul style="list-style-type: none"> ■ Range: on, or off ■ Default: off

Parameter	Description
<pre>enable {on off}</pre>	<p>If the configured limit is reached, the user is locked out (unable to log in) for a configured time.</p> <p> 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.</p> <ul style="list-style-type: none"> ▪ Range: on, or off ▪ Default: off
<pre>failures- allowed <2- 1000></pre>	<p>This only takes effect if "set password-controls deny-on-fail enable" is set to "on".</p> <p>The number of failed login attempts that a user is allowed before being locked out.</p> <p>After making that many successive failed attempts, future attempts fail.</p> <p>When one login attempt succeeds, counting of failed attempts stops, and the count is reset to zero,</p> <ul style="list-style-type: none"> ▪ Range: 2 - 1000 ▪ Default: 10

Configuring Hashing Algorithm

Syntax

- To configure the hashing algorithm:

```
set password-controls password-hash-type {SHA256 | SHA512}
```

- To show the configured hashing algorithm:

```
show password-controls password-hash-type
```

```
show password-controls all
```

Parameters

Parameter	Description
{SHA256 SHA512}	<p>Configures the hashing algorithm to store new passwords in the Gaia database.</p> <ul style="list-style-type: none"> ▪ Range: SHA256, or SHA512 ▪ Default: SHA512

Monitoring Password Policy in Gaia Clish

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

Syntax

```
show password-controls
  all
  complexity
  deny-on-fail
    allow-after
    block-admin
    enable
    failures-allowed
  deny-on-nonuse
    allowed-days
    enable
  expiration-lockout-days
  expiration-warning-days
  force-change-when
  history-checking
  history-length
  min-password-length
  palindrome-check
  password-expiration
  password-hash-type
```

Example

```
gaia> show password-controls all

Password Strength
  Minimum Password Length 6
  Password Complexity 2
  Password Palindrome Check on

Password History
  Password History Checking off
  Password History Length 10

Mandatory Password Change
  Password Expiration Lifetime 5
  Password Expiration Warning Days 8
  Password Expiration Lockout Days never
  Force Password Change When no

Configuration Deny Access to Unused Accounts
  Deny Access to Unused Accounts off
  Days Nonuse Before Lockout 365

Configuration Password hash
  Password hashing algorithm MD5
gaia>
```

Configuring SSH Authentication with RSA Key Files

Prerequisites

- Console access / LOM access to the Gaia server
- Administrator access to the Gaia server, or an equivalent user with the required permission
- The Gaia server must run version R80.40 with Take 83, or a higher version.

Notes:

- For the initial setup, it is necessary to do each step only one time.
- To configure more SSH users, it is necessary to do only steps 1 through 7.

Procedure

1. Create a pair of SSH keys.

You can use these tools:

- On a Windows OS computer - the PuTTYgen tool.
- On the Gaia server (or on a 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 406](#)
- ["Configuring Roles in Gaia Portal" on page 416](#)

In Gaia Clish:

- a. Create a new user.

See ["Managing User Accounts in Gaia Clish" on page 410](#).

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 420](#).



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 420.

Example:

```
MyGW> set user filecopy shell /bin/bash
```

- d. Save the configuration:

```
MyGW> save config
```

3. Connect with an SSH client to the Gaia server.

4. Log in with the new user.

In our example, the username is: `filecopy`.

5. Make sure you are in the home directory:

```
cd ~ ; pwd
```

6. Configure the required directory `".ssh"`:

- a. Create the directory `".ssh"`:

```
mkdir -v .ssh
```

- b. Assign the required permissions to the new directory `".ssh"`:

```
chmod -v u=rwx,g=,o= ~/.ssh
```

7. Configure the required file `"authorized_keys"`:

- a. Create the required file `"authorized_keys"`:

```
touch ~/.ssh/authorized_keys
```

- b. Assign the required permissions to the new file `"authorized_keys"`:

```
chmod -v u=rw,g=,o= ~/.ssh/authorized_keys
```

- c. Edit the `"authorized_keys"` file:

```
vi ~/.ssh/authorized_keys
```

- d. Paste the SSH key you created earlier into this file.

- e. Save the changes in the file and exit the editor.

8. Make the required changes in the SSH configuration template for the Gaia Operating System:

- a. Back up the `sshd_config.templ` file:

```
cp -v /etc/ssh/templates/sshd_config.templ{, _BKP}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 defined locally.

This is a good way of centrally managing the credentials of multiple Security Gateways.

To define non-local Gaia users, you define Gaia as a client of an authentication server.

Gaia supports these types of authentication servers:

Server	Description
RADIUS	<p>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.</p> <p>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.</p>
TACACS+	<p>The TACACS+ (Terminal Access Controller Access Control System) authentication protocol uses 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.</p> <p>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.</p> <p> Note - For TACACS authentication to work on a Virtual System, see the R81.20 VSX Administration Guide.</p>

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	476
Configuring RADIUS Servers in Gaia Clish	478

Configuring RADIUS Servers in Gaia Portal

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

Configuring a RADIUS server

Step	Instructions
1	In the navigation tree, click User Management > Authentication Servers .
2	In the RADIUS Servers section, click Add .
3	<p>Enter the RADIUS Server parameters:</p> <ul style="list-style-type: none"> <p>■ 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.</p> <p>■ Host Host name or IP address (IPv4 or IPv6) of RADIUS server.</p> <p>■ 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.</p> <p> 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.</p> <p>■ Shared Secret Shared secret used for authentication between the RADIUS server and the Gaia client. Enter the shared secret text string up to 256 characters, without any whitespace characters and without a backslash. Make sure that the shared string defined on the Gaia matches the shared string defined on the RADIUS server. RFC 2865 recommends that the secret be at least 16 characters in length. Some RADIUS servers have a maximum string length for shared secret of 15 or 16 characters. See the documentation for your RADIUS server.</p> <p>■ 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.</p>

Step	Instructions
4	Click OK .
5	<p>Optional: Select the Network Access Server (NAS) IP address. This setting applies to all configured RADIUS servers. This parameter records the IP address, from which Gaia sends the RADIUS packet. This IP address is stored in the RADIUS packet, even when the packet goes through NAT, or some other address translation that changes the source IP address of the packet. The "NAS-IP-Address" is defined in 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).</p>
6	<p>Optional: Select RADIUS Users Default Shell (for details about the shells, see <i>"Users" on page 404</i>). This setting applies to all configured RADIUS servers.</p>
7	<p>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 <code>sudo</code> command to get super user permissions (see <i>"Configuring RADIUS Servers for Non-Local Gaia Users" on page 482</i>).</p>
8	Click Apply .

Editing the RADIUS server

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

Deleting a RADIUS server

Step	Instructions
1	In the navigation tree, click User Management > Authentication Servers .
2	Select the RADIUS server.
3	Click Delete .
4	Click OK to confirm.

Configuring RADIUS Servers in Gaia Clish

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

Description

Use the "aaa radius-servers" commands to add, configure, and delete RADIUS authentication servers.

Syntax

Configuring RADIUS settings for use in a single authentication profile

```
add aaa radius-servers priority <Priority> host <Hostname, or IP
Address of RADIUS Server> [port <1-65535>]
    prompt-secret timeout <1-50>
    secret <Shared Secret> timeout <1-50>
```

Changing the configuration of a specific RADIUS server

```
set aaa radius-servers priority <Priority>
    host <Hostname, or IP Address of RADIUS Server>
    new-priority <New Priority>
    port <1-65535>
    prompt-secret
    secret <Shared Secret>
    timeout <1-50>
```

Changing the configuration that applies to all configured RADIUS servers

```
set aaa radius-servers
    NAS-IP<SPACE><TAB>
    default-shell<SPACE><TAB>
    super-user-uid <0 | 96>
```

Viewing a list of all configured RADIUS servers associated with an authentication profile

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

Viewing the configuration of a specific RADIUS server

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

Viewing the configuration that applies to all configured RADIUS servers


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

Deleting a specific RADIUS server


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

Deleting the configuration that applies to all configured RADIUS servers

```
delete aaa radius-servers
  NAS-IP
```

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

Parameters**CLI Parameters**

Parameter	Description
priority <Priority>	Configures the RADIUS server priority. Enter an integer between -999 and 999 (default is 0). 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
<code>prompt secret</code>	The system will prompt you to enter the Shared Secret.
<code>secret <Shared Secret></code>	<p>Configures the shared secret used for authentication between the RADIUS server and the Gaia.</p> <p>Enter the shared secret text string up to 256 characters, without any whitespace characters and without a backslash.</p> <p>Make sure that the shared string defined on the Gaia matches the shared string defined on the RADIUS server.</p> <p>RFC 2865 recommends that the secret be at least 16 characters in length.</p> <p>Some RADIUS servers have a maximum string length for shared secret of 15 or 16 characters.</p> <p>See the documentation for your RADIUS server.</p>
<code>timeout <1-50></code>	<p>Configures the timeout in seconds (from 1 to 5), during which Gaia waits for the RADIUS server to respond.</p> <p>The default value is 3.</p> <p>If there is no response after the configured timeout, Gaia tries to connect to a different configured RADIUS server.</p> <p>Set this timeout, so that the sum of all RADIUS server timeouts is less than 50.</p>
<code>default-shell <SPACE><TAB></code>	Optional: Configures the default shell for RADIUS Users (for details about the shells, see "Users" on page 404).
<code>super-user-uid <0 96></code>	Optional: Configures the UID for the RADIUS super user. If the UID is 0, there is no need to run the <code>sudo</code> command to get super user permissions (see "Configuring RADIUS Servers for Non-Local Gaia Users" on page 482).
<code>NAS-IP<SPACE><TAB></code>	<p>Optional: This parameter records the IP address, from which Gaia sends the RADIUS packet.</p> <p>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.</p> <p>The "NAS-IP-Address" is defined in RFC2865.</p> <p>If no NAS IP Address is chosen, the IPv4 address of the Gaia Management Interface is used (run the <code>"show management interface"</code> command).</p>


Configuring Gaia as a RADIUS Client

Gaia acts as a RADIUS client. You must define a role for the RADIUS client, and the features for that role.

To allow login with non-local users to Gaia, you must define a default Gaia role for all non-local users that are configured in the RADIUS server.

The default role can include a combination of:

- Administrative (read/write) access to some features
- Monitoring (read-only) access to other features
- No access to other features.

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


To configure Gaia as a RADIUS Client

Step	Instructions
1	Define the role for the RADIUS client: <ul style="list-style-type: none"> ▪ If no group is defined on the RADIUS server for the client, define this role: <pre>radius-group-any</pre> ▪ If a group is defined on RADIUS server for the client (group XXX, for example), define this role: <pre>radius-group-<XXX></pre>
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 415](#).

 **Note** - Do **not** define a new user for external users. An external user is one that is defined on an authentication server (such as RADIUS or TACACS), and not on the local Gaia system.

Configuring RADIUS Servers for Non-Local Gaia Users

Non-local users can be defined on a RADIUS server and not in Gaia.

When a non-local user logs in to Gaia, the RADIUS server authenticates the user and assigns the applicable permissions.

You must configure the RADIUS server to correctly authenticate and authorize non-local users.

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

Configuring a RADIUS server for non-local Gaia users

In addition, see [sk72940](#).

Step	Instructions
1	<p>Copy the applicable dictionary file to your RADIUS server.</p> <p>Example for the "Steel-Belted RADIUS server"</p> <ol style="list-style-type: none"> Copy this file from the Gaia to the RADIUS server: <code>/etc/radius-dictionaries/checkpoint.dct</code> Add these lines to the <code>vendor.ini</code> file on the RADIUS server (keep in alphabetical order with the other vendor products in this file): <pre>vendor-product = Check Point Gaia dictionary = nokiaipso ignore-ports = no port-number-usage = per-port-type help-id = 2000</pre> Add this line to the <code>dictiona.dcm</code> file: <code>"@checkpoint.dct"</code> <p>Example for the "FreeRADIUS server"</p> <ol style="list-style-type: none"> Copy this file from the Gaia to the RADIUS server to the <code>/etc/freeradius/</code> directory: <code>/etc/radius-dictionaries/dictionary.checkpoint</code> Add this line to the <code>/etc/freeradius/dictionary</code> file: <code>"\$INCLUDE dictionary.checkpoint"</code>

Step	Instructions
	<p>Example for the "OpenRADIUS server"</p> <ol style="list-style-type: none"> a. Copy this file from the Gaia to the RADIUS server to the <code>/etc/openradius/subdicts/</code> directory: <code>/etc/radius-dictionaries/dict.checkpoint</code> b. Add this line <code>/etc/openradius/dictionaries</code> file immediately after the <code>dict.ascend</code>: <code>\$include subdicts/dict.checkpoint</code>
2	<p>Define the user roles on Gaia. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:</p> <pre>CP-Gaia-User-Role = "role1,role2,..."</pre> <p>For example:</p> <pre>CP-Gaia-User-Role = "adminrole, backuprole, securityrole"</pre>
3	<p>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:</p> <ul style="list-style-type: none"> ▪ If this user should not receive superuser permissions: <pre>CP-Gaia-SuperUser-Access = 0</pre> ▪ If this user can receive superuser permissions: <pre>CP-Gaia-SuperUser-Access = 1</pre>

Logging in as the superuser

A user with super user permissions can use the Gaia shell to do system-level operations, including working with the file system.

Super user permissions are defined in the Check Point Vendor-Specific Attributes.

Users that have a UID of 0 have super user permissions.

They can run all the commands that the root user can run.

Users that have a UID of 96 must run the `sudo` command to get super user permissions.

The UIDs of all non-local users are defined in the `/etc/passwd` file.

Getting the superuser permissions (for users that have a UID of 96)

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


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

Configuring TACACS+ Servers

In This Section:

Configuring TACACS+ Servers in Gaia Portal	485
Configuring TACACS+ Servers in Gaia Clish	488
Checking if the Logged In User is Enabled for TACACS+	490

Configuring TACACS+ Servers in Gaia Portal

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

Configuring a TACACS+ server

Step	Instructions
1	In the navigation tree, click User Management > Authentication Servers .
2	In the TACACS+ Configuration section, select Enable TACACS+ authentication . This setting applies to all configured TACACS+ servers.
3	Click Apply .
4	In the TACACS+ Servers section, click Add .

Step	Instructions
5	<p>Configure the TACACS+ parameters:</p> <ul style="list-style-type: none"> <p>▪ Priority The priority of the TACACS+ server - from 1 to 20. Must be unique for this operating system. Gaia uses the priority:</p> <ul style="list-style-type: none"> • 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 <code>priority 1</code> applies to the TACACS+ server with priority 1. <p>▪ Server IPv4 address of the TACACS+ server.</p> <p>▪ 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.</p> <p>▪ 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.</p>
6	Click OK .
7	<p>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.</p>

Disabling TACACS+ authentication

Step	Instructions
1	In the navigation tree, click User Management > Authentication Servers .

Step	Instructions
2	In the TACACS+ configuration section, clear Enable TACACS+ authentication . This setting applies to all configured TACACS+ servers.
3	Click Apply .

Deleting the TACACS+ server

Step	Instructions
1	In the navigation tree, click User Management > Authentication Servers .
2	In the TACACS+ Servers section, select a TACACS+ server.
3	Click Delete .
4	Click OK to confirm.

Configuring TACACS+ Servers in Gaia Clish

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

Syntax

Configuring a TACACS+ server for use in a single authentication profile

```
add aaa tacacs-servers priority <Priority> server <IPv4 Address
of TACACS+ Server> key <Shared Secret> timeout <1-60>
```

Changing the configuration of a specific TACACS+ server

```
set aaa tacacs-servers priority <Priority>
  server <IPv4 Address of TACACS+ Server>
  new-priority <New Priority>
  key <Shared Secret>
  timeout <1-60>
```

Changing the configuration that applies to all configured TACACS+ servers

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

Viewing the list of all configured TACACS+ servers associated with an authentication profile

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

Viewing the configuration of a specific TACACS+ server

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

Viewing the configuration that applies to all configured TACACS+ servers

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

Deleting a specific TACACS+ server

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


Deleting the configuration that applies to all configured TACACS+ servers

```
delete aaa tacacs-servers
NAS-IP
```

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

Parameters**CLI Parameters**

Parameter	Description
<pre>priority <Priority></pre>	<p>The priority of the TACACS+ server - from 1 to 20. Must be unique for this operating system. The priority is used:</p> <ul style="list-style-type: none"> 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 <code>priority 1</code> applies to the TACACS+ server with priority 1. <p>Values:</p> <ul style="list-style-type: none"> Range: 1 - 20 Default: No default
<pre>server <IPv4 Address of TACACS+ Server></pre>	IPv4 address of the TACACS+ server.
<pre>key <Shared Secret></pre>	<p>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.</p>

Parameter	Description
<code>timeout <1-60></code>	<p>Enter the timeout in seconds, during which Gaia waits for the TACACS+ server to respond.</p> <p>If there is no response after the configured timeout, Gaia tries to connect to a different configured TACACS+ server.</p> <ul style="list-style-type: none"> ▪ Range: 1 - 60 ▪ Default: 5
<code>new-priority <New Priority></code>	Configures the new priority for the TACACS+ server.
<code>state {on off}</code>	<p>Configures the state of TACACS+ authentication.</p> <ul style="list-style-type: none"> ▪ 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	On Scalable Platforms, go to Gaia gClish: Type <code>gclish</code> and press Enter.
4	Run: <pre>show tacacs_enable</pre>

Configuring Gaia as a TACACS+ Client

Gaia acts as a TACACS+ client for Gaia users that are defined on the TACACS+ server and are not defined locally on Gaia.

The **admin** user must define a role called `TACP-0` for the TACACS+ users, and the allowed features for the `TACP-0` role.

Important:

1. All TACACS+ users must log in to Gaia OS with the password assigned to the default role `TACP-0`.
2. To get their applicable TACP role in Gaia OS, after this initial login, TACACS+ users must log in for the second time with the password assigned to their applicable TACP role.

Privilege Escalation

The Gaia admin user can define roles that make it possible for Gaia users to get temporarily higher privileges, than their regular privileges.

For example, Gaia user Fred needs to configure the interfaces, but his role does not support interfaces configuration. To configure the interfaces, Fred enters his user name together with a password given him by the admin user. This password lets him change his default role to the role that allows him to configure the interfaces.

There are sixteen different privilege levels (0 - 15) defined in TACACS+.

Each level can be mapped to a different Gaia role.

For example:

- Privilege level 0 - monitor-only
- Privilege level 1 - basic network configuration
- Privilege level 15 - admin user

By default, all non-local TACACS+ Gaia users are assigned the role `TACP-0`.

The Gaia admin can define for them roles with the name `TACP-N` that give them different privileges, where `N` is a privilege level - a number from 1 to 15.

The TACACS+ users can changes their own privileges by moving to another `TACP-N` role.

To do this, the TACACS+ users need to get a password from the Gaia admin user.

Configuring Gaia as a TACACS+ Client


Step	Instructions
1	Connect to Gaia OS as the <code>admin</code> user.

Step	Instructions
2	Define the role <code>TACP-0</code> .
3	Define the features for the role. For instructions, see "Roles" on page 415 .
4	Optional: Define one or more roles with the name <code>TACP-N</code> where <code>N</code> is a privilege level - a number from 1 to 15, and define the features for each role.

Raising the "TACP" privileges


You can raise the "TACP" privileges in either Gaia Portal, or Gaia Clish.

Raising "TACP" privileges in Gaia Portal

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

Step	Instructions
1	In your web browser, connect to Gaia Portal.
2	Enter the username and password of the TACACS+ user. After the TACACS server authentication, you have the privileges of the <code>TACP-0</code> role.
3	To raise the privileges to the <code>TACP-N</code> role (<code>N</code> is a number from 1 to 15), click Enable at the top of the Overview page.
4	Enter the password for the user.

Raising "TACP" privileges in Gaia Clish


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

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

Step	Instructions
3	<p>After you are authenticated by the TACACS server, you get the Gaia Clish prompt.</p> <p>At this point, you have the privileges of the TACP-0 role.</p> <p>Run:</p> <pre>tacacs_enable TACP-<N></pre> <p>Where <i>N</i> is the new TACP role (an integer from 1 to 15).</p>
4	When prompted, enter the applicable password.

To go back to the TACP-0 role, press **CTRL+D**, or enter **exit** at the command prompt.

The user automatically exits the current shell and goes back to TACP-0.

 **Note** - Do **not** define a new user for external users. An external user is one that is defined on an authentication server (such as RADIUS, or TACACS), and not on the local Gaia system.

Viewing if the currently logged in user is authenticated by TACACS+

Step	Instructions
1	Connect to the command line on Gaia.
2	Log in to Gaia Clish.
3	On Scalable Platforms, go to Gaia gClish: Type <code>gclish</code> and press Enter.
3	<p>Run:</p> <pre>show tacacs_enable</pre>

Configuring TACACS+ Servers for Non-Local Gaia Users

You can define Gaia users on a TACACS server instead of defining them on the Gaia computer.


Gaia users that are defined on a TACACS server are called non-local users.

Cisco ACS servers are the most commonly used TACACS+ servers.

For help with the configuration of a Cisco ACS server as a TACACS+ server for Gaia clients, see [sk98733](#) (as an example of best practices and **not** a replacement for the official Cisco documentation).

When a non-local user logs in to Gaia, the TACACS server authenticates the user and assigns the permissions to the user.

You must configure the TACACS server to correctly authenticate and authorize non-local Gaia users.

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

System Groups

In This Section:

Introduction	495
Configuring System Groups in Gaia Portal	496
Configuring System Groups in Gaia Clish	498

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 415](#).

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

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

Viewing the list of all System Groups

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

Adding a System Group

Step	Instructions
1	In the navigation tree, click User Management > System Groups .
2	Click Add .
3	In the Group Name field, enter the applicable unique name - between 1 and 16 alphanumeric characters without spaces.
4	<p>In the Group ID field, enter a unique Group ID number - between 101 and 65530:</p> <ul style="list-style-type: none"> ▪ 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. <p>If you specify a value in the reserved ranges, an error message is displayed.</p>
5	Click OK .

Adding a user to the System Group

Step	Instructions
1	In the navigation tree, click User Management > System Groups .
2	Select the System Group.
3	Click Edit .
4	<p>In the Available Members list, select a user. To select several users:</p> <ol style="list-style-type: none"> a. Press and hold the CTRL key on the keyboard. b. Left-click the applicable users. The selected users become highlighted.

Step	Instructions
5	Click Add > . The selected users move to the Members of Group list.
6	Click OK .

Removing a user from the System Group

Step	Instructions
1	In the navigation tree, click User Management > System Groups .
2	Select the System Group.
3	Click Edit .
4	In the Members of Group list, select a user. To select several users: <ul style="list-style-type: none"> 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 .

Deleting the System Group

Step	Instructions
1	In the navigation tree, click User Management > System Groups .
2	Select the System Group.
3	Click Delete .
4	Click OK to confirm.

Configuring System Groups in Gaia Clish

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

Syntax

Adding a System Group

```
add group <Group Name> gid <Group ID>
```

Adding a user to the System Group

```
add group <Group Name> member<SPACE><TAB>
```

```
add group <Group Name> member <UserName>
```

Changing the Group ID of a System Group

```
set group <Group Name> gid <Group ID>
```

Viewing all users in the System Group

```
show group <Group Name>
```

Viewing all configured System Groups

```
show groups
```

Removing a user from a System Group

```
delete group <Group Name> member<SPACE><TAB>
```

```
delete group <Group Name> member <UserName>
```

Deleting a System Group

```
delete group <Group Name>
```

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

Parameters

CLI Parameters

Parameter	Description
<code>group <Group Name></code>	Unique name of System Group - between 1 and 16 alphanumeric characters without spaces
<code>gid <Group ID></code>	Unique Group ID number - between 101 and 65530: <ul style="list-style-type: none">▪ 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.
<code>member <UserName></code>	Name of an existing user.

GUI Clients

In This Section:

Configuring GUI Clients in Gaia Portal	500
Configuring GUI Clients in Command Line	501

If this is a Security Management Server, you can configure which computers can connect to this Security Management Server with SmartConsole.



Note - This section does **not** appear, if this is a Multi-Domain Server.

Configuring GUI Clients in Gaia Portal

Step	Instructions
1	In the navigation tree, click User Management > GUI Clients .
2	Click Add . The Add GUI Client window opens.
3	Define the GUI clients (trusted hosts). These are the values: <ul style="list-style-type: none"> ▪ Any IP Address All clients are allowed to log in, regardless of their IP address. This option only shows if Any was not defined during the initial configuration. ▪ This machine - IP address ▪ Network ▪ Range of IPv4 addresses

Configuring GUI Clients in Command Line

Step	Instructions
1	Connect to the command line on the Security Management Server.
2	Run: <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>cpconfig</pre> </div> For more information, see the R81.20 CLI Reference Guide > Chapter <i>Security Management Server Commands</i> > Section <i>cpconfig</i> .
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: <ul style="list-style-type: none"> ▪ IP address - One computer defined by its IPv4 or IPv6 address. ▪ Machine name - One computer defined by its hostname. ▪ "Any" - An IPv4 address without restriction. You must: <ol style="list-style-type: none"> 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	502
VRRP Terminology	503
VRRP on Gaia OS	504
VRRP Configuration Methods	505
Monitoring of VRRP Interfaces	506
How VRRP Failover Works	506
Typical VRRP Use Cases	508

- i** **Important** - Scalable Platforms (Maestro and Chassis) do **not** support this feature in Gaia operating system (Known Limitation MBS-2521).
 To configure Maestro in Dual Site, see the [R81.20 Quantum Maestro Administration Guide](#).
 To configure Scalable Chassis in Dual Chassis, see the [R81.20 Quantum Scalable Chassis Administration Guide](#).

Understanding VRRP

Virtual Routing Redundancy Protocol (VRRP) is a high-availability solution, where two Gaia Security Gateways can provide backup for each other. Gaia offers two ways to configure VRRP:

- **Monitored Circuit/Simplified VRRP** - All the VRRP interfaces automatically monitor other VRRP interfaces.
- **Advanced VRRP** - Every VRRP interface must be explicitly configured to monitor every other VRRP interface.

i **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 <i>enabled</i>	<p>This is the most common use case.</p> <p>You can deploy only an Active/Backup environments.</p> <p>VRRP supports a maximum of one VRID with one Virtual IP Address (VIP) for each interface.</p> <p>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.</p> <p>You must also configure <i>priority deltas</i> to allow a failover to the VRRP Backup node, when the VRID on any on interface fails over.</p>
VRRP with ClusterXL <i>disabled</i>	<p>You can deploy an Active/Active environment.</p> <p>You can configure two VRIDs on the same interface, with one VIP for each VRID.</p> <p>This configuration supports only static routes on the VRRP interfaces.</p> <p>You must disable the VRRP monitoring of the Check Point Firewall (see "Preparing a VRRP Cluster" on page 511).</p>

VRRP Configuration Methods

VRRP Method	Description
Monitored Circuit/Simplified VRRP	<p>To configure this simplified VRRP method, in the Gaia Portal go to High Availability > VRRP.</p> <p>This method contains all of the basic parameters, and is applicable for most environments.</p> <p>You configure each Virtual Router as one unit and configure the same VRID on all interfaces.</p> <p>Monitored Circuit VRRP automatically monitors all VRRP interfaces. This make a complete node failover possible.</p> <p>You can configure only one VRID, which is automatically added to all the VRRP interfaces.</p> <p>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.</p>
Advanced VRRP	<p>To configure this advanced VRRP method, in the Gaia Portal go to High Availability > Advanced VRRP.</p> <p>This method allows configuration of different VRIDs on different interfaces.</p> <p>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</p> <ul style="list-style-type: none"> ■ With ClusterXL <i>enabled</i>, 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 <i>disabled</i>, 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

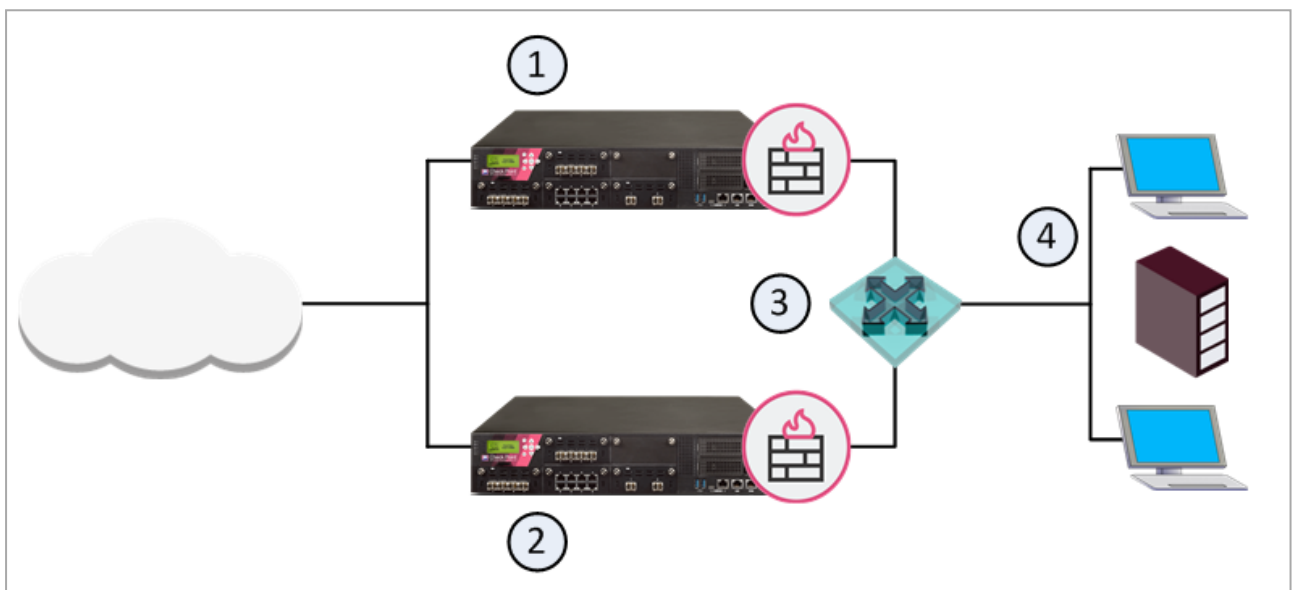
These are examples of some VRRP environments.

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

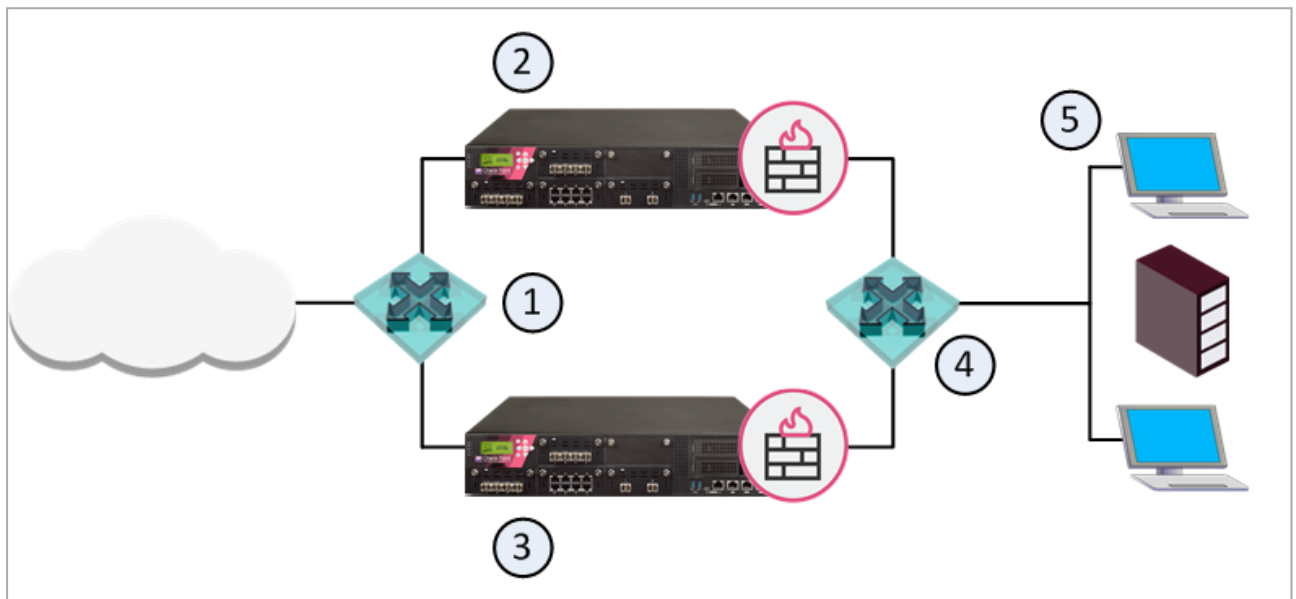
VRRP Use Case 2 - Internal and External Network High Availability

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.

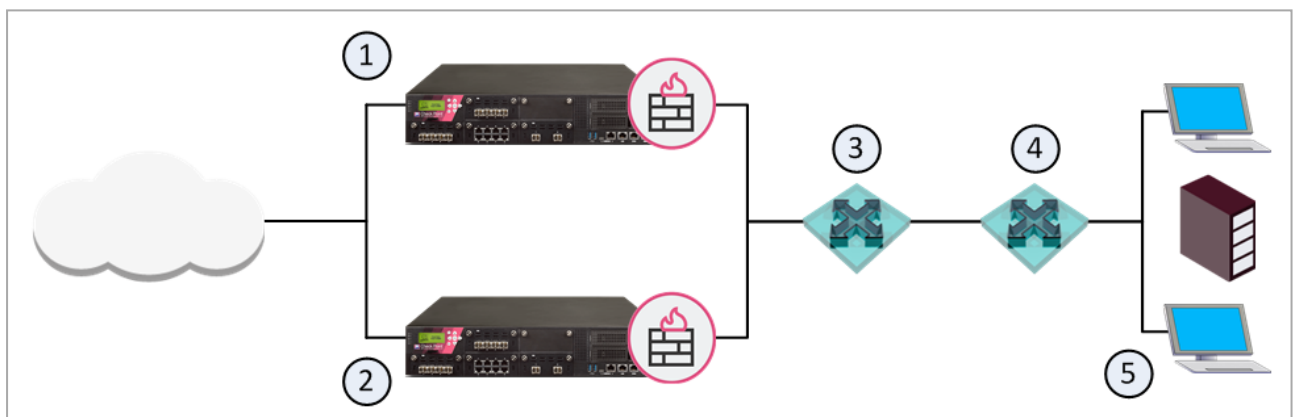
The monitoring of the Check Point Firewall by VRRP must be disabled (it is enabled by default).

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	511
Preparing VRRP Cluster Members	511
Configuring Global Settings for VRRP	512

i Important - Scalable Platforms (Maestro and Chassis) do **not** support this feature (Known Limitation MBS-2521).

Configuring Network Switches

Recommendations

- ★ Best Practice** - If you use the Spanning Tree protocol on Cisco switches connected to Check Point VRRP clusters, we recommend that you enable PortFast. It sets interfaces to the Spanning Tree forwarding state, which prevents them from waiting for the standard forward-time interval.

If you use switches from a different vendor, we recommend that you use the equivalent feature for that vendor. If you use the Spanning Tree protocol without PortFast, or its equivalent, you may see delays during VRRP failover.

Preparing VRRP Cluster Members

Procedure

Step	Instructions
1	Install the VRRP Cluster Members See the R81.20 Installation and Upgrade Guide > Chapter <i>Installing a ClusterXL, VSX Cluster, VRRP Cluster</i> > Section <i>Installing a VRRP Cluster</i> .
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 290). 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 237). This lets you use host names as an alternative to IP addresses or DNS servers.


Step	Instructions
4	<p>Enable Virtual Routers:</p> <ol style="list-style-type: none"> With a web browser, connect to Gaia Portal at: <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <code>https://<IP address of Gaia Management Interface></code> </div> In the navigation tree, click High Availability > VRRP. Configure the VRRP Global Settings. See the section "Configuring Global Settings for VRRP" below. If the Disable All Virtual Routers option is currently selected, clear it. Click Apply Global Settings.
5	<p>Configure your Virtual Routers in either Gaia Portal, or Gaia Clish. See:</p> <ul style="list-style-type: none"> ▪ "Configuring Monitored Circuit/Simplified VRRP" on page 514 ▪ "Configuring Advanced VRRP" on page 523

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	<p>In the navigation tree, click one of these:</p> <ul style="list-style-type: none"> ▪ High Availability > VRRP. ▪ High Availability >Advanced VRRP.

Step	Instructions
2	<p>In the VRRP Global Settings section:</p> <ul style="list-style-type: none"> ▪ 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 <i>Interface Delay</i> 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. <p> 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.</p>
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	514
Configuring Monitored Circuit/Simplified VRRP in Gaia Clish	518
Configuring the VRRP Cluster for Simplified VRRP in SmartConsole	522

 **Important** - Scalable Platforms (Maestro and Chassis) do **not** support this feature (Known Limitation MBS-2521).


This section includes the procedure for configuring Monitored Circuit/Simplified VRRP.

Configuring Monitored Circuit/Simplified VRRP in Gaia Portal

Procedure

Step	Instructions
1	In the navigation tree, click High Availability > VRRP .
2	Configure the VRRP Global Settings . See " Preparing a VRRP Cluster " on page 511.
3	In the Virtual Routers section, click Add .

Step	Instructions
4	<p>In the Add Virtual Router window, configure these parameters:</p> <ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> • 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
	<p>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.</p>
5	<p>In the Backup Addresses section, click Add. Configure these parameters in the Add Backup Address window:</p> <ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> • VRRP - Sets the VMAC to use the standard VRRP protocol. It is automatically set to the same value on all Security Gateways in the Virtual Router. This is the default setting. • Interface - Sets the VMAC to the local interface MAC address. If you define this mode for the VRRP Master and the VRRP Backup, the VMAC is different for each. VRRP IP addresses are related to different VMACs. This is because they are dependent on the physical interface MAC address of the currently defined VRRP Master. Note -If you configure different VMACs on the VRRP Master and VRRP Backup, you must make sure that you select the correct proxy ARP setting for NAT. • Static - Manually set the VMAC address. Enter the VMAC address in the applicable field. • Extended - Gaia dynamically calculates and adds three bytes to the interface MAC address to generate VMAC address that is more random. If you select this mode, Gaia constructs the same MAC address for VRRP Master and VRRP Backups in the Virtual Router. <p> 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.</p> <p>Click OK. The new VMAC mode shows in the in the Backup Address table.</p>
6	<p>To remove a Backup Address, select an address and click Delete. The address is removed from the Backup Address table.</p>

Step	Instructions
7	Click Save .

Configuring Monitored Circuit/Simplified VRRP in Gaia Clish

Syntax

Adding the Monitored Circuit/Simplified VRRP

1. Configure the priority:

```
add mcvr vrid VALUE priority VALUE priority-delta VALUE
[authtype {none | simple VALUE} hello-interval VALUE
```

2. Configure the backup address:

```
add mcvr vrid VALUE backup-address VALUE vmac-mode VALUE
```

Configuring the Monitored Circuit/Simplified VRRP

```
set mcvr vrid VALUE
  authtype {none | simple VALUE}
  auto-deactivation {on | off}
  backup-address VALUE vmac-mode VALUE [static-mac VALUE]
  hello-interval VALUE
  preempt-mode {on | off}
  priority VALUE
  priority-delta VALUE
```

Viewing the Monitored Circuit/Simplified VRRP configuration

```
show mcvr
  vrid VALUE
    all
    authtype
    backup-address VALUE
    backup-addresses
    hello-interval
    priority
    priority-delta
  vrids
```

Deleting the Monitored Circuit/Simplified VRRP

```
delete mcvr vrid VALUE [backup-address VALUE]
```




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

Parameters

CLI Parameters

Parameter	Description
<code>vrid VALUE</code>	<p>Configures the Virtual Router ID.</p> <ul style="list-style-type: none"> ▪ Range: 1 - 255 ▪ Default: No default value
<code>authtype {none simple VALUE}</code>	<p>Configures authentication for the given Virtual Router. You must use the same authentication method for all Security Gateways in a Virtual Router.</p> <ul style="list-style-type: none"> ▪ Range: <ul style="list-style-type: none"> • <code>none</code> - Disables authentication • <code>simple <plain-text password></code> - Authenticates VRRP packets using a plain-text password ▪ Default: No default value
<code>auto- deactivation {on off}</code>	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <ul style="list-style-type: none"> ▪ Range: <code>on</code>, or <code>off</code> ▪ Default: <code>off</code>
<code>backup- address VALUE</code>	<p>Configures the IPv4 address of the VRRP Backup Security Gateway.</p> <p>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.</p>

Parameter	Description
<pre>vmac-mode {default-vmac extended- vmac interface- vmac static-vmac VALUE}</pre>	<p>Configures how the Virtual MAC (VMAC) address is calculated for the given Virtual IP Address.</p> <p>Each Virtual IP Address for a Virtual Router implies the existence of a virtual network interface.</p> <ul style="list-style-type: none"> ▪ Range: <ul style="list-style-type: none"> • <code>default-vmac</code> - Generates the VMAC using the standard method described in Section 7.3 of RFC 3768. • <code>extended-vmac</code> - Generates the VMAC using an extended range of uniqueness by dynamically calculating 3 bytes of the VMAC instead of only 1. • <code>interface-vmac</code> - Configures the VMAC to use the interface hardware MAC address. • <code>static-vmac <VALUE></code> - Configures the Virtual Router to use a specified static VMAC address. ▪ Default: <code>default-vmac</code> <p> Note - If you set the VMAC mode to "<code>interface-vmac</code>" or "<code>static-vmac</code>", 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.</p>
<pre>hello- interval VALUE</pre>	<p>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.</p> <ul style="list-style-type: none"> ▪ Range: <code>default</code>, or 1 - 255 ▪ Default: 1

Parameter	Description
<pre>preempt-mode {on off}</pre>	<p>Configures Preempt Mode for the given Virtual Router.</p> <p>When the Preempt Mode is <i>enabled</i>, if the Virtual Router has a higher Priority than the current VRRP Master, it preempts the VRRP Master.</p> <p>If the Preempt Mode is <i>disabled</i>, all Virtual Routers that have monitored interfaces, are participating to avoid potential split-brain network topology.</p> <p>For more information on the implications of disabling Preempt Mode, see the help text for the "set mcvr vrid <VALUE> monitor-vrrp" command.</p> <ul style="list-style-type: none"> ▪ Range: on, or off ▪ Default: off
<pre>priority VALUE</pre>	<p>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.</p> <p>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.</p> <ul style="list-style-type: none"> ▪ Range: default, or 1 - 254 ▪ Default: 100
<pre>priority- delta VALUE</pre>	<p>Updates the Priority Delta of the given Virtual Router.</p> <p>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.</p> <p>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.</p> <ul style="list-style-type: none"> ▪ Range: default, or 1 - 254 ▪ Default: No default value

Configuring the VRRP Cluster for Simplified VRRP in SmartConsole

Follow the [R81.20 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	523
Configuring Advanced VRRP in Gaia Portal	524
Configuring Advanced VRRP in Gaia Clish	528
Configuring the VRRP Cluster for Advanced VRRP in SmartConsole	534

i Important - Scalable Platforms (Maestro and Chassis) do **not** support this feature (Known Limitation MBS-2521).

Advanced VRRP lets you configure Virtual Routers at the interface level.

This section contains only those procedures that are directly related to Advanced VRRP configuration.

The general procedures for configuring VRRP clusters are described in "[Configuring Monitored Circuit/Simplified VRRP](#)" on page 514.

With Advanced VRRP, you must configure every Virtual Router to monitor every configured VRRP interface.

Changing from Advanced VRRP to Monitored Circuit/Simplified VRRP

Procedure

Step	Instructions
1	Delete all existing Virtual Routers.
2	Create new Virtual Routers in accordance with the procedures.

You cannot move a Backup Address from one interface to another while a Security Gateway is a VRRP Master.

Perform these steps to delete and add new interfaces with the necessary IP addresses:

Step	Instructions
1	Cause a failover from the VRRP Master to the VRRP Backup.
2	Reduce the priority, or disconnect an interface.

Step	Instructions
3	Delete the Virtual Router on the interface.
4	Create new Virtual Router using the new IP address.
5	Configure the Virtual Router as before.

Configuring Advanced VRRP in Gaia Portal

Procedure

Step	Instructions
1	In the navigation tree, click High Availability >Advanced VRRP .
2	Configure the VRRP Global Settings (see "Preparing a VRRP Cluster" on page 511).
3	In the Virtual Routers section, click Add .
4	In the Add New Virtual Router window, configure these parameters: <ul style="list-style-type: none"> ▪ 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
	<ul style="list-style-type: none"> <li data-bbox="395 241 1430 517"> <p>▪ 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.</p> <p>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.</p> <li data-bbox="395 555 1449 909"> <p>▪ 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.</p> <p>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.</p> <p>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.</p>

Step	Instructions
	<ul style="list-style-type: none"> ■ 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. <p>Select the mode:</p> <ul style="list-style-type: none"> • VRRP - Sets the VMAC to use the standard VRRP protocol. It is automatically set to the same value on all Security Gateways in the Virtual Router. This is the default setting. • Interface - Sets the VMAC to the local interface MAC address. If you define this mode for the VRRP Master and the VRRP Backup, the VMAC is different for each. VRRP IP addresses are related to different VMACs. This is because they are dependent on the physical interface MAC address of the currently defined VRRP Master. <ul style="list-style-type: none"> i 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. <ul style="list-style-type: none"> i 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. <ul style="list-style-type: none"> ■ Authentication: <ul style="list-style-type: none"> • None - To disable authentication of VRRP packets. • Simple - To authenticate VRRP packets using a plain-text password. <p>You must use the same authentication method for all Security Gateways in a Virtual Router.</p>

Step	Instructions
5	<p>In the Backup Addresses section:</p> <ol style="list-style-type: none"> Click Add. In the IPv4 address field, enter the IPv4 address. Click OK. <p>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.</p>
6	<p>In the Monitored Interfaces section:</p> <ol style="list-style-type: none"> Click Add. Gaia shows a warning that adding a Monitored Interface will lock the Interface for this Virtual Router. Click OK to confirm. In the Interface field, select the interface. 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. Click OK. <p>To change a Monitored Interface, select a Monitored Interface and click Edit. To remove a Monitored Interface, select a Monitored Interface and click Delete.</p>
7	Click Save .

Configuring Advanced VRRP in Gaia Clish

Syntax

Configuring Advanced VRRP

```
set vrrp
  accept-connections {on | off}
  coldstart-delay VALUE
  disable-all-virtual-routers {on | off}
  monitor-firewall {on | off}
  interface-delay VALUE
```

Configuring an Advanced VRRP interface

```
set vrrp interface VALUE
  authtype
    none
    simple VALUE
  monitored-circuit vrid VALUE
    auto-deactivation {on | off}
    backup-address VALUE {on | off}
    hello-interval VALUE
    monitored-interface VALUE
      on
      off
    priority-delta <default | 1 - 254>}
  off
  on
  preempt-mode {on | off}
  priority VALUE
  vmac-mode
    default-vmac
    extended-vmac
    interface-vmac
    static-vmac VALUE
  off
  virtual-router legacy off
```

Viewing the Advanced VRRP configuration

```
show vrrp
  [interface VALUE]
  [interfaces]
  [stats]
  [summary]
```



Important - After you add, configure, or delete features, run the "save config" command to save the settings permanently.

Parameters

CLI Parameters

Parameter	Description
<code>accept-connections {on off}</code>	<p>Controls the Accept Connections option.</p> <p>This option causes packets destined to VRRP Virtual IP Address(es) to be accepted, and any required responses be generated.</p> <p>Enabling this option enhances VRRP's interaction with network management tools, which in turn allows for faster failure detection.</p> <p>This option is required for High Availability applications (for example, routing protocols), whose service is tied to a Virtual IP Address.</p> <ul style="list-style-type: none"> ▪ Range: <code>on</code>, or <code>off</code> ▪ Default: <code>off</code>
<code>coldstart-delay <VALUE></code>	<p>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.</p> <ul style="list-style-type: none"> ▪ Range: 0 - 3600 ▪ Default: 0
<code>disable-all-virtual-routers {on off}</code>	<p>Enables or disables all IPv4 VRRP Virtual Routers.</p> <p>If disabled, the VRRP configuration is preserved and can be enabled again.</p> <ul style="list-style-type: none"> ▪ Range: <code>on</code>, or <code>off</code> ▪ Default: <code>off</code>
<code>monitor-firewall {on off}</code>	<p>Enables or disables VRRP monitoring of the Security Gateway state.</p> <p>If this option is enabled, and the Firewall is not ready, the cluster member will refuse to be the VRRP Master.</p> <ul style="list-style-type: none"> ▪ Range: <code>on</code>, or <code>off</code> ▪ Default: <code>on</code>

Parameter	Description
<pre>interface-delay <VALUE></pre>	<p>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.</p> <ul style="list-style-type: none"> ▪ Range: 0 - 3600 ▪ Default: 0
<pre>interface VALUE authtype {none simple VALUE}</pre>	<p>The name of the interface, on which to enable the VRRP.</p> <p>Configures authentication for the given Virtual Router. You must use the same authentication method for all Security Gateways in a Virtual Router.</p> <ul style="list-style-type: none"> ▪ Range: <ul style="list-style-type: none"> • none - Disables authentication • simple <plain-text password> - Authenticates VRRP packets using a plain-text password ▪ Default: No default value
<pre>monitored-circuit vrid <VALUE></pre>	<p>Configures the Virtual Router ID.</p> <ul style="list-style-type: none"> ▪ Range: 1 - 255 ▪ Default: No default value

Parameter	Description
<pre>monitored-circuit vrid VALUE auto- deactivation {on off}</pre>	<p>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.</p> <p>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.</p> <ul style="list-style-type: none"> ▪ Range: on, or off ▪ Default: off
<pre>monitored-circuit vrid VALUE backup-address VALUE {on off}</pre>	<p>Configures the IPv4 address of the VRRP Backup Security Gateway.</p> <p>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.</p>
<pre>monitored-circuit vrid VALUE hello- interval VALUE</pre>	<p>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.</p> <ul style="list-style-type: none"> ▪ Range: default, or 1 - 255 ▪ Default: 1

Parameter	Description
<pre>monitored- interface VALUE {on off priority-delta <default 1 - 254>}</pre>	<p>Configures the list of monitored interfaces names for the given Virtual Router.</p> <ul style="list-style-type: none"> ▪ on - Creates a VRRP Virtual Router ▪ off - Removes a VRRP Virtual Router ▪ priority-delta - Configures the Priority Delta value <p>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).</p> <p>Otherwise, network destinations will become unreachable, etc. This coordinated failover is achieved by adding all dependent interfaces to the list of monitored interfaces.</p> <p>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.</p> <p>Refer to the following commands for additional details:</p> <ul style="list-style-type: none"> ▪ set vrrp interface <VALUE> monitored-circuit vrid <VALUE> priority ▪ set vrrp interface <VALUE> monitored-circuit vrid <VALUE> monitored-interface <VALUE> priority-delta
<pre>monitored-circuit vrid VALUE {on off}</pre>	<p>Creates (on) or removes (off) a VRRP Virtual Router.</p>
<pre>monitored-circuit vrid VALUE preempt-mode {on off}</pre>	<p>Configures Preempt Mode for the given Virtual Router.</p> <p>When Preempt Mode is enabled, if the Virtual Router has a higher Priority than the current VRRP Master, it preempts the VRRP Master.</p> <p>If Preempt Mode is disabled, all Virtual Routers that have monitored interfaces, are participating to avoid potential split-brain network topology.</p> <p>For more information on the implications of disabling Preempt Mode, see the help text for the <code>set mcvr vrid <VALUE> monitor-vrrp</code> command.</p> <ul style="list-style-type: none"> ▪ Range: on, or off ▪ Default: off

Parameter	Description
<pre>monitored-circuit vrid VALUE priority VALUE</pre>	<p>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.</p> <p>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.</p> <ul style="list-style-type: none"> ▪ Range: default, or 1 - 254 ▪ Default: 100
<pre>monitored-circuit vrid VALUE vmac- mode {default- vmac extended- vmac interface- vmac static- vmac VALUE}</pre>	<p>Configures how the Virtual MAC (VMAC) address is calculated for the given Virtual IP Address.</p> <p>Each Virtual IP Address for a Virtual Router implies the existence of a virtual network interface.</p> <ul style="list-style-type: none"> ▪ Range: <ul style="list-style-type: none"> • <code>default-vmac</code> - Generates the VMAC using the standard method described in Section 7.3 of RFC 3768. • <code>extended-vmac</code> - Generates the VMAC using an extended range of uniqueness by dynamically calculating 3 bytes of the VMAC instead of only 1. • <code>interface-vmac</code> - Configures the VMAC to use the interface hardware MAC address. • <code>static-vmac <VALUE></code> - Configures the Virtual Router to use a specified static VMAC address. ▪ Default: <code>default-vmac</code>
<pre>set vrrp interface VALUE off</pre>	<p>Deletes all Virtual Routers from the interface.</p>
<pre>set virtual- router legacy off</pre>	<p>Disables legacy VRRPv2 configuration.</p> <p>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.</p> <p>Hence, you must replace all legacy "virtual-router" configuration commands using the equivalent "monitored-circuit" configuration commands.</p>


Configuring the VRRP Cluster for Advanced VRRP in SmartConsole

Follow the [R81.20 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	535
General Configuration Considerations	537
Firewall Policies	537
Monitored-Circuit VRRP in Switched Environments	537

 **Important** - Scalable Platforms (Maestro and Chassis) do **not** support this feature (Known Limitation MBS-2521).

This section shows known issues with VRRP configurations and fixes.


Read this section before contacting [Check Point Support](#).

Traces (Debug) for VRRP

You can log information about errors and events for troubleshooting VRRP.

Enabling traces for VRRP

Step	Instructions
1	In the navigation tree, click Routing > Routing Options .
2	In the Trace Options section, in the Filter Visible Tables Below drop down list, select VRRP .
3	<p>In the VRRP table, select the applicable options. We recommend you select All.</p> <p>To select several specific options:</p> <ol style="list-style-type: none"> Press and hold the CTRL key on the keyboard. Left-click on the applicable options. The selected options become highlighted. <p>To select several consecutive options:</p> <ol style="list-style-type: none"> Left-click on the first consecutive applicable option. Press and hold the SHIFT key on the keyboard. Left-click on the last consecutive applicable option. The selected options become highlighted.

Step	Instructions
4	Click Add . The selected options show Enabled .
5	Scroll to the top of this page.
6	In the Routing Options section, click Apply . The Gaia restarts the routing subsystem and signals it to reread its configuration. The debug information is saved in <code>/var/log/routed.log*</code> files and <code>/var/log/routed_messages*</code> files.  Note - As an <i>example</i> , see sk84520 - How to debug OSPF and Routed daemon on Gaia .

Disabling traces for VRRP

Step	Instructions
1	In the navigation tree, click Routing > Routing Options .
2	In the Trace Options section, in the Filter Visible Tables Below drop down list, select VRRP . 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	540
On Check Point Maestro	540
On Open Servers and Virtual Machines	541
Activating a License in Gaia Portal	542

You can view, add, or delete licenses in one of these ways:

- In Gaia Portal > **Maintenance** section > **License Status** page.
 -  **Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.
- With the "cplic db_add" and "cplic del" commands (see the [R81.20 CLI Reference Guide](#)).
 -  **Important** - On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
 -  **Note** - While all the "cplic" commands are available in Gaia, they are not grouped into a Gaia feature.

On Check Point Appliances

If a Management Server and its managed Security Gateways are *able* to connect to Check Point User Center, licenses and contracts activated and updated automatically.

If a Management Server and its managed Security Gateways are **not** able to connect to Check Point User Center, then manage licenses and contracts in either SmartConsole or the command line.

On Check Point Maestro

See the [R81.20 Quantum Maestro Administration Guide](#) > Chapter *Configuring Security Groups* > Section *License Installation*.


On Open Servers and Virtual Machines

If a Management Server and its managed Security Gateways are *able* to connect to Check Point User Center, then activate the license during the Gaia First Time Configuration Wizard, or later in Gaia Portal, SmartConsole, or the command line. After the activation is completed, licenses and contracts are updated automatically.

If a Management Server and its managed Security Gateways are **not** able to connect to Check Point User Center, then manage licenses and contracts in either SmartConsole or the command line.

Activating a License in Gaia Portal

Activating a license manually online

Step	Instructions
1	<p>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:</p> <p> Note - The prerequisite for Security Gateways and Cluster Members is to establish a Secure Internal Communication (SIC Trust) with a Management Server.</p> <ul style="list-style-type: none"> ▪ To configure the same default proxy for all objects: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> • 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	<p>With a web browser, connect to Gaia Portal at:</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 5px;"> <p><code>https://<IP address of Gaia Management Interface></code></p> </div>
3	<p>In the navigation tree, click Maintenance > License Status.</p>


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.

Activating a license manually offline

Step	Instructions
1	With a web browser, connect to Gaia Portal at: <pre>https://<IP address of Gaia Management Interface></pre>
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 .

Deleting an installed license

Step	Instructions
1	With a web browser, connect to Gaia Portal at: <pre>https://<IP address of Gaia Management Interface></pre>
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 [R81.20 CLI Reference Guide](#)).

Snapshot Management

A snapshot is a backup of the system settings and products. It includes:

- File system, with customized files
- System configuration (interfaces, routing, hostname, and similar)
- Software Blades configuration
- Management database (on a Security Management Server or a Multi-Domain Server)

A snapshot is very large. A snapshot includes the entire root partition, part of the `/var/log` partition, and other important files.

For this reason, snapshots cannot be scheduled the same way that Backups can.

Backup and Restore is the preferred method of recovery.

Notes:

- When Gaia creates a snapshot, all system processes and services continue to run.
Policy enforcement is not interrupted.
- You can import a snapshot created on a different software release or on this software release.
You must import a snapshot on the appliance or open server of the same hardware model, from which it was exported.
- After importing the snapshot, you must activate the device license from the Gaia Portal or the User Center.
- We do not recommend to use snapshots as a way of regularly backing up your system.
System Backup is the preferred method.
Schedule system backups on a regular basis, daily or weekly, to preserve the Gaia OS configuration and Firewall database.

Best Practice for creating snapshots:

- Immediately after Gaia installation and first time configuration.
- Before making a major system change, such as installing a hotfix or route changes.

 **Important:**

- After you take the Gaia snapshot, export it to an external storage. You must **not** rename the exported image. If you rename a snapshot image, it is not possible to revert to it.
- See [sk98068: Gaia Limitations after Snapshot Recovery](#).
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Snapshot operations (in the Global Gaia Portal or Global Gaia Clish).
To collect or import a Gaia Snapshot in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

Snapshot Options

Option	Description
Revert	Reverts to a user created image. Reverts to a factory default image, which is automatically created on Check Point appliances by the installation or upgrade procedure.
Delete	Deletes an image from the local file system.
Export	Exports an existing image. 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 local file system. This saves disk space.
Import	Imports an exported image.
View	Shows a list of images that are stored locally.

Notes:


- You must not rename the exported image. If you rename a snapshot image, it is not possible to revert to it.
- You can import a snapshot only on the machine of the same hardware type, from which it was exported.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Snapshot operations (in the Global Gaia Portal or Global Gaia Clish).
To collect or import a Gaia Snapshot in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

Snapshot Prerequisites

Important:

Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Snapshot operations (in the Global Gaia Portal or Global Gaia Clish). To collect or import a Gaia Snapshot in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

- We recommended to configure the GRUB password. See ["System Passwords" on page 277](#).
- Before you **revert** to a snapshot on a new appliance, or after a reset to factory defaults, you must run the Gaia First Time Configuration Wizard and configure the same settings as before you created the snapshot.
- Before you **create** a new snapshot image, make sure the appliance or storage destination meets these prerequisites:
 - The required free disk space is the size of the system root partition multiplied by 1.15.

-  **Note** - A snapshot image is created in unallocated space on the disk. Not all of the unallocated space on a disk can be used for snapshots. To find out if you have enough free space for snapshots:

Step	Instructions
1	Connect to the command line on the Gaia computer.
2	Log in to Gaia Clish.
3	On Scalable Platforms, go to Gaia gClish: Type <code>gclish</code> and press Enter.
4	Run: <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <pre>show snapshots</pre> </div> 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.

Snapshot Management in Gaia Portal

Important:

- On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Snapshot operations (in the Global Gaia Portal or Global Gaia Clish).
To collect or import a Gaia Snapshot in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.


Before you create a snapshot image, make sure the appliance or storage destination meets the prerequisites.

Creating a new snapshot image

Step	Instructions
1	In the navigation tree, click Maintenance > Snapshot Management .
2	In the Snapshot Management section, click New . 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 <code>/var/log/</code> partition: <ol style="list-style-type: none"> Connect to the command line on Gaia. Log in to the Expert mode. Run: <pre>df -kh egrep "Mounted /var/log"</pre> Check the value in the <code>Avail</code> 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 .

Scheduled Snapshots

To configure scheduled snapshots in Gaia Clish, see "[Snapshot Management in Gaia Clish - Scheduled Snapshots](#)" on page 562.

Step	Instructions
1	In the navigation tree, click Maintenance > Snapshot Management . Refer to the Scheduled Snapshots section.
2	Click the Scheduled Snapshot Settings button.
3	Select the Enable option to configure a schedule. (Clear the Enable option to disable the configured schedule.)
4	<p>In the Snapshot name field, enter the name of the job. The final name of the snapshot consists of two parts - the prefix (you enter in this field) and the time stamp (format is hard-coded):</p> <pre><Prefix>_<YYYY_MM_DD__HH_mm></pre> <ul style="list-style-type: none"> ▪ The prefix maximal length is 15 characters. ▪ The prefix can consist only of letters, numbers, or underscore "_". ▪ Default prefix: <code>snap</code>.
5	Optional: In the Description field, enter the description of the snapshot image. Default description : <code>default_snapshot</code>
6	<p>In the Destination section, configure the location of the backup file:</p> <ul style="list-style-type: none"> ▪ Local LVM To keep the collected snapshot locally in the <code>/var/log/CPbackup/backups/</code> directory. ▪ SCP server To send the collected snapshot to an SCP server. Enter the IP address, User name, Password, and Upload path. <ul style="list-style-type: none"> ❗ Important: <ul style="list-style-type: none"> • First, you must follow sk164234 to configure the SCP server as a trusted host on Gaia. • The username must have permissions to delete files on the SCP server. ▪ FTP server To send the collected snapshot to an FTP server. Enter the IP address, User name, Password, and Upload path. <ul style="list-style-type: none"> ❗ Important -The username must have permissions to delete files on the FTP server.

Step	Instructions
7	<p>In the Recurrence section, configure the frequency (Daily, Weekly, Monthly, Minute Interval, Hourly) for this snapshot.</p> <p> Note - This is available only for the Local LVM location.</p>
8	<p>Optional: In the Retention Policy section, configure the snapshot retention policy:</p> <ul style="list-style-type: none">▪ In the Maximum snapshots field, configure the maximum number of snapshot images to save. If the new snapshot image exceeds this number, then Gaia deletes the oldest snapshot.▪ In the Keep disk-space above (in GB) field, configure the amount of free disk space to maintain at all times. If the new snapshot image exceeds this number, then Gaia does not create the new snapshot image.▪ In the Minimum snapshots field, configure the minimum number of snapshot images to save. When Gaia deletes the old snapshots, it always keeps the specified number of snapshot images. <p> Important:</p> <ul style="list-style-type: none">▪ The retention policy supports only the local LVM volume.▪ The retention policy applies only to the new snapshots (and does not apply to existing snapshots).▪ If the retention policy fails to calculate the configured criteria, Gaia does not create the new snapshot image. In this case, Gaia does not show a notification. An administrator must manually check why Gaia did not create the new snapshot image.

Step

Instructions

The disk space limit you need to configure is:

```
Limit = (Available free disk space for all snapshot
images) - (Free disk space to maintain)
```

Where:

```
Available free disk space for all snapshot images =
= (Output of: vdisplay | grep Free) - 1.1*(Output of:
lvs | egrep "LSize|lv_current")
```

Example

For more information, see [sk80260](#).

- A. Log in to the Expert mode.
- B. Get the free disk space in volume groups:

```
[Expert@MyGaia:0]# vdisplay | grep Free
Free PE / Size          4090 / 127.81 GiB
[Expert@MyGaia:0]#
```

- C. Get the free disk space in the "lv_current" partition:

```
[Expert@MyGaia:0]# lvs | egrep "LSize|lv_current"
LV          VG          Attr          LSize  Pool Origin
Data%      Meta%      Move Log Cpy%Sync Convert
lv_current vg_splat  -wi-ao----- 40g
[Expert@MyGaia:0]#
```

- D. Calculate the free disk space available for snapshot images:

```
Available free disk space for all snapshot images =
= (Output of "vdisplay" command) - 1.1*(Output of
"lvs" command) =
= (127.81) - 1.1*(40) = 83.81 GB
```

- E. Calculate the limit for the scheduled snapshot task:
For example, you need to maintain 30 GB of free disk space at all times.

```
Limit = (Available free disk space for all snapshot
images) - (Free disk space to maintain) =
= (83.81 GB) - (30 GB) = 53.81 GB
```

9

Click **Apply**.

The scheduled snapshot configuration appears in the **Scheduled Snapshot** section.

Troubleshooting

- If a snapshot was not created, examine these files:

```
/var/log/messages*
```

- If a snapshot was created, but there were some issues, examine this file:

```
/var/log/CPsnapshot/<Snapshot Name>_<Timestamp>
```

Snapshot Management in Gaia Clish - Regular Snapshots

Important:

- On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Snapshot operations (in the Global Gaia Portal or Global Gaia Clish).
To collect or import a Gaia Snapshot in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

Before you create a snapshot image, make sure the appliance or storage destination meets the prerequisites - see "[Snapshot Prerequisites](#)" on page 548.

Description

Manage system images (snapshots).


Syntax

Creating a new snapshot image

These commands only create a new snapshot image.

Creating a new snapshot image as a local LVM volume

```
add snapshot-onetime name <Name of Snapshot> [description  
"<Description of Snapshot>"]
```

-  **Note** - Gaia Snapshots are not files, but Logical Volume Management (LVM) volumes. Gaia stores these snapshots as a disk partition. To show the list of virtual drives, run the "lvs" command in the Expert mode.

Creating a new snapshot image and exporting it to a local file

```
add snapshot-onetime name <Name of Snapshot> [description  
"<Description of Snapshot>"] target local path <Local Path>
```

Creating a new snapshot image as a file and uploading it to an FTP server

```
add snapshot-onetime name <Name of Snapshot> [description  
"<Description of Snapshot>"] target ftp ip <IPv4 Address of  
FTP Server> path <Path on FTP Server> username <User Name on  
FTP Server> password <Password in Plain Text>
```

Creating a new snapshot image as a file and uploading it to an SCP server

```
add snapshot-onetime name <Name of Snapshot> [description  
"<Description of Snapshot>"] target scp ip <IPv4 Address of  
SCP Server> path <Path on SCP Server> username <User Name on  
SCP Server> password <Password in Plain Text>
```

Exporting an existing snapshot image

These commands only export an existing snapshot image from a local LVM volume.

Exporting an existing snapshot image and saving it as a local file

```
set snapshot-onetime export <Name of Exported Snapshot> target  
local path <Local Path>
```

Exporting an existing snapshot image as a file and uploading it to an FTP server

```
set snapshot-onetime export <Name of Exported Snapshot> target  
ftp path <Path on FTP Server> ip <IPv4 Address of FTP Server>  
username <User Name on FTP Server> password <Password in Plain  
Text>
```

Exporting an existing snapshot image as a file and uploading it to an SCP server

```
set snapshot-onetime export <Name of Exported Snapshot> target  
scp path <Path on SCP Server> ip <IPv4 Address of SCP Server>  
username <User Name on SCP Server> password <Password in Plain  
Text>
```

Importing an existing snapshot image

These commands only import an existing snapshot image file and store it on Gaia as a local LVM volume.

Importing an existing snapshot image from a local file

```
set snapshot-onetime import <Name of Imported Snapshot> target  
local path <Local Path>
```

Importing an existing snapshot image from an FTP server

```
set snapshot-onetime import <Name of Imported Snapshot> target  
ftp ip <IPv4 Address of FTP Server> path <Path on FTP Server>  
username <User Name on FTP Server> password <Password in Plain  
Text>
```

Importing an existing snapshot image from an SCP server

```
set snapshot-onetime import <Name of Imported Snapshot> target  
scp ip <IPv4 Address of SCP Server> path <Path on SCP Server>  
username <User Name on SCP Server> password <Password in Plain  
Text>
```

Importing and reverting to an existing snapshot image


These commands import an existing snapshot image, store it on Gaia as a local LVM volume, and then revert to that imported snapshot image.

Important:

- When Gaia reverts to a snapshot, it overwrites the existing running configuration and settings. Make sure you know credentials of the snapshot, to which you revert.
- Before you **revert** to a snapshot on a new appliance, or after a reset to factory defaults, you must run the Gaia First Time Configuration Wizard and configure the same settings as before you created the snapshot.
- If you reverted a snapshot on a Security Gateway / Cluster Member, install the Security Policy.

Importing and reverting an existing snapshot image from a local LVM volume

```
set snapshot-onetime revert target lvm name <External Name of Snapshot>
```

-  **Note** - Gaia Snapshots are not files, but disk volumes. Gaia stores these snapshots as a disk partition. To show the list of virtual drives, run the "lvs" command in the Expert mode.

Importing and reverting an existing snapshot image from a local file

```
set snapshot-onetime revert target local name <Imported Name of Snapshot> path <Local Path>
```

Importing and reverting an existing snapshot image from an FTP server

```
set snapshot-onetime revert target ftp name <Imported Name of Snapshot> path <Path on FTP Server> ip <IPv4 Address of FTP Server> username <User Name on FTP Server> password <Password in Plain Text>
```

Import and reverting an existing snapshot image from an SCP server

```
set snapshot-onetime revert target scp name <Imported Name of Snapshot> path <Path on SCP Server> ip <IPv4 Address of SCP Server> username <User Name on SCP Server> password <Password in Plain Text>
```


Viewing existing snapshot images

```
show snapshots
```

```
show snapshot <Name of Snapshot>  
  all  
  date  
  description  
  size
```

Deleting a local snapshot image

```
delete snapshot <Name of Snapshot>
```

-  **Important** - After you add, configure, or delete features, run the "save config" command to save the settings permanently.

Parameters

Parameter	Description
<code>name <Name of Snapshot></code>	Configures the name of the new snapshot image. You must enter a string that does not contain spaces.
<code>name <Name of Exported Snapshot></code>	Configures the name, under which the exported snapshot image file is stored. You must enter a string that does not contain spaces. You must not add an extension.
<code>name <Name of Imported Snapshot></code>	Configures the name, under which the imported snapshot image is stored on this Gaia. You must enter a string that does not contain spaces.
<code>description "<Description of Snapshot>"</code>	Optional. Configures the description of the snapshot image. You must enclose the text in double quotes, or enter the string that does not contain spaces.
<code>export <Name of Snapshot></code>	Exports the snapshot image by the specified name. You must enter a string that does not contain spaces.
<code>import <Name of Snapshot></code>	Imports the snapshot image by the specified name. You must enter a string that does not contain spaces.
<code>target</code>	When you create or export a snapshot, specifies the destination for the snapshot image. When you import a snapshot, specifies the source of the snapshot image. <ul style="list-style-type: none"> ▪ <code>target lvm</code> - Local LVM volume on this Gaia ▪ <code>target local</code> - Local file on this Gaia ▪ <code>target ftp</code> - Remote FTP server ▪ <code>target scp</code> - Remote SCP server
<code>ip</code>	Specifies the IPv4 address of the remote server: <ul style="list-style-type: none"> ▪ <code>ip <IPv4 Address of FTP Server></code> Specifies the IPv4 address of the remote FTP server. ▪ <code>ip <IPv4 Address of SCP Server></code> Specifies the IPv4 address of the remote SCP server.

Parameter	Description
path	<p>Specifies the path to the snapshot image file.</p> <p>When you export, this is the path to the directory (/path_to/directory/).</p> <p>When you import, this is the path to the directory and the snapshot image (/path_to/directory/snapshot).</p> <ul style="list-style-type: none"> ▪ path <Local Path> Specifies the local absolute path on this Gaia. ▪ path <Path on FTP Server> Specifies the path on the remote FTP server. ▪ path <Path on SCP Server> Specifies the path on the remote SCP server.
username	<p>Specifies the login username on the remote server:</p> <ul style="list-style-type: none"> ▪ 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>	<p>Specifies the password (in plain text) required to log in to the remote server.</p>

Examples

- Creating a new snapshot image locally as a file:

```
gaia> add snapshot-onetime name 1st_image_after_install
description "First image after installation" target local
path /var/log/
```

- Creating a new snapshot image as a file and uploading it to an SCP server:

```
gaia> add snapshot-onetime name 1st_image_after_install
description "First image after installation" target scp ip
192.168.20.30 path /var/log/ username scp_admin password
123456
```

- Importing an existing snapshot image from an SCP server:

```
gaia> set snapshot-onetime import 1st_image_after_install
target scp ip 192.168.20.30 path /var/log/ username scp_
admin password 123456
```

Troubleshooting

- If a snapshot was not created, examine these files:

```
/var/log/messages*
```

- If a snapshot was created, but there were some issues, examine this file:

```
/var/log/CPsnapshot/<Snapshot Name>_<Timestamp>
```

Snapshot Management in Gaia Clish - Scheduled Snapshots

Important:

- On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Snapshot operations (in the Global Gaia Portal or Global Gaia Clish).
To collect or import a Gaia Snapshot in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

Before you create a snapshot image, make sure the appliance or storage destination meets the prerequisites.

Description

Manage system images (snapshots).

From R81, you can also configure scheduled system images (snapshots).

Notes:

- R81.20 supports only *one* scheduled snapshot task.
- It is not possible to change any of the settings in the scheduled snapshot task. You must configure the task from scratch.
- To configure scheduled snapshots in Gaia Portal, see "[Snapshot Management in Gaia Portal](#)" on page 549.

Syntax

```

set snapshot-scheduled activation {enabled | disabled}

set snapshot-scheduled recurrence
  daily time <HH:MM>
  hourly hours {<Hours> | all} at <0-59>
  interval minutes <1-59>
  monthly month {<Months> | all} days <Days> time <HH:MM>
  weekly days {<Days> | all} time <HH:MM>

set snapshot-scheduled retention-policy
  keep-disk-space-above-in-GB <Limit>
  max-snapshots-to-keep <1-9999>
  min-snapshots-to-keep <1-9999>

set snapshot-scheduled settings snapshot-name-prefix <Prefix of
Snapshot Name> description <Description of Snapshot>
  target ftp ip <IPv4 Address of FTP Server> path <Path on FTP
Server> username <User Name on FTP Server> {password <Password in
Plain Text> | password-hash <Password Hash>}
  target lvm
  target scp ip <IPv4 Address of SCP Server> path <Path on SCP
Server> username <User Name on SCP Server> {password <Password in
Plain Text> | password-hash <Password Hash>}

show snapshot-scheduled <Prefix of Snapshot Name>

```

Procedure

1. Configure the scheduled snapshot task

R81.20 supports only *one* of these scheduled snapshot tasks.


You can only configure one task for a local LVM volume, one task for an FTP server, or one task for an SCP server.

Creating a new snapshot image as a local LVM volume

```

set snapshot-scheduled settings snapshot-name-prefix
<Prefix of Snapshot Name> [description "<Description of
Snapshot>"] target lvm

```

 **Note** - Gaia Snapshots are not files, but Logical Volume Management (LVM) volumes. Gaia stores these snapshots as a disk partition. To show the list of virtual drives, run the "lvs" command in the Expert mode.

Creating a new snapshot image as a file and uploading it to an SCP server

```
set snapshot-scheduled settings snapshot-name-prefix
<Prefix of Snapshot Name> [description "<Description of
Snapshot>"] target scp ip <IPv4 Address of SCP Server>
path <Path on SCP Server> username <User Name on SCP
Server> {password <Password in Plain Text> | password-hash
<Password Hash>}
```

Important:

- First, you must follow [sk164234](#) to configure the SCP server as a trusted host on Gaia.
- The username must have permissions to delete files on the SCP server.

Creating a new snapshot image as a file and uploading it to an FTP server

```
set snapshot-scheduled settings snapshot-name-prefix
<Prefix of Snapshot Name> [description "<Description of
Snapshot>"] target ftp ip <IPv4 Address of FTP Server>
path <Path on FTP Server> username <User Name on FTP
Server> {password <Password in Plain Text> | password-hash
<Password Hash>}
```

- Important** -The username must have permissions to delete files on the FTP server.

2. Configure the recurrence for the snapshot schedule**Running one time on each day at specified time**

```
set snapshot-scheduled recurrence daily time <HH:MM>
```

Running several times each day at specified times

```
set snapshot-scheduled recurrence hourly hours {<Hours> |
all} at <0-59>
```

Running several times each day at specified intervals

```
set snapshot-scheduled recurrence interval minutes <1-59>
```

Running in specified months on specified days and at specified time

```
set snapshot-scheduled recurrence monthly month {<Months>
| all} days <Days> time <HH:MM>
```

Running each week on specified days of week and at specified time

```
set snapshot-scheduled recurrence weekly days {<Days> |  
all} time <HH:MM>
```

3. Configure the snapshot retention policy** Important:**

- This step applies only if you save the new snapshot image as a local LVM volume.
- The retention policy applies only to the new snapshots (and does not apply to existing snapshots).
- When Gaia creates new snapshots, it deletes the oldest snapshot that exceeds the configured policy parameters.

Configuring the maximum number of snapshot images to save

```
set snapshot-scheduled retention-policy max-snapshots-to-  
keep <1-9999>
```

Configuring the minimum number of snapshot images to save

```
set snapshot-scheduled retention-policy min-snapshots-to-  
keep <1-9999>
```

Configuring the amount of free disk space to maintain

This command lets you configure how much of the disk space must remain free at all times:

```
set snapshot-scheduled retention-policy keep-disk-space-
above-in-GB <Limit>
```

The limit you need to configure with this command is:

```
Limit = (Available free disk space for all snapshot
images) - (Free disk space to maintain)
```

Where:

```
Available free disk space for all snapshot images =
= (Output of: vdisplay | grep Free) - 1.1*(Output of: lvs
| egrep "LSize|lv_current")
```

Example

For more information, see [sk80260](#).

- a. Log in to the Expert mode.
- b. Get the free disk space in volume groups:

```
[Expert@MyGaia:0]# vdisplay | grep Free
Free PE / Size          4090 / 127.81 GiB
[Expert@MyGaia:0]#
```

- c. Get the free disk space in the "lv_current" partition:

```
[Expert@MyGaia:0]# lvs | egrep "LSize|lv_current"
LV          VG          Attr          LSize  Pool Origin
Data%      Meta%      Move Log Cpy%Sync Convert
lv_current vg_splat  -wi-ao---- 40g
[Expert@MyGaia:0]#
```

- d. Calculate the free disk space available for snapshot images:

```
Available free disk space for all snapshot images =
= (Output of "vdisplay" command) - 1.1*(Output of
"lvs" command) =
= (127.81) - 1.1*(40) = 83.81 GB
```

- e. Calculate the limit for the scheduled snapshot task:

For example, you need to maintain 30 GB of free disk space at all times.

```
Limit = (Available free disk space for all snapshot
images) - (Free disk space to maintain) =
= (83.81 GB) - (30 GB) = 53.81 GB
```

- f. Log in to Gaia Clish.
- g. Configure the limit (round up or round down the limit you calculated in the previous step):

```
set snapshot-scheduled retention-policy keep-disk-
space-above-in-GB 54
save config
```

4. Enable the scheduled snapshot feature

- To control this feature in Gaia Clish:

- To enable the snapshot schedule:

```
set snapshot-scheduled activation enabled
```

 **Important:**

- You must run this command after you configure a scheduled snapshot for the first time.
- You must run this command after any change in the existing configuration of a scheduled snapshot.

- To disable the snapshot schedule:

```
set snapshot-scheduled activation disabled
```

- To control this feature in Gaia Portal:

- a. In the navigation tree, click **Maintenance > Snapshot Management**.
- b. In the section **Scheduled Snapshots**:
 - To enable the snapshot schedule, select **Activate / Deactivate**.
 - To disable the snapshot schedule, clear **Activate / Deactivate**.
- c. Click **Apply**.


5. Examine the scheduled snapshot configuration

```
show snapshot-scheduled
```


Deleting a scheduled snapshot


You can only disable the snapshot schedule to stop the scheduled task:

```
set snapshot-scheduled activation disabled
```

-  **Important** - After you add, configure, or delete features, run the "save config" command to save the settings permanently.

Parameters

Parameter	Description
snapshot-name-prefix <i><Prefix of Snapshot Name></i>	The final name of the snapshot consists of two parts - the prefix (configured by the user) and the time stamp (format is hard-coded): <i><Prefix>_<YYYY_MM_DD__HH_mm></i> <ul style="list-style-type: none"> ▪ The prefix maximal length is 15 characters. ▪ The prefix can consist only of letters, numbers, or underscore "_". ▪ Default prefix: <code>snap</code>.
description " <i><Description of Snapshot></i> "	Optional. Configures the description of the snapshot image. You must enclose the text in double quotes, or enter the string that does not contain spaces. Default description : <code>default_snapshot</code>
target	Specifies the destination for the snapshot image: <ul style="list-style-type: none"> ▪ <code>target lvm</code> - Local LVM volume on this Gaia (this is the default) ▪ <code>target ftp</code> - Remote FTP server ▪ <code>target scp</code> - Remote SCP server
ip	Specifies the IPv4 address of the remote server: <ul style="list-style-type: none"> ▪ <code>ip <IPv4 Address of FTP Server></code> Specifies the IPv4 address of the remote FTP server. ▪ <code>ip <IPv4 Address of SCP Server></code> Specifies the IPv4 address of the remote SCP server. <p> Important - First, you must follow sk164234 to configure the SCP server as a trusted host on Gaia.</p>

Parameter	Description
path	<p>Specifies the path to the snapshot image file:</p> <ul style="list-style-type: none"> ■ path <i><Local Path></i> Specifies the local absolute path on this Gaia to save the snapshot image file (/path_to/directory/). ■ path <i><Path on FTP Server></i> Specifies the path on the remote FTP server where to upload the snapshot image file (/path_to/directory/). ■ path <i><Path on SCP Server></i> Specifies the path on the remote SCP server where to upload the snapshot image file (/path_to/directory/).
username	<p>Specifies the login username on the remote server:</p> <ul style="list-style-type: none"> ■ username <i><User Name on FTP Server></i> Specifies the user name required to log in to the remote FTP server. ■ username <i><User Name on SCP Server></i> Specifies the user name required to log in to the remote SCP server. <p> Important - The username must have permissions to delete files on the remote server.</p>
password <i><Password in Plain Text></i>	<p>Specifies the password (in plain text) required to log in to the remote server.</p>
password-hash <i><Password Hash></i>	<p>Specifies the hash of the password required to log in to the remote server.</p>

Parameter	Description
<pre>recurrence daily time <HH:MM></pre>	<p>Specifies that the job should run once a day - every day, at specified time.</p> <p>Enter the time of day in the 24-hour clock format - <Hours>:<Minutes>.</p> <p>Example:</p> <pre>HostName> set snapshot-scheduled recurrence daily time 14:35</pre> <pre>HostName> show snapshot-scheduled Scheduled snapshot configuration: ... Every day at 14:35</pre>
<pre>recurrence hourly hours {<Hours> all} at <Minutes 0-59></pre>	<p>Specifies that the job must run many times during the day - at the specified time.</p> <ul style="list-style-type: none"> ▪ You can specify a single hour of a day by a number from 0 to 23. ▪ You can specify several hours of a day. Enter the hours separated by commas. Example - for hours 14, 15, and 16, enter: 14,15,16 ▪ To specify each hour of a day, enter: all ▪ You must specify the minutes of each configured hour by a number from 0 to 59. <p>Example:</p> <pre>HostName> set snapshot-scheduled recurrence hourly hours 14,15,16 at 35</pre> <pre>HostName> show snapshot-scheduled Scheduled snapshot configuration: ... Every day at 14:35,15:35,16:35</pre>

Parameter	Description
<pre>recurrence interval minutes <1-59></pre>	<p>Specifies that the job must run many times during the day - at intervals of the specified number of minutes.</p> <p>Example:</p> <pre>HostName> set snapshot-scheduled recurrence interval minutes 30</pre> <pre>HostName> show snapshot-scheduled Scheduled snapshot configuration: ... Every 30 minutes.</pre>
<pre>recurrence monthly month {<Months> all} days <Days> time <HH:MM></pre>	<p>Specifies that the job must run once a month - on the specified months, on the specified dates, and at the specified time.</p> <ul style="list-style-type: none"> ▪ Specify the months by numbers from 1 to 12: January = 1, February = 2, ..., December = 12. ▪ To specify several months, enter their numbers separated by commas. Example - for January, February, and March, enter: 1,2,3 ▪ To specify each month of the year, enter: all ▪ Specify the dates of a month by numbers from 1 to 31. ▪ To specify several dates, enter their numbers separated by commas. Example - for 1st, 2nd and 3rd day of month, enter: 1,2,3 <p>Example:</p> <pre>HostName> set snapshot-scheduled recurrence monthly month 1,2,3 days 1,2,3 time 14:35</pre> <pre>HostName> show snapshot-scheduled Scheduled snapshot configuration: ... Each January, February, March on days 1, 2, 3 at 14:35</pre>

Parameter	Description
<pre>recurrence weekly days {<Days> all} time <HH:MM></pre>	<p>Specifies that the job must run once a week - on specified days of week, and at specified time.</p> <ul style="list-style-type: none"> ■ Specify the days of a week by numbers from 0 to 6: Sunday = 0, Monday = 1, Tuesday = 2, Wednesday = 3, Thursday = 4, Friday = 5, Saturday = 6. ■ To specify several days of a week, enter their numbers separated by commas. Example- for Sunday, Monday, and Tuesday, enter: 0,1,2 ■ To specify each day of the week, enter: all <p>Example:</p> <pre>HostName> set snapshot-scheduled recurrence weekly days 1,3 time 14:35</pre> <pre>HostName> show snapshot-scheduled Scheduled snapshot configuration: ... Every week on Monday, Wednesday at 14:35</pre>
<pre>retention-policy</pre>	<p>Configures the retention policy when you save the new snapshot image as a local LVM volume: (when Gaia creates new snapshots, it deletes the oldest snapshot that exceeds the configured policy parameters)</p> <ul style="list-style-type: none"> ■ <code>max-snapshots-to-keep <1-9999></code> Specifies the maximum number of snapshot images to save. The default threshold is: 9999. ■ <code>min-snapshots-to-keep <1-9999></code> Specifies the minimum number of snapshot images to save. The default threshold is: 1. ■ <code>keep-disk-space-above-in-GB <1-Maximum></code> Specifies the amount of free disk space to maintain between 1 GB and the maximum available space.

Parameter	Description
activation {enabled disabled}	Enables or disables the snapshot schedule.

Examples

- **Creating a daily snapshot image as a local LVM volume:**

```
gaia> set snapshot-scheduled settings snapshot-name-prefix
Daily description "Daily snapshot image" target lvm
gaia>
gaia> set snapshot-scheduled recurrence daily time 22:00
gaia>
gaia> set snapshot-scheduled retention-policy max-snapshots-
to-keep 10
gaia>
gaia> set snapshot-scheduled retention-policy min-snapshots-
to-keep 3.
gaia>
gaia> set snapshot-scheduled retention-policy keep-disk-
space-above-in-GB 50
gaia>
gaia> show snapshot-scheduled
Scheduled snapshot configuration:
name: Daily
description: Daily
activation: disabled
target: lvm
max-snapshots-to-keep: 10
min-snapshots-to-keep: 3
keep-disk-space-above-in-GB: 50
Every day at 22:00
gaia>
gaia> set snapshot-scheduled activation enabled
gaia>
gaia> save config
```

- **Creating a monthly snapshot image as a file and uploading it to an SCP server:**


```
gaia> set snapshot-scheduled settings snapshot-name-prefix
Monthly description "Monthly snapshot image" target scp ip
192.168.20.30 path /var/log/my_snapshots/ username backup_
user password 123456
gaia>
gaia> set snapshot-scheduled recurrence monthly month all
days 1 time 22:00
gaia>
gaia> show snapshot-scheduled
Scheduled snapshot configuration:
name: Monthly
description: Monthly
activation: disabled
target: scp
username: backup_user
ip: 192.168.20.30
uploadPath: /var/log/my_snapshots/
Every month on day 1 at 22:00
gaia>
gaia> set snapshot-scheduled activation enabled
gaia>
gaia> save config
```

Troubleshooting

If a scheduled snapshot task fails, there is no notification about it. You must manually check if a snapshot was created.

- If a snapshot was not created, examine these files:

```
/var/log/messages*
```

- If a snapshot was created, but there were some issues, examine this file:

```
/var/log/CPsnapshot/<Snapshot Name>_<Timestamp>
```

Working with Snapshot Management in the Expert mode (g_snapshot)

Important:

- This section applies **only** to Scalable Platforms (Maestro and Chassis).
- On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in the Expert mode on the applicable Security Group.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Snapshot operations (in the Global Gaia Portal or Global Gaia Clish).
To collect or import a Gaia Snapshot in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

Description

Use the "g_snapshot" command in the Expert mode to show and revert snapshots for specific Security Group Members.

This command is different from the Gaia Clish "snapshot" command, which works for all Security Group Members together.

Syntax

```
g_snapshot [-b <SGM IDs>] show
```

```
g_snapshot [-b <SGM IDs>] revert <Name of Snapshot>
```

Parameters

Parameter	Description
show	Shows saved snapshots for the specified Security Group Members.
revert	Restores the specified Security Group Members to the specified snapshot.
<Name of Snapshot>	Specifies the snapshot file name to restore.

Parameter	Description
-b <SGM IDs>	<p>Applies to Security Group Members as specified by the <SGM IDs>.</p> <p><SGM IDs> can be:</p> <ul style="list-style-type: none"> ▪ No <SGM IDs> specified, or all <ul style="list-style-type: none"> • In a Maestro configuration: Applies to all Security Group Members and all Maestro Sites • On 60000 / 40000 Appliances: Applies to all Security Group Members and all Chassis ▪ One Security Group Member (for example, 1_1) ▪ A comma-separated list of Security Group Members (for example, 1_1, 1_4) ▪ A range of Security Group Members (for example, 1_1-1_4) ▪ One Maestro Site, or one Chassis (chassis1, or chassis2) ▪ The Active Maestro Site, or Active Chassis (chassis_active)

Examples

Example 1 - Restore Security Group Members 1_1 and 1_4 to the snapshot called "My_Snapshot"

```
[Expert@HostName-ch0x-0x:0]# g_snapshot -b 1_1,1_4 revert My_Snapshot
```

Example 2 - Restore the Chassis2 to the snapshot called "My_Snapshot"

```
[Expert@HostName-ch0x-0x:0]# g_snapshot -b chassis2 revert My_Snapshot
```

Example 3 - Show the saved snapshots for all Security Group Members on the Chassis1

```
[Expert@HostName-ch0x-0x:0]# g_snapshot -b chassis1 show
```

SMO Image Cloning

 **Important** - This section applies **only** to Scalable Platforms (Maestro and Chassis).

Background

You can use SMO Image Cloning as a tool for cloning images from the Single Management Object (SMO) in a Security Group.

In addition to cloning the SMO version, this mechanism clones all installed Hotfixes, if there are any.

Best Practice:

- On Maestro, we recommend to use this tool when you add a new Maestro Security Appliance (an additional one, or a replacement for a failed one) to a Security Group
- On Chassis, we recommend to use this tool when you add a new SGM (an additional one, or a replacement for a failed one) to a Chassis.


When you activate the auto-clone feature, each Security Group Member updates these:

- MD5 of its local image during reboot
- Admin UP state
- Installed Hotfixes

If the MD5 of the local image is different from the MD5 of the SMO image, the Security Group Member clones the SMO image.

Working with image auto-clone in Gaia gClish:

Command	Instructions
<code>show smo image auto-clone state</code>	Shows the current auto-clone state.
<code>set smo image auto-clone state {on off}</code>	Controls the auto-cloning state: <ul style="list-style-type: none"> ▪ <code>on</code> - enabled ▪ <code>off</code> - disabled

 **Note** - SMO Image Cloning does **not** support Gaia snapshot (the included *fcd*).

Working with image's MD5 in Gaia gClish:

Command	Instructions
<code>show smo image md5sum</code>	Shows the MD5 of the local image.
<code>set smo image md5sum</code>	Updates the MD5 of the local image. This is done automatically on reboot, admin UP, and hotfix installation.

Restoring a Factory Default Image on Check Point Appliance

Factory default images on Check Point appliances are created automatically when you install or upgrade an appliance to another release.

You can restore your Check Point appliance to the factory default image for a specified release.

 **Important** - This procedure overwrites all existing configuration settings.

 **Best Practices:**

- Create a snapshot image before you restore a factory default image.
- Export all existing snapshots from the appliance before you restore a factory default image.

Restoring a Factory Default image in Gaia Portal

Step	Instructions
1	In the navigation tree, click Maintenance > Factory Defaults .
2	Select the factory image.
3	Click Apply .

Restoring a Factory Default image in Gaia Clish

Step	Instructions
1	Connect to the command line on your appliance.
2	Log in to Gaia Clish.
3	Run: <pre style="border: 1px solid black; padding: 5px; margin-top: 10px;">set fcd revert<SPACE><TAB> set fcd revert <Name of Default Image></pre>
4	Follow the instructions on the screen.
5	Reboot: <pre style="border: 1px solid black; padding: 5px; margin-top: 10px;">reboot</pre>

Download SmartConsole

You can download the SmartConsole application package from the Gaia Portal of your Security Management Server / Multi-Domain Server / Standalone Server.

Step	Instructions
1	With a web browser, connect to Gaia Portal at: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <code>https://<IP address of Gaia Management Interface></code> </div>
2	There are two options to get the SmartConsole package. Option 1: <ol style="list-style-type: none"> a. In the navigation tree, click Overview. b. At the top of the page, click the Download Now! button. c. On the download page, click the Download button. d. Save the package. Option 2: <ol style="list-style-type: none"> a. In the navigation tree, click Maintenance > Download SmartConsole. b. Click the Download button. c. On the download page, click the Download button. d. Save the package.
3	Double-click the SmartConsole package and follow the installation wizard instructions.

For next steps in SmartConsole, refer to the [R81.20 Security Management Administration Guide](#).

Hardware Health Monitoring

In This Section:

Showing Hardware Health Information in Gaia Portal	584
Showing Hardware Health Information in Gaia Clish	585
Showing Hardware Information	587

You can monitor these hardware elements:

- Fan sensors - Shows the fan number, status, and speed.
- System Temperature sensors
- Voltage sensors
- Power Supplies (on servers that support it)


In addition, see [sk119232 - Hardware sensors thresholds on Check Point appliances](#).

Important:

- For Maestro, see the [R81.20 Quantum Maestro Administration Guide](#) > Chapter *Logging and Monitoring* > Section *Hardware Monitoring and Control*.
- For Scalable Chassis, see the [R81.20 Quantum Scalable Chassis Administration Guide](#) > Chapter *Logging and Monitoring* > Section *Hardware Monitoring and Control*.

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
<code>show asset<SPACE><TAB></code>	You can run it in Gaia Clish only.
<code>cpstat os -f sensors</code>	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

<code>show asset<SPACE><TAB></code>
<code>show asset all</code>
<code>show asset <Category Name></code>

Parameters

Parameter	Description
<code><SPACE><TAB></code>	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.
<i><Category Name></i>	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 584](#)
- ["Monitoring RAID Synchronization" on page 592](#)
- [sk171436 - HealthCheck Point \(HCP\) Release Updates](#)

Requirement

To save the tool logs on a USB device, you must format it as FAT, FAT32, EXT2, or EXT3 file system. (NTFS or extFAT are not supported.)

Running the tool through the LCD (recommended)

1. In the LCD on your appliance, select the **HW Diagnostics** option.
2. Follow the instructions on the LCD.

Running the tool over the Console connection (recommended)

1. Connect a computer to the console port on your appliance.
Configure the serial connection in your Terminal application.
See the [Getting Started Guide](#) for your appliance model.
2. Reboot your appliance.
3. In the Terminal application, press any key to get the Boot Menu.
4. In the **Boot Menu**, select the option **HW Diagnostics**.


5. Follow the instructions on the screen.
6. When you exit the **HW Diagnostics** tool, the appliance reboots.

Running the tool in the Expert mode (optional)

1. Connect to the command line over SSH (or console port).
2. Log in to the Expert mode.
3. Run:

```
diagMain
```

4. Follow the instructions on the screen.
5. When you exit the **HW Diagnostics** tool, the appliance reboots.

-  **Note** - If you do not want the appliance to reboot:
- a. Connect over SSH for the second time.
 - b. In the second shell, run:

```
killall diagMain
```

Limitations

On 3100 and 3200 appliances: The Network Test using an external loopback device in interfaces eth1, eth2, eth3, and eth4 is not supported.

Monitoring RAID Synchronization

You can monitor the RAID status of the disks to see when the hard disks are synchronized.

If you reboot the appliance before the hard disks are synchronized, the synchronization starts again at the next boot.

Showing RAID Information in Gaia Portal

In the navigation tree, click **Maintenance > RAID Monitoring**.

You can see the information about **RAID Volumes** and **RAID Volume Disks**.

Showing RAID Information in Command Line

Run one of these commands in Gaia Clish or Expert mode:

- The `"raid_diagnostic"` command

Description

This command shows data about the RAID and hard disks, with the percent synchronization done.

Syntax

```
raid_diagnostic
```

Example output from a Smart-1 225 appliance

```
Raid Status:
VolumeID:0 RaidLevel: RAID-1 NumberOfDisks:2 RaidSize:465GB State:DEGRADED Flags:
ENABLED RESYNC _IN_PROGRESS
DiskID:0 DiskNumber:0 Vendor:ATA      ProductID:<HDD Model> Size:465GB State:ONLINE
Flags:NONE
DiskID:1 DiskNumber:1 Vendor:ATA      ProductID:<HDD Model> Size:465GB
State:INITIALIZING Flags:OUT_OF-SYNC SyncState: 12%
```

- DiskID 0 is the left hard disk.
- DiskID 1 is the right hard disk.

- The `"cpstat os -f raidInfo"` command

Description

This command shows almost the same information as the "raid_diagnostic" command, in tabular format.

Syntax

```
cpstat os -f raidInfo
```

Example output

```
Volume list
-----
|Volume id|Volume type|Number of disks|Max LBA  |Volume state|Volume flags|Volume size
(GB)|
-----
|      0|      2|          2|975175680|      0|      1|
465|
-----

Volume list
-----
|Volume id|Disk id|Disk number|Disk vendor|Disk product id|Disk revision|Disk max
LBA|Disk state|Disk flags|Disk sync state|Disk size (GB)|
-----
|      0|      0|          0|NONE      |NONE          |NONE          |      0|
1|      0|          0|          0|          0|          0|
|      0|      1|          1|NONE      |NONE          |NONE          |      0|
1|      0|          0|          0|          0|          0|
-----
```

Shut Down

There are two ways to shut down:

- **Reboot:** Shuts down the system and then immediately restarts it.
- **Halt:** Shuts down the system. You start the system manually with the power switch.

Rebooting and Shutting Down in Gaia Portal

Important:

- If you connected to the Gaia Portal of the applicable Security Group, these actions apply to the entire Security Group.
- If you connected to the Gaia Portal of the applicable Security Group Member, these actions apply only to that Security Group Member.

Shutting down the system and then immediately restarting it

Step	Instructions
1	In the navigation tree, click Maintenance > Shut Down .
2	Click Reboot .

Shutting down the system completely

Step	Instructions
1	In the navigation tree, click Maintenance > Shut Down .
2	Click Halt .

Rebooting and Shutting Down in Gaia Clish

Important:

- If you connected to the Gaia gClish of the applicable Security Group, these commands apply to the entire Security Group.
- If you connected to the Gaia Clish of the applicable Security Group Member, these commands apply only to that Security Group Member.

Shutting down the system and then immediately restarting it

```
reboot
```

Shutting down the system completely

```
halt
```

System Backup

- Back up the configuration of the Gaia operating system and of the Security Management Server database.

You can restore a previously saved configuration.


You can run the backup manually, or on a schedule.

The configuration backup is saved in a *.tgz file in the `/var/log/CPbackup/backups/` directory (on Check Point Appliances and Open Servers).

You can store backups locally, or remotely to a TFTP, SCP or FTP server.

- Save your Gaia system configuration settings as a ready-to-run CLI shell script.

This lets you quickly restore your system configuration after a system failure or migration.

 **Note** - You can only do a migration using the same Gaia version on the source and target computers.

 **Important:**

- When you create a backup on a Security Management Server, make sure to close all SmartConsole clients. Otherwise, backup does not start.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Backup operations (in the Global Gaia Portal or Global Gaia Clish).

To collect or import a Gaia Backup in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

Backing Up and Restoring the System

In This Section:

Excluding Files from the Gaia Backup	597
Backing Up and Restoring the System in Gaia Portal	600
Backing Up the System in Gaia Clish	603
Restoring the System in Gaia Clish	605

Important:

- You can restore a backup file on Gaia OS with the same software version, Jumbo Hotfix Accumulator, and hotfixes as installed on the source Gaia OS, on which you collected this backup file.
- If you restored a backup on a Security Gateway / Cluster Member, install the Security Policy.
- To back up the Quantum Maestro Orchestrator configuration, follow the instructions in [sk174202](#).
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Backup operations (in the Global Gaia Portal or Global Gaia Clish).

To collect or import a Gaia Backup in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

Note - Gaia Operating System uses this template for the name of a manual backup output file regardless of the Gaia Display Format for Time and Date:

```
backup_--_<HostName>.<Domain>_<DD>_<MMM>_<YYYY>_<HH>_<MM>_<SS>.tgz
```

Example for 20 Nov 2022, 18:04:43:

```
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.

File	Software Blade / Feature	Security Gateway	Management Server, Log Server
/var/CPbackup/schemes/cvpn.cpbak	Mobile Access		
/var/CPbackup/schemes/dlp_gw.cpbak	Data Loss Prevention		
/var/CPbackup/schemes/dtps.cpbak	Desktop Policy Server for SecureClients		
/var/CPbackup/schemes/fg1.cpbak	QoS		
/var/CPbackup/schemes/fw1.cpbak	Firewall		
/var/CPbackup/schemes/fw1logs.cpbak	Firewall Logs		
/var/CPbackup/schemes/ioc.cpbak	External IoC Feeds		
/var/CPbackup/schemes/mgmts.cpbak	Network Management		
/var/CPbackup/schemes/ppak.cpbak	SecureXL		
/CPbackup/schemes/rt.cpbak	SmartReporter		
/var/CPbackup/schemes/rtm.cpbak	Monitoring		
/var/CPbackup/schemes/scalable_platform.cpbak	Scalable Platforms (Maestro and Chassis)		
/var/CPbackup/schemes/snapshot.cpbak	Snapshot Utility		
/var/CPbackup/schemes/svn.cpbak	Common Infrastructure (\$CPDIR)		

File	Software Blade / Feature	Security Gateway	Management Server, Log Server
/var/CPbackup/schemes/system_configuration.cpbak	Gaia OS		
/var/CPbackup/schemes/te.cpbak	Threat Emulation		
/var/CPbackup/schemes/uepm.cpbak	Endpoint Policy Management		
/var/CPbackup/schemes/vsx.cpbak	VSX		
/var/CPbackup/schemes/vsx_mgmt.cpbak	VSX Policy		

Procedure

Step	Instructions
1	Connect to the Command Line on the Gaia Server.
2	Log in to the Expert mode.
3	Back up the current configuration file: <pre>cp -v /var/CPbackup/schemes/<Name-of-File>.cpbak{, _BKP}</pre>
4	Edit the current configuration file: <pre>vi /var/CPbackup/schemes/<Name-of-File>.cpbak</pre>
5	Make the required changes in the applicable section: <ul style="list-style-type: none"> ▪ 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

Creating a backup

Step	Instructions
1	In the navigation tree, click Maintenance > System Backup . Refer to the Local Backup section.
2	Click Backup .
3	Select the location of the backup file: <ul style="list-style-type: none"> ▪ This appliance To store the collected backup locally ▪ Management To send the collected backup to the Management Server that manages this Security Gateway. ▪ SCP server To send the collected backup to an SCP server. Enter the IPv4 address, User name, Password and Upload path. ▪ FTP server To send the collected backup to an FTP server. Enter the IPv4 address, User name, Password and Upload path. ▪ TFTP server To send the collected backup to a TFTP server Enter the IPv4 address.

Important:

- Gaia Portal does not support the change of backup file names. You can change a backup file name in the Expert mode. Make sure **not** to use special characters.
- Gaia OS backup on Quantum Maestro Orchestrators does not contain the Maestro configuration files (for example, *sgdb.json*).
To back up the Quantum Maestro Orchestrator configuration, use this Gaia Clish command on the Quantum Maestro Orchestrator:

```
set maestro export <options>
```

For a use case, see [sk174202](#).

Restoring from a locally saved backup

Step	Instructions
1	In the navigation tree, click Maintenance > System Backup . Refer to the Local Backup section.
2	Select the backup file.
3	Click Restore .

Restoring from a remotely saved backup

Step	Instructions
1	In the navigation tree, click Maintenance > System Backup . Refer to the Local 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: <ul style="list-style-type: none"> ▪ Management To restore the backup from the Management Server that manages this Security Gateway ▪ SCP server To restore the backup from an SCP server. Enter the IPv4 address, User name, Password and Upload path. ▪ FTP server To restore the backup from an FTP server. Enter the IPv4 address, User name, Password and Upload path. ▪ TFTP server To restore the backup from a TFTP server. Enter the IPv4 address.
5	Click Restore .

Exporting an existing backup

Step	Instructions
1	In the navigation tree, click Maintenance > System Backup . Refer to the Local 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.

Importing a backup

Step	Instructions
1	In the navigation tree, click Maintenance > System Backup . Refer to the Local Backup section.
2	Select the backup file.
3	Click Import .
4	Click Browse and select the backup file on your computer.
5	Click Import .

Deleting a backup

Step	Instructions
1	In the navigation tree, click Maintenance > System Backup . Refer to the Local Backup section.
2	Select the backup file.
3	Click Delete .
4	Click OK to confirm.

Backing Up the System in Gaia Clish

Syntax

Collecting a backup and storing it locally

```
add backup local [interactive]
```

Collecting a backup and uploading it to an SCP server

```
add backup scp ip <IPv4 Address of SCP Server> path <Path on SCP Server> username <User Name on SCP Server> [password <Password in Plain Text>] [interactive]
```

Collecting a backup and uploading it to an FTP server

```
add backup ftp ip <IPv4 Address of FTP Server> path <Path on FTP Server> username <User Name on FTP Server> [password <Password in Plain Text>] [interactive]
```

Collecting a backup and uploading it to a TFTP server

```
add backup tftp ip <IPv4 Address of TFTP Server> [interactive]
```

Viewing the status of the latest backup

```
show backup {last-successful | logs | status}
```

Viewing the list of local backups and their location

```
show backups
```



Important - After you add, configure, or delete features, run the "save config" command to save the settings permanently.



Important:

- Gaia Clish does not support the change of backup file names. You can change a backup file name in the Expert mode. Make sure **not** to use special characters.

Example

```
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

Restoring a backup from a local hard disk

```
set backup restore local<SPACE><TAB>
```

Restoring a backup from an SCP Server

```
set backup restore scp ip <IPv4 Address of SCP Server> path  
<Path on SCP Server> file <Name of Backup File> username <User  
Name on SCP Server> [password <Password in Plain Text>]  
[interactive]
```

Restoring a backup from an FTP Server

```
set backup restore ftp ip <IPv4 Address of FTP Server> path  
<Path on FTP Server> file <Name of Backup File> username <User  
Name on FTP Server> [password <Password in Plain Text>]  
[interactive]
```

Restoring a backup from a TFTP Server

```
set backup restore tftp ip <IPv4 Address of TFTP Server> file  
<Name of Backup File> [interactive]
```



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 622](#)).

Configuring Scheduled Backups

In This Section:

Configuring Scheduled Backups in Gaia Portal	606
Configuring Scheduled Backups in Gaia Clish	609
Troubleshooting	621

Important:

- When you create a backup on a Management Server, make sure to close all SmartConsole clients. Otherwise, scheduled backup does not start.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Backup operations (in the Global Gaia Portal or Global Gaia Clish).
To collect or import a Gaia Backup in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.
- See "[Backing Up and Restoring the System](#)" on page 597.


Note - Gaia Operating System uses this template for the name of a manual backup output file regardless of the Gaia Display Format for Time and Date:

```
backup_-<Name_of_Scheduled_Backup>-_<HostName>.<Domain>_
<DD>_<MMM>_<YYYY>_<HH>_<MM>_<SS>.tgz
```




Example for 20 Nov 2022, 18:04:43:


```
backup_-MyDailyBkp-_MyGW.MyDomain.com_20_Nov_2022_18_04_
43.tgz
```

Configuring Scheduled Backups in Gaia Portal

-  **Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

Adding a scheduled backup

Step	Instructions
1	In the navigation tree, click Maintenance > System Backup . Refer to the Scheduled Backup section.
2	Click Add Scheduled Backup .
3	<p>In the Backup Name field, enter the name of the job.</p> <ul style="list-style-type: none"> ▪ The maximal length is 15 characters. ▪ The name can consist only of letters, numbers, or underscore "_".
4	<p>In the Backup Type section, configure the location of the backup file:</p> <ul style="list-style-type: none"> ▪ This appliance To keep the collected backup locally in the <code>/var/log/CPbackup/backups/</code> directory. ▪ Management To send the collected backup to the Management Server that manages this Security Gateway (or Cluster Member). Enter the User name and Password for the applicable SCP user. The Security Gateway (or Cluster Member) uploads the file to the <code>/home/<username>/</code> directory on the Management Server.  Important - Follow sk164234 to configure the Security Gateway (or Cluster Member) as a trusted host on the Management Server. ▪ SCP server To send the collected backup to an SCP server. Enter the IP address, User name, Password, and Upload path.  Important: <ul style="list-style-type: none"> • First, you must follow sk164234 to configure the SCP server as a trusted host on Gaia. • The username must have permissions to delete files on the SCP server. ▪ FTP server To send the collected backup to an FTP server. Enter the IP address, User name, Password, and Upload path.  Important -The username must have permissions to delete files on the FTP server. ▪ 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 , Minute Interval , Hourly) for this backup.

Step	Instructions
6	<p>Optional: In the Retention Policy section, configure the backup retention policy:</p> <ul style="list-style-type: none"> ▪ In the Maximum backups to keep field, configure the maximum number of backup files to save. If the new backup files exceeds this number, then Gaia deletes the oldest backup file. ▪ In the Maximum disk space to be used (in MB) field, configure the amount of free disk space to maintain at all times. If the new backup files exceeds this number, then Gaia does not create the new backup file. <p> Important:</p> <ul style="list-style-type: none"> ▪ These settings apply only to the new backup files (and do not apply to existing backup files). ▪ If the job creates a new backup file, it deletes the oldest existing backup file. ▪ The scheduled backup job stops, if Gaia cannot meet the configured retention policy. For example, the disk space limit is not enough to create a new backup file, and the minimum number of backup files does not allow to delete the existing backup files. In this case, Gaia does not show a notification. An administrator must manually check why Gaia did not create the new backup file. ▪ These settings do not support a job that uploads a backup file to a TFTP server because TFTP servers cannot delete files. ▪ These settings apply only to scheduled backup files configured and created in R81.20 version.
7	<p>Click Add. The scheduled backup appears in the Scheduled Backups table.</p>

Deleting a scheduled backup

Step	Instructions
1	In the navigation tree, click Maintenance > System Backup . Refer to the Scheduled Backup section.
2	Select the backup to delete.
3	Click Delete .

Configuring Scheduled Backups in Gaia Clish

Important - On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

Syntax

```

add backup-scheduled name <Name of Schedule>
    ftp path <Path on FTP Server> ip <IPv4 Address of FTP
Server> username <User Name on FTP Server> {password <Password
in Plain Text> | internal <Password>}
    local
    management username <SCP User Name on Management Server>
password <Password in Plain Text>
    scp path <Path on SCP Server> ip <IPv4 Address of SCP
Server> username <User Name on SCP Server> {password <Password
in Plain Text> | internal <Password>}
    tftp ip <IPv4 Address of TFTP Server>

set backup-scheduled name <Name of Schedule> recurrence
    daily time <HH:MM>
    hourly hours {<Hours> | all} at <0-59>
    interval minutes <1-59>
    monthly month {<Months> | all} days <Days> time <HH:MM>
    weekly days {<Days> | all} time <HH:MM>

set backup-scheduled name <Name of Schedule> retention-policy
    keep-occupied-disk-space-in-MB {<Disk Space> | 0}
    max-backups-to-keep {<Number> | 0}
    min-backups-to-keep {<Number> | 0}

show backup-scheduled <Name of Schedule>

delete backup-scheduled <Name of Schedule>

```

Procedure

1. Add a backup schedule

R81.20 supports only *one* of these scheduled backup tasks.

You can configure only one task for one location.

Adding a backup schedule that keeps the backup file locally

```
add backup-scheduled name <Name of Schedule> local
```

Adding a backup schedule that uploads the backup file to the Management Server

```
add backup-scheduled name <Name of Schedule> management
username <SCP User Name on Management Server> password
<Password in Plain Text>
```

- i Important** - Follow [sk164234](#) to configure the Security Gateway (or Cluster Member) as a trusted host on the Management Server.

Adding a backup schedule that uploads the backup file to an FTP server

```
add backup-scheduled name <Name of Schedule> ftp ip <IPv4
Address of FTP Server> path <Path on FTP Server> username
<User Name on FTP Server> password <Password on FTP Server
in Plain Text>
```

Adding a backup schedule that uploads the backup file to an SCP server

```
add backup-scheduled name <Name of Schedule> scp ip <IPv4
Address of SCP Server> path <Path on SCP Server> username
<User Name on SCP Server> password <Password on SCP Server
in Plain Text>
```

- i Important:**
- First, you must follow [sk164234](#) to configure the SCP server as a trusted host on Gaia.
 - The username must have permissions to delete files on the SCP server.

Adding a backup schedule that uploads the backup file to a TFTP server

```
add backup-scheduled name <Name of Schedule> tftp ip <IPv4
Address of TFTP Server>
```

2. Configure the backup schedule recurrence**Running one time on each day at specified time**

```
set backup-scheduled name <Name of Schedule> recurrence
daily time <HH:MM>
```

Running several times each day at specified times

```
set backup-scheduled name <Name of Schedule> recurrence
hourly hours {<Hours> | all} at <0-59>
```

Running several times each day at specified intervals

```
set backup-scheduled name <Name of Schedule> recurrence
interval minutes <1-59>
```

Running in specified months on specified days and at specified time

```
set backup-scheduled name <Name of Schedule> recurrence
monthly month {<Months> | all} days <Days> time <HH:MM>
```

Running each week on specified days of week and at specified time

```
set backup-scheduled name <Name of Schedule> recurrence
weekly days {<Days> | all} time <HH:MM>
```

3. Configure the backup retention policy**a. Configure the amount of free disk space to maintain:**

```
set backup-scheduled name <Name of Schedule> retention-
policy keep-occupied-disk-space-in-MB {<Disk Space> | 0}
```

b. Configure the maximum number of backup files to save:

```
set backup-scheduled name <Name of Schedule> retention-
policy max-backups-to-keep {<Number> | 0}
```

c. Configure the maximum number of backup files to save:

```
set backup-scheduled name <Name of Schedule> retention-
policy min-backups-to-keep {<Number> | 0}
```

4. Examine the scheduled backup configuration

```
show backup-scheduled<SPACE><TAB>
```

```
show backup-scheduled <Name of Schedule>
```

Deleting a scheduled backup

```
delete backup-scheduled<SPACE><TAB>
```

```
delete backup-scheduled <Name of Schedule>
```



Important - After you add, configure, or delete features, run the "save config" command to save the settings permanently.

Parameters

Parameter	Description
<code>name <Name of Schedule></code>	<p>Defines the name of the scheduled backup:</p> <ul style="list-style-type: none"> ▪ The maximal length is 15 characters. ▪ The name can consist only of letters, numbers, or underscore "_".
<code>local</code>	<p>Keeps the backup file locally on this Security Gateway (or Cluster Member). Gaia keeps the file in the <code>/var/log/CPbackup/backups/</code> directory.</p>
<code>management username <SCP User Name on Management Server></code> <code>password <Password in Plain Text></code>	<p>Uploads the backup file over SCP to the Management Server that manages this Security Gateway. The Security Gateway (or Cluster Member) uploads the file to the <code>/home/<username>/</code> directory on the Management Server.</p> <p>i Important - Follow sk164234 to configure the Security Gateway (or Cluster Member) as a trusted host on the Management Server.</p>
<code>ftp ip <IPv4 Address of FTP Server></code>	<p>Specifies the IPv4 address of the remote FTP server.</p>
<code>scp ip <IPv4 Address of SCP Server></code>	<p>Specifies the IPv4 address of the remote SCP server.</p> <p>i Important - First, you must follow sk164234 to configure the SCP server as a trusted host on Gaia.</p>
<code>tftp ip <IPv4 Address of TFTP Server></code>	<p>Specifies the IPv4 address of the remote TFTP server.</p>
<code>path <Path on FTP Server></code>	<p>Specifies the path on the remote FTP server where to upload the backup file.</p>
<code>path <Path on SCP Server></code>	<p>Specifies the path on the remote SCP server where to upload the backup file.</p>

Parameter	Description
<pre>username <User Name on FTP Server></pre>	<p>Specifies the user name required to log in to the remote FTP server.</p> <p>i Important - The username must have permissions to delete files on the FTP server.</p>
<pre>username <User Name on SCP Server></pre>	<p>Specifies the user name required to log in to the remote SCP server.</p> <p>i Important - The username must have permissions to delete files on the SCP server.</p>
<pre>password <Password in Plain Text></pre>	<p>Specifies the password (in plain text) required to log in to the remote server.</p>
<pre>recurrence daily time <HH:MM></pre>	<p>Specifies that the job must run once a day - each day, at specified time.</p> <p>Enter the time of day in the 24-hour clock format - <Hours>:<Minutes>.</p> <p>Example:</p> <pre>HostName> set backup- scheduled name MyBackup recurrence daily time 14:35</pre> <pre>HostName> show backup- scheduled MyBackup The scheduled backup is performed locally. Every day at 14:35</pre>


Parameter	Description
<pre>recurrence hourly hours {<Hours> all} at <Minutes 0-59></pre>	<p>Specifies that the job must run many times during the day - at the specified time.</p> <ul style="list-style-type: none"> ■ You can specify a single hour of a day by a number from 0 to 23. ■ You can specify several hours of a day. Enter the hours separated by commas. Example - for hours 14, 15, and 16, enter: 14,15,16 ■ To specify each hour of a day, enter: all ■ You must specify the minutes of each configured hour by a number from 0 to 59. <p>Example:</p> <pre>HostName> set backup- scheduled name MyBackup recurrence hourly hours 14,15,16 at 35</pre> <pre>HostName> show backup- scheduled MyBackup The scheduled backup is performed locally. Every day at 14:35,15:35,16:35</pre>

Parameter	Description
<code>recurrence interval minutes <1-59></code>	<p>Specifies that the job must run many times during the day - at intervals of the specified number of minutes.</p> <p>Example:</p> <pre>HostName> set backup- scheduled name MyBackup recurrence interval minutes 30</pre> <pre>HostName> show backup- scheduled MyBackup The scheduled backup is performed locally. Every 30 minutes.</pre>

Parameter	Description
<pre>recurrence monthly month {<Months> all} days <Days> time <HH:MM></pre>	<p>Specifies that the job must run once a month - on the specified months, on the specified dates, and at the specified time.</p> <ul style="list-style-type: none"> ■ Specify the months by numbers from 1 to 12: January = 1, February = 2, ..., December = 12. ■ To specify several months, enter their numbers separated by commas. Example - for January, February, and March, enter: 1,2,3 ■ To specify each month of the year, enter: <code>all</code> ■ Specify the dates of a month by numbers from 1 to 31. ■ To specify several dates, enter their numbers separated by commas. Example - for 1st, 2nd and 3rd day of month, enter: 1,2,3 <p>Example:</p> <pre>HostName> set backup- scheduled name MyBackup recurrence monthly month 1,2,3 days 1,2,3 time 14:35</pre> <pre>HostName> show backup- scheduled MyBackup The scheduled backup is performed locally. Each January, February, March on days 1, 2, 3 at 14:35</pre>

Parameter	Description
<pre>recurrence weekly days {<Days> all} time <HH:MM></pre>	<p>Specifies that the job must run once a week - on specified days of week, and at specified time.</p> <ul style="list-style-type: none"> ■ Specify the days of a week by numbers from 0 to 6: Sunday = 0, Monday = 1, Tuesday = 2, Wednesday = 3, Thursday = 4, Friday = 5, Saturday = 6. ■ To specify several days of a week, enter their numbers separated by commas. Example- for Sunday, Monday, and Tuesday, enter: 0,1,2 ■ To specify each day of the week, enter: all <p>Example:</p> <pre>HostName> set backup- scheduled name MyBackup recurrence weekly days 1,3 time 14:35</pre> <pre>HostName> show backup- scheduled MyBackup The scheduled backup is performed locally. Every week on Monday, Wednesday at 14:35</pre>

Parameter	Description
<pre>retention-policy <Options></pre>	<p>Specifies how much disk space the backup files can take and how many backup files to keep on Gaia:</p> <ul style="list-style-type: none"> <p>■ <code>retention-policy keep-occupied-disk-space-in-MB {<Disk Space> 0}</code> Specifies how many much disk space (in megabytes) the existing backup files can take on Gaia.</p> <p>■ <code>retention-policy max-backups-to-keep {<Number> 0}</code> Specifies how many backup files to keep on Gaia at maximum. If the job creates a new backup file, it deletes the oldest existing backup file. The value for maximum number of backup files to keep must be greater than the value for minimum number of backup files.</p> <p>■ <code>retention-policy min-backups-to-keep {<Number> 0}</code> Specifies how many backup files to keep on Gaia at minimum.</p>

Parameter	Description
	<p data-bbox="847 241 1007 280"> Notes:</p> <ul style="list-style-type: none"> <li data-bbox="951 309 1406 376">■ Each of these retention policy settings is optional. <li data-bbox="951 389 1434 501">■ These settings apply only to the new backup files (and do not apply to existing backup files). <li data-bbox="951 515 1437 627">■ To change the current configuration, run the command again with a new value. <li data-bbox="951 640 1449 752">■ To disable this configuration, run the command again with the value 0 (zero). <li data-bbox="951 766 1434 878">■ If the job creates a new backup file, it deletes the oldest existing backup file. <li data-bbox="951 891 1449 1025">■ If the job uploads a backup file to a remote server, the username must have permissions to delete files on the remote server. <li data-bbox="951 1039 1453 1599">■ The scheduled backup job stops, if Gaia cannot meet the configured retention policy. For example, the disk space limit is not enough to create a new backup file, and the minimum number of backup files does not allow to delete the existing backup files. In this case, Gaia does not show a notification. An administrator must manually check why Gaia did not create the new backup file. <li data-bbox="951 1612 1458 1747">■ These settings do not support a job that uploads a backup file to a TFTP server because TFTP servers cannot delete files. <li data-bbox="951 1760 1458 1917">■ These settings apply only to scheduled backup files configured and created in R81.20 version.

Examples

- **Creating a daily backup file as a local LVM volume:**

```
gaia> add backup-scheduled name Daily local
gaia>
gaia> set backup-scheduled name Daily recurrence daily time
22:00
gaia>
gaia> set backup-scheduled name Daily retention-policy keep-
occupied-disk-space-in-MB 50000
gaia>
gaia> set backup-scheduled name Daily retention-policy max-
backups-to-keep 10
gaia>
gaia> set backup-scheduled name Daily retention-policy min-
backups-to-keep 3
gaia>
gaia> show backup-scheduled Daily
The scheduled backup is performed locally.
Retention-policy:
    max-backups-to-keep 10
    min-backups-to-keep 3
    keep-occupied-disk-space-in-MB 50000
Every day at 22:00
gaia>
gaia> save config
```

- **Creating a monthly snapshot image as a file and uploading it to an SCP server:**

```
gaia> add backup-scheduled name Monthly ftp ip 192.168.20.30
path /var/log/my_backups/ username backup_user password
123456
gaia>
gaia> set backup-scheduled name Monthly recurrence monthly
month all days 1 time 22:00
gaia>
gaia> show backup-scheduled Monthly
The scheduled backup is performed to an ftp server.
  IP: 192.168.20.30
  Username: backup_user
Every month on day 1 at 22:00
gaia>
gaia> save config
```

Troubleshooting


Examine the location of the backup file.

Examine the `/var/log/messages` files.

Working with System Configuration in Gaia Clish

You can save your Gaia configuration settings as a ready-to-run CLI shell script.

This feature lets you quickly restore your system configuration after a system failure or migration.

 **Note** - You can only do a migration using the same Gaia version on the source and target computers.

 **Important:**

- In a Management Data Plane Separation (MDPS) environment (see [sk138672](#)), you must run these commands in each plane.
- On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.
- Maestro Security Groups that contain different Security Appliance models do **not** support Gaia Backup operations (in the Global Gaia Portal or Global Gaia Clish).

To collect or import a Gaia Backup in such a Security Group, connect directly to Gaia Portal or Gaia Clish on each Security Appliance in the Security Group.

Syntax

Saving the system configuration to a CLI script

```
save configuration <Name of Script>
```

Restoring the configuration settings

```
load configuration <Name of Script>
```

Viewing the latest configuration settings

```
show configuration
```

Example

This example shows part of the configuration settings as last saved to a CLI shell script:

```
mygaia> show configuration
#
# Configuration of mygaia
# Language version: 10.0v1
#
# Exported by admin on Mon Mar 19 15:06:22 2012
#
set hostname mygaia
set timezone Asia / Jerusalem
set password-controls min-password-length 6
set password-controls complexity 2
set password-controls palindrome-check true
set password-controls history-checking true
set password-controls history-length 10
set password-controls password-expiration never
set ntp active off
set router-id 6.6.6.103
set ipv6-state off
set snmp agent off
set snmp agent-version any
set snmp community public read-only
set snmp traps trap authorizationError disable
set snmp traps trap coldStart disable
set snmp traps trap configurationChange disable
... .. [truncated for brevity]... ..
mygaia>
```

LVM Overview

Description

The Gaia Clish command "show system lvm overview" shows information about system logical volumes.

Syntax

```
show system lvm overview
```

Example

```
gaia> show system lvm overview
LVM overview
=====
          Size(GB)  Used(GB)  Configurable  Description
lv_current      38         8         yes          Check Point OS and products
lv_log          56         2         yes          Logs volume
upgrade reserved 42        N/A        no           Reserved space for version
upgrade
swap            16        N/A        no           Swap memory volume
unallocated space 148      N/A        no           Unused space
-----
total          300      N/A        no           Total size

gaia>
```

Related information

See ["Configuring Log Volume" on page 388](#).

Advanced Gaia Configuration

In This Section:

Configuring the Gaia Portal Web Server	625
Resetting the Expert Mode Password on a Security Gateway	627
Configuring Supported SSH Ciphers, MACs, and KexAlgorithms	627

Important:

- On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.
- On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in Gaia gClish of the applicable Security Group.

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. <ul style="list-style-type: none"> ▪ Range: on, or off ▪ Default: on
session- timeout <Timeout>	Configures the time (in minutes), after which the HTTPS session to the Gaia Portal terminates. <ul style="list-style-type: none"> ▪ Range: 1 - 720 ▪ Default: 15
ssl-port <Port>	Configures the TCP port number, on which the Gaia Portal can be accessed over HTTPS. <ul style="list-style-type: none"> ▪ Range: 1 - 65535 ▪ Default: 443 <p>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.</p> <p> 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 <code>https://<Hostname or IP Address>/to</code> to <code>https://<Hostname or IP Address>:<PORTNUMBER></code></p>
ssl3- enabled {on off}	Enables or disables the HTTPS SSLv3 connection to Gaia Portal. <ul style="list-style-type: none"> ▪ 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. <ul style="list-style-type: none"> ▪ Range: 10 - 240 ▪ Default: 10

Resetting the Expert Mode Password on a Security Gateway

Follow [sk106490](#) if you forget your Expert mode password for a Security Gateway, Cluster Member, or Scalable Platform Security Group.

Configuring Supported SSH Ciphers, MACs, and KexAlgorithms

Description

You can configure different settings for the SSH daemon on the Gaia Operating System.

You can configure these SSH settings in Gaia Clish.

Description

Setting	Description
SSH Ciphers	SSH uses ciphers for privacy of data it sends over an SSH connection.
SSH Message Authentication Codes	SSH uses Message Authentication Codes to maintain the integrity of each message it sends over and SSH connection. This provides integrity between SSH peers.
SSH Key Exchange Algorithms	SSH uses Key Exchange Algorithms to exchange a shared session key securely with an SSH peer.
SSH Client Alive Interval	In SSHv2, this is a timeout interval (in seconds), after which if no data is received from an SSH client, the <i>sshd</i> daemon sends a message through the encrypted channel to request a response from the client. This controls the "ClientAliveInterval" parameter for the <i>sshd</i> daemon. By default, this feature is disabled (the default value is 0). See https://linux.die.net/man/5/sshd_config .
SSH Password Authentication	Specifies whether password authentication is allowed. This controls the "PasswordAuthentication" parameter for the <i>sshd</i> daemon. By default, this feature is enabled (the default value is "yes"). See https://linux.die.net/man/5/sshd_config .

Setting	Description
SSH Permit Root Login	<p>Specifies whether the root user can log in over SSH. This controls the "PermitRootLogin" parameter for the <i>sshd</i> daemon.</p> <p>By default, this feature is enabled (the default value is "yes"). See https://linux.die.net/man/5/sshd_config.</p>
SSH DNS Usage	<p>Specifies whether the <i>sshd</i> daemon needs to look up the remote hostname and make sure the resolved hostname for the remote IP address maps back to the same IP address. This controls the "UseDNS" parameter for the <i>sshd</i> daemon.</p> <p>By default, this feature is disabled (the default value is "no"). See https://linux.die.net/man/5/sshd_config.</p>

Complete Syntax

```
set ssh server
  cipher <Cipher>{on | off}
  client-alive-interval 0-65535
  kex <Key Exchange Algorithm> {on | off}
  mac <Message Authentication Code> {on | off}
  password-authentication {yes | no}
  permit-root-login {yes | no | without-password | prohibit-
password | forced-commands-only}
  use-dns {yes | no}
```

```
show ssh server
  cipher enabled
  cipher supported
  client-alive-interval
  kex enabled
  kex supported
  mac enabled
  mac supported
  password-authentication
  permit-root-login
  use-dns
```

Syntax for SSH Ciphers

- To view the supported SSH Ciphers:

```
show ssh server cipher supported
```

These are the supported SSH Ciphers:

- 3des-cbc
- aes128-cbc
- aes128-ctr
- aes128-gcm@openssh.com
- aes192-cbc
- aes192-ctr
- aes256-cbc
- aes256-ctr
- aes256-gcm@openssh.com
- chacha20-poly1305@openssh.com
- rijndael-cbc@lysator.liu.se

- To view the enabled SSH Ciphers:


```
show ssh server cipher enabled
```

These are the SSH Ciphers that are enabled by default:

- aes128-ctr
- aes128-gcm@openssh.com
- aes192-ctr
- aes256-ctr
- aes256-gcm@openssh.com
- chacha20-poly1305@openssh.com

- To enable or disable the supported SSH Ciphers:

```
set ssh server cipher <Cipher> {on | off}
```

 **Important** - After you add, configure, or delete features, run the "save config" command to save the settings permanently.

Syntax for SSH Key Exchange Algorithms

- To view the supported SSH Key Exchange Algorithms:

```
show ssh server kex supported
```

These are the supported SSH Key Exchange Algorithms:

- curve25519-sha256
- curve25519-sha256@libssh.org
- diffie-hellman-group1-sha1
- diffie-hellman-group14-sha1
- diffie-hellman-group14-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group-exchange-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

- To view the enabled SSH Key Exchange Algorithms:

```
show ssh server kex enabled
```

These are the SSH Key Exchange Algorithms that are enabled by default:

- curve25519-sha256
- curve25519-sha256@libssh.org
- diffie-hellman-group14-sha1
- diffie-hellman-group14-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512
- diffie-hellman-group-exchange-sha256
- ecdh-sha2-nistp256

- `ecdh-sha2-nistp384`
- `ecdh-sha2-nistp521`

- To enable or disable the supported SSH Key Exchange Algorithms:

```
set ssh server kex <Key Exchange Algorithm> {on | off}
```

i **Important** - After you add, configure, or delete features, run the "save config" command to save the settings permanently.

Syntax for SSH Message Authentication Codes (MACs)

- To view the supported SSH Message Authentication Codes:

```
show ssh server mac supported
```

These are the supported SSH Message Authentication Codes:

- `hmac-md5-96-etm@openssh.com`
- `hmac-md5-etm@openssh.com`
- `hmac-sha1`
- `hmac-sha1-96-etm@openssh.com`
- `hmac-sha1-etm@openssh.com`
- `hmac-sha2-256`
- `hmac-sha2-256-etm@openssh.com`
- `hmac-sha2-512`
- `hmac-sha2-512-etm@openssh.com`
- `umac-64-etm@openssh.com`
- `umac-64@openssh.com`
- `umac-128-etm@openssh.com`
- `umac-128@openssh.com`

- To view the enabled SSH Message Authentication Codes:

```
show ssh server mac enabled
```

These are the SSH Message Authentication Codes that are enabled by default:

- hmac-sha1
- hmac-sha1-etm@openssh.com
- hmac-sha2-256
- hmac-sha2-256-etm@openssh.com
- hmac-sha2-512
- hmac-sha2-512-etm@openssh.com
- umac-64-etm@openssh.com
- umac-64@openssh.com
- umac-128-etm@openssh.com
- umac-128@openssh.com

- To enable or disable the supported SSH Message Authentication Codes:

```
set ssh server mac <Message Authentication Code> {on | off}
```

i **Important** - After you add, configure, or delete features, run the "save config" command to save the settings permanently.

Syntax for SSH Client Alive Interval

- To view the current interval:

```
show ssh server client-alive-interval
```

- To configure the required interval (in seconds):

```
set ssh server client-alive-interval 0-65535
```

i **Important** - After you add, configure, or delete features, run the "save config" command to save the settings permanently.

Syntax for SSH Password Authentication

- To view the current permission:

```
show ssh server password-authentication
```

- To configure the required permission:

```
set ssh server password-authentication {yes | no}
```

i **Important** - After you add, configure, or delete features, run the "save config" command to save the settings permanently.


Syntax for SSH Permit Root Login

- To view the current permission:

```
show ssh server permit-root-login
```

- To configure the required permission:

```
set ssh server permit-root-login {yes | no | without-  
password | prohibit-password | forced-commands-only}
```

 **Important** - After you add, configure, or delete features, run the "save config" command to save the settings permanently.


Syntax for SSH DNS Usage

- To view the current permission:

```
show ssh server use-dns
```

- To configure the required permission:

```
set ssh server use-dns {yes | no}
```

 **Important** - After you add, configure, or delete features, run the "save config" command to save the settings permanently.

Monitoring Transceivers

Background

To connect fiber optic cables to Check Point Appliances, you use Small Form-Factor Pluggable (SFP) and Quad Small Form-factor Pluggable (QSFP) transceivers.

The Gaia Clish commands described below provide real-time data about the transceivers installed in the Appliance

Viewing Information About an Interface Transceiver

Syntax

```
show interface <Name of Interface> xcvr
```

Example Output

```
gaia> show interface eth1-01 xcvr

  Port  Check Point  Temp  Voltage  Laser Bias  Transmit  Rec
LOS    Transmitter
      Certified  (°C)   (V)     Current    Power     Power
      Fault
      Transceiver
      (mA)     (dBm)    (dBm)
-----  ---  -----  -----  -----  -----  -----
--  -----
eth1-01  Yes    26.53  3.35    39.19    -1.30    -0.02
Off      Off

gaia>
```

Viewing Detailed Information About an Interface Transceiver

Syntax

```
show interface <Name of Interface> xcvr_detail
```

Example Output

```

gaia> show interface eth1-01 xcvr_detail

eth1-01 SFP is present
Product Type: 10G Base-LR
Vendor name: FINISAR CORP.
Vendor PN: FTLX1471D3BCV-CK
Vendor rev: A
Vendor SN: AWN0L3T
Check Point part number: CPAC-TR-10LR
Check Point Material ID: 309856
Laser wavelength: 1310nm
Link Length for SMF,km: 10km
Link Length for SMF: 10000m
Link Length for 50um: 0m
Link Length for 62.5um: 0m
Link Length for Copper: 0m
Link Length for OM3: 0m
No tx fault, No rx loss

QSFP Diagnostic Information
-----
-----
                                     Alarms
Warnings                               High           Low           High
      Low
-----
-----
Temperature      26.80 C                78.00 C        -13.00 C       73.00 C
                 -8.00 C
Voltage          3.35 V                3.70 V         2.90 V         3.60 V
                 3.00 V
Current          39.21 mA                85.00 mA       7.00 mA        80.00
mA              12.00 mA
Tx Power         -1.29 dBm                2.00 dBm       -8.00 dBm      1.00
dBm             -7.00 dBm
Rx Power         -0.02 dBm                2.50 dBm       -20.00 dBm     2.00
dBm            -18.01 dBm

gaia>

```

Viewing Information About Transceivers for All Interfaces

Syntax

```
show interfaces xcvr
```

Example Output

```
gaia> show interfaces xcvr

  Port  Check Point  Temp  Voltage  Laser Bias  Transmit  Rec
LOS    Transmitter
      Certified  (°C)   (V)     Current    Power     Power
      Fault
      Transceiver          (mA)    (dBm)    (dBm)
  ----  ---  -----  -----  -----  -----  -----  -
  --  -----
eth1    transceiver information not available
eth1-01  Yes    26.94  3.35    39.30     -1.30     -0.06
Off     Off
eth1-02  Yes    30.36  3.35     8.79     -2.53     -2.86
Off     Off
eth1-03  Yes    27.96  3.35    35.08     -1.43     -0.53
Off     Off
eth1-04  transceiver information not available
eth2    transceiver information not available
eth2-01  Yes    27.46  3.35     7.51     -2.18     -2.78
Off     Off
eth2-02  transceiver information not available
eth2-03  transceiver information not available
eth2-04  transceiver information not available
eth3    transceiver information not available
eth4    transceiver information not available
eth5    transceiver information not available
eth6    transceiver information not available
eth7    transceiver information not available
eth8    transceiver information not available

gaia>
```

Viewing Detailed Information About Transceivers for All Interfaces

Syntax

```
show interfaces xcvr_detail
```

Example Output

```
gaia> show interfaces xcvr_detail
eth1 no information available
```

```
eth1-01 SFP is present
Product Type: 10G Base-LR
Vendor name: PROLABS
Vendor PN: ER-SFP-10G-I-CPA
Vendor rev: A1__
Vendor SN: CPT111BF7903
Check Point part number: CPAC-TR-10ER-C
Check Point Material ID: 328822
Laser wavelength: 1550nm
Link Length for SMF,km: 40km
Link Length for SMF: 25500m
Link Length for 50um: 0m
Link Length for 62.5um: 0m
Link Length for Copper: 0m
Link Length for OM3: 0m
No tx fault, Yes rx loss
```

QSFP Diagnostic Information

```
-----
-----
                                     Alarms
Warnings
                                     High      Low      High
      Low
-----
-----
Temperature      33.32 C          88.00 C      -43.00 C      85.00 C
                  -40.00 C
Voltage          3.33 V          3.60 V       3.00 V       3.50 V
                  3.10 V
Current          67.08 mA          120.00 mA     10.00 mA     110.00
mA              20.00 mA
Tx Power         1.08 dBm          5.00 dBm     -3.00 dBm     4.00
dBm             -2.00 dBm
Rx Power         1.88 dBm          1.50 dBm     -20.00 dBm     0.50
dBm            -18.01 dBm
```



```

eth1-02 SFP is present
Product Type: 10G Base-SR
Vendor name: FINISAR CORP.
Vendor PN: FTLX8574D3BCV-CP
Vendor rev: A
Vendor SN: UWC2M1S
Check Point part number: CPAC-TR-10SR-B
Check Point Material ID: 317353
Laser wavelength: 850nm
Link Length for SMF,km: 0km
Link Length for SMF: 0m
Link Length for 50um: 80m
Link Length for 62.5um: 30m
Link Length for Copper: 0m
Link Length for OM3: 300m
No tx fault, No rx loss

```

QSFP Diagnostic Information

```

-----
-----

```

		Alarms		
Warnings		High	Low	High
Low				

Temperature	30.46 C	78.00 C	-13.00 C	73.00 C
	-8.00 C			
Voltage	3.33 V	3.70 V	2.90 V	3.60 V
	3.00 V			
Current	8.56 mA	13.20 mA	2.00 mA	12.60
	3.00 mA			
Tx Power	-2.67 dBm	0.00 dBm	-8.00 dBm	-1.00
	-7.00 dBm			
Rx Power	-2.98 dBm	0.00 dBm	-20.00 dBm	-1.00
	-18.01 dBm			

```

eth1-03 SFP is present
Product Type: 10G Base-LR
Vendor name: FINISAR CORP.

```

```

or PN: FTLX8574D3BCV-CP
Vendor rev: A
Vendor SN: A0SC750
Check Point part number: CPAC-TR-10SR-B
Check Point Material ID: 317353
Laser wavelength: 850nm
Link Length for SMF,km: 0km
Link Length for SMF: 0m
Link Length for 50um: 80m
Link Length for 62.5um: 30m
Link Length for Copper: 0m
Link Length for OM3: 300m
No tx fault, No rx loss

```

QSFP Diagnostic Information

```

-----
-----
                                     Alarms
Warnings                               High           Low           High
      Low
-----
-----
Temperature      27.19 C                78.00 C       -13.00 C      73.00 C
                 -8.00 C
Voltage          3.34 V                3.70 V        2.90 V        3.60 V
                 3.00 V
Current          8.64 mA                13.20 mA       2.00 mA       12.60
mA              3.00 mA
Tx Power         -2.31 dBm                0.00 dBm       -8.00 dBm     -1.00
dBm             -7.00 dBm
Rx Power         -2.60 dBm                0.00 dBm      -20.00 dBm    -1.00
dBm            -18.01 dBm

```


```

eth2-02 no information available
eth2-03 no information available
eth2-04 no information available
eth3 no information available
eth4 no information available
eth5 no information available
eth6 no information available
eth7 no information available
eth8 no information available

```

```
gaia>
```

CPUSE - Software Updates

 **Important** - It is **not** supported to manually upgrade the CPUSE Agent on Scalable Platforms (Known Limitation MBS-2372).

With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself. The software update packages and full images are for major releases, minor releases and Hotfixes. All of the CPUSE processes are handled by the Deployment Agent daemon (DA).

Gaia automatically locates and shows the available software update packages and full images that are applicable to the Gaia operating system version installed on the computer, the computer's role (Security Gateway, Security Management Server, Standalone), and other specific properties. The images and packages can be downloaded from the [Check Point Support Center](#) and installed.

You can add a private package to the list of available packages. A private package is a Hotfix, which is located on the Check Point Support Center, and is only available to limited audiences.

When you update Check Point software, make sure to:

- Define the CPUSE policy for downloads and installation.

Downloads can be:

- Manual
- Automatic
- Scheduled (daily, weekly, monthly, or one time only).

Installations are:

- Hotfixes are downloaded and installed automatically by default
- Full installation and upgrade packages must be installed manually
- Define mail notifications for completed package actions and for the new package updates.
- Run the software download and installation.

 **Note** - You must have a CPUSE policy defined, before you download and run upgrades.

For details, see [sk92449](#).

Gaia API Proxy

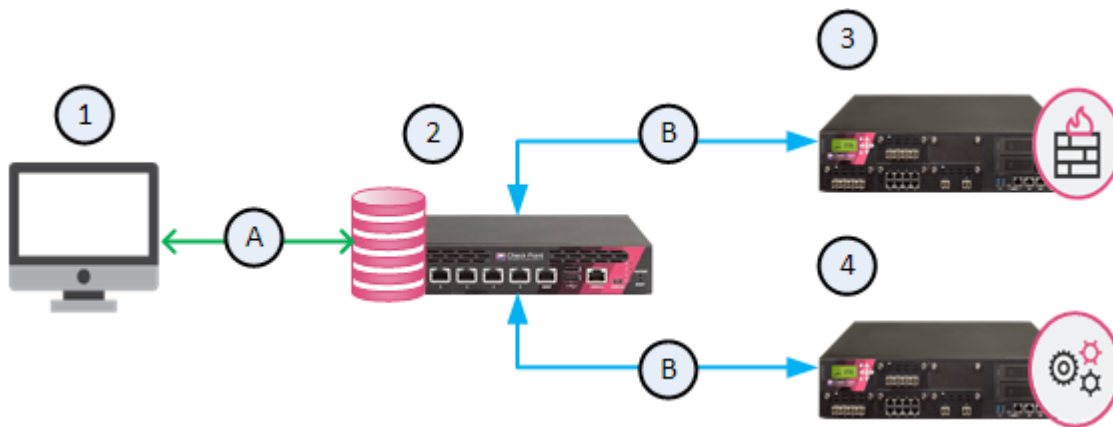
Check Point products support API commands. See the [Check Point API Reference](#).

With the Gaia API Proxy feature on a Management Server, you run the Gaia API commands on managed Security Gateways and Cluster Members:

1. An administrator connects with an API Client to a Management Server.
2. From the Management Server, an administrator runs the Gaia API commands on managed Security Gateways and Cluster Members.

The Gaia API Proxy feature on the R81.20 Management Server works with all managed Security Gateways and Cluster Members that support the Gaia API.

Example diagram



Item	Description
1	An API Client
2	A Management Server with the Gaia API Proxy feature
3	A managed Security Gateway
4	A managed ClusterXL
A	Management API communication
B	Gaia API communication

- i Important** - Scalable Platforms (Maestro and Chassis) do **not** support this feature (Known Limitation MBS-10832).

Workflow:

1. Run the Management API "login" command to log in to the Management Server

When you work with an API Client, run the Check Point API "login" command to log in to the Management Server (see the [Check Point Management API Reference](#)).

- i Important** - The administrator that logs in must have the **Run One Time Script** permission enabled in the assigned permission profile:
 - a. Connect with SmartConsole to the Management Server.
 - b. From the left navigation panel, click **Manage & Settings**.
 - c. In the top section, click **Permissions & Administrators > Permission Profiles**.
 - d. Open the applicable permission profile.
 - e. From the left tree, click **Overview**.
 - If you selected **Read/Write All**, then click **Cancel**.
The required permission is already enabled.
 - If you selected **Customized**, then:
 - i. From the left tree, click **Gateways**.
 - ii. In the **Scripts** section, select **Run One Time Script**.
 - iii. Click **OK**.
 - iv. Publish the SmartConsole session

2. Run the Gaia API commands on managed Security Gateways and Cluster Members

The Management API "login" command returns the Session Unique Identifier (SID) token.

In the same API Client, use this SID token in the "x-chkp-sid" field of the Gaia API commands you run on managed Security Gateways and Cluster Members.

Gaia API Syntax:

```
POST https://<IP Address of Management Server>/web_api/gaia-api/<Gaia API Version>/<Gaia API Command>
```

See the [Check Point Gaia API Reference](#).

The body of the Gaia API command must identify the managed Security Gateway or Cluster Member by one of these parameters:

- Object name
- Object primary IP address
- Object UID

3. The Gaia API Proxy logs in to the specified Security Gateway or Cluster Member

The Gaia API Proxy on the Management Server interprets the Gaia API command and logs in to the specified Security Gateway or Cluster Member.

- a. This login returns the SID for the Security Gateway or Cluster Member.
- b. The Gaia API Proxy uses this SID to run the Gaia API commands.
- c. The Gaia API Proxy saves this SID in its database:
 - The SID timeout is 580 seconds on the Management Server.
 - The SID timeout is 10 minutes on a Security Gateway or Cluster Member.

4. The Gaia API Proxy forwards the response from the Security Gateway or Cluster Member to the API client

- To increase performance, the Gaia API Proxy saves the response in the Gaia API Proxy cache on the Management Server.
- If the Gaia API Proxy gets the same Gaia API request during the cache timeout, it returns the Gaia API response from its cache and updates the cache.

- An administrator can configure these cache parameters in the `$FWDIR/api/conf/cache.conf` file on the Management Server:

Note - After you change the `$FWDIR/api/conf/cache.conf` file, you must reload the API server configuration with the `api reconf` command in the Expert mode.

Parameter	Accepted Values	Description
<code>timeout</code>	0, or greater	Specifies the time, after which the next Gaia API command triggers a cache update for that Gaia API command: <ul style="list-style-type: none"> • 0 - The Gaia API proxy does not use cache • <code><integer></code> - The Gaia API proxy saves the Gaia API responses in its cache for the specified number of seconds (default: 60 seconds)
<code>total_gateways</code>	integer	Specifies the number of unique Security Gateways and Cluster Members, from which to save the Gaia API responses.
<code>maximum_entries</code>	integer	Specifies the number of unique Gaia API commands to save for each Security Gateway and Cluster Member.

Important - The Gaia API Proxy sends Gaia API command over HTTPS. The Access Control policy for the Security Gateway or ClusterXL must explicitly allow HTTPS traffic from the Management Server to the Security Gateway or Cluster Members.

Examples

Gaia API command "show-hostname"

In this example, we identify the managed Security Gateway by the object primary IP address.

Request

```
POST https://<IP Address of Management Server>/gaia-api/show-  
hostname  
Content-Type: application/json  
X-chkp-sid: <Session ID>  
{  
  "target" : "192.168.1.1"  
}
```

Response

```
{  
  "command-name" : "show-hostname",  
  "response-message" : {  
    "name" : "gw-832546"  
  }  
}
```


Gaia API command "show-interface"

In this example, we identify the managed Security Gateway by the object name.

Request

```
POST https://<IP Address of Management Server>/gaia-  
api/v1.4/show-interfaces  
Content-Type: application/json  
X-chkp-sid: <Session ID>  
{  
  "target" : "gw-832546",  
  "name" : "eth0"  
}
```

Response

```
{  
  "command-name" : "v1.4/show-interfaces",  
  "response-message" : {  
    "ipv6-local-link-address": "Not Configured",  
    "type": "physical",  
    "name": "eth0",  
    "ipv6-mask-length": "Not-Configured",  
    "ipv6-address": "Not-Configured",  
    "ipv6-autoconfig": "Not configured",  
    "ipv4-address": "192.168.1.1",  
    "enabled": true,  
    "comments": "",  
    "ipv4-mask-length": "24"  
  }  
}
```

Gaia API command "show-diagnostics"

In this example, we identify the managed Security Gateway by the object UID.

Request

```
POST https://<IP Address of Management Server>/gaia-
api/v1.4/show-diagnostics
Content-Type: application/json
X-chkp-sid: <Session ID>
{
  "target" : "52048978-c507-8243-9d84-074d11154616",
  "category" : "os",
  "topic" : "disk"
}
```

Response

```
{
  "command-name" : "v1.4/show-diagnostics",
  "response-message" : {
    "to": 3,
    "total": 3,
    "from": 1,
    "objects": [
      {
        "total": "34342961152",
        "partition": "/",
        "used": "5718065152",
        "free": "28624896000"
      },
      {
        "total": "304624640",
        "partition": "/boot",
        "used": "26991616",
        "free": "277633024"
      },
      {
        "total": "34342961152",
        "partition": "/var/log",
        "used": "455684096",
        "free": "33887277056"
      }
    ]
  }
}
```

Running Check Point Commands in Shell Scripts

To run Check Point commands in your shell scripts, it is necessary to add the calls to the required Check Point shell scripts.

You must add these calls below the top line `#!/bin/bash`.

On a Security Management Server / Log Server / SmartEvent Server

You must add the call to the `/etc/profile.d/CP.sh` script.

```
#!/bin/bash

source /etc/profile.d/CP.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

On a Multi-Domain Server / Multi-Domain Log Server

You must add the calls to these scripts (in the order listed below):

1. `/etc/profile.d/CP.sh`
2. `$MDSDIR/scripts/MDSprofile.sh`
3. `$MDS_SYSTEM/shared/mds_environment_utils.sh`
4. `$MDS_SYSTEM/shared/sh_utilities.sh`

```
#!/bin/bash

source /etc/profile.d/CP.sh
source $MDSDIR/scripts/MDSprofile.sh
source $MDS_SYSTEM/shared/mds_environment_utils.sh
source $MDS_SYSTEM/shared/sh_utilities.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

On a Security Gateway / Cluster Members (non-VSX)

You must add the call to the `/etc/profile.d/CP.sh` script.

```
#!/bin/bash

source /etc/profile.d/CP.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

On a VSX Gateway / VSX Cluster Members

You must add the calls to these scripts (in the order listed below):

1. `/etc/profile.d/CP.sh`
2. `/etc/profile.d/vsenv.sh`

```
#!/bin/bash

source /etc/profile.d/CP.sh
source /etc/profile.d/vsenv.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

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*').