



Check Point
SOFTWARE TECHNOLOGIES LTD.

30 August 2017

GAIA

R80.10

Administration Guide

Classification: [Protected]



Check Point
SOFTWARE TECHNOLOGIES LTD.

INFINITY

Important Information



Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

For third party independent certification of Check Point Products, see the Check Point Certification page

<https://www.checkpoint.com/products-solutions/certified-check-point-solutions/>



Check Point R80.10

For more about this release, see the R80.10 home page

<http://supportcontent.checkpoint.com/solutions?id=sk111841>.



Latest Version of this Document

Download the latest version of this document

http://supportcontent.checkpoint.com/documentation_download?ID=54824.

To learn more, visit the Check Point Support Center

<http://supportcenter.checkpoint.com>.



Feedback

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

Please help us by sending your comments

mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Gaia R80.10 Administration Guide.



Searching in Multiple PDFs

To search for text in all the R80.10 PDF documents, download and extract the complete R80.10 documentation package

<http://downloads.checkpoint.com/dc/download.htm?ID=54846>.

Use **Shift-Control-F** in Adobe Reader or Foxit reader.

Revision History

Date	Description
30 August 2017	Updated To import a package from your local drive to the list of available package ("Configuring CPUSE - WebUI" on page 206) Updated License Activation (on page 186) Updated Snapshot Image Management (on page 187) Link to Check Point third party certifications added to this Important Information page.
14 June 2017	Updated Centrally Managing Gaia Device Settings (on page 35). General updates

Date	Description
15 May 2017	First release of this document

© 2017 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 <http://www.checkpoint.com/copyright.html> for a list of our trademarks.

Refer to the Third Party copyright notices http://www.checkpoint.com/3rd_party_copyright.html for a list of relevant copyrights and third-party licenses.

Contents

Important Information.....	2
Gaia Overview.....	10
Introduction to the WebUI	11
WebUI Overview	11
Logging in to the WebUI	12
Working with the Configuration Lock.....	12
Using the Interface Elements.....	13
Toolbar Accessories	13
Search Tool	13
Navigation Tree	13
Status Bar.....	13
Configuration Tab	14
Monitoring Tab	14
System Information Overview	15
Showing System Overview Information - WebUI	15
Showing System Overview Information - CLI	16
Changing System Edition	17
Introduction to the Command Line Interface	18
Saving Configuration Changes	18
Commands and Features	18
Command Completion.....	20
Command History	21
Command Reuse	21
Command Line Movement and Editing.....	22
Obtaining a Configuration Lock.....	22
32 and 64-bit Gaia Editions.....	23
Environment Commands.....	24
Client Environment Output Format.....	25
Expert Mode	26
User Defined (Extended) Commands	27
Configuring Gaia for the First Time	29
Running the First Time Configuration Wizard in WebUI.....	29
Running the First Time Configuration Wizard in CLI.....	29
config_system	30
Centrally Managing Gaia Device Settings.....	35
Overview of the Gateways & Servers View	35
Managing Gaia Devices in SmartConsole.....	35
Running Command Scripts	35
Understanding One-Time Scripts	36
Running Repository Scripts	36
Backup and Restore	36
Opening Gaia WebUI and Gaia command line.....	38
Network Management.....	39
Network Interfaces	39
Interface Link Status	39
Physical Interfaces	40

Aliases.....	42
VLAN Interfaces.....	43
Bond Interfaces (Link Aggregation).....	46
Bridge Interfaces.....	51
Loopback Interfaces.....	53
VPN Tunnel Interfaces.....	54
CLI Reference (interface)	60
ARP	62
Configuring ARP- WebUI	62
Configuring ARP - CLI (arp)	63
DHCP Server	64
Configuring a DHCP Server- WebUI.....	65
Configuring a DHCP Server - CLI (dhcp)	66
Hosts and DNS	68
Host Name.....	68
Host Addresses	69
Domain Name Service (DNS)	70
IPv4 Static Routes	72
Configuring IPv4 Static Routes - WebUI.....	73
Configuring Static Routes - CLI (static-route).....	74
IPv6 Static Routes	77
Configuring IPv6 Static Routes - WebUI.....	77
Configuring IPv6 Static Routes - CLI (set ipv6 static-route)	78
Netflow Export	80
Flow Records.....	81
Configuring Netflow Export - WebUI.....	81
Configuring Netflow Export - CLI (netflow).....	82
Monitoring NetFlow Configuration	82
Performance Optimization	83
Configuring Performance Optimization - WebUI.....	84
Configuring Performance Optimization - CLI (cpconfig)	85
System Management.....	86
Time	86
Setting the Time and Date - WebUI.....	87
Configuring NTP - CLI (ntp)	87
Showing the Time & Date - CLI (clock).....	88
Setting the Date - CLI (date)	89
Setting the Time - CLI (Time).....	89
Setting the Time Zone - CLI (timezone).....	89
Cloning Groups.....	90
Configuring Cloning Groups - WebUI	91
Configuring Cloning Groups - CLI (Cloning Groups).....	93
SNMP	99
Configuring SNMP - WebUI.....	102
Configuring SNMP - CLI (snmp).....	105
Interpreting Error Messages.....	109
Job Scheduler	111
Configuring Job Scheduler - WebUI.....	112
Configuring Job Scheduler - CLI (cron)	112
Mail Notification	114
Configuring Mail Notification - WebUI	114
Configuring Mail Notification - CLI (mail-notification)	114

Messages	115
Configuring Messages - WebUI.....	115
Configuring Messages - CLI (message)	115
Session.....	117
Configuring the Session - WebUI.....	117
Configuring the Session - CLI (inactivity-timeout)	117
Core Dumps	117
Configuring Core Dumps - WebUI.....	117
Configuring Core Dumps -CLI (core-dump)	118
System Configuration.....	119
Configuring IPv6 Support - WebUI.....	119
Configuring IPv6 Support - CLI	119
System Logging.....	120
Configuring System Logging - WebUI	120
Configuring System Logging - CLI (syslog)	120
Configuring Log Volume - CLI (volume)	121
Redirecting Routed System Logging Messages.....	122
Network Access	123
Configuring Telnet Access - WebUI	123
Configuring Telnet Access - CLI (net-access)	123
Configuring the WebUI Web server	123
Host Access.....	125
Configuring Allowed Gaia Clients - WebUI.....	125
Configuring Allowed Gaia Clients - CLI (allowed-client)	126
Advanced Routing.....	127
User Management.....	128
Change My Password	128
Change My Password - WebUI.....	128
Change My Password - CLI (selfpasswd)	128
Users.....	129
Managing User Accounts - WebUI.....	129
Managing User Accounts - CLI (user)	131
Roles	133
Configuring Roles - WebUI	134
Configuring Roles - CLI (rba).....	135
Password Policy	137
Configuring Password Policy- WebUI	138
Configuring Password Policy- CLI (password-controls)	141
Monitoring Password Policy	145
Authentication Servers	146
Configuring RADIUS Servers - WebUI.....	147
Configuring RADIUS Servers - CLI (aaa)	148
Configuring Gaia as a RADIUS Client	149
Configuring RADIUS Servers for Non-Local Gaia Users	150
Configuring TACACS+ Servers - WebUI	151
Configuring TACACS+ Servers - CLI (aaa).....	152
Configuring Gaia as a TACACS+ Client.....	154
Configuring TACACS+ Servers for Non-Local Gaia Users	155
System Groups	156
Configuring System Groups - WebUI	156
Configuring System Groups - CLI (group)	157
GUI Clients	157

Security Management GUI Clients - WebUI.....	158
GUI Clients - CLI (cpconfig).....	158
High Availability	159
VRRP	159
Understanding VRRP	159
Preparing a VRRP Cluster	164
Configuring Monitored Circuit/Simplified VRRP	166
Configuring Monitored Circuit/Simplified VRRP - CLI (mcvr).....	166
Configuring Monitored Circuit/Simplified VRRP - WebUI.....	168
Configuring the VRRP Security Gateway Cluster in SmartConsole	170
Configuring VRRP Rules for the Security Gateway.....	170
Configuring Advanced VRRP	171
Configuring Advanced VRRP - WebUI	171
Configuring Advanced VRRP - CLI (vrrp).....	173
Configuring VRRP Clusters in SmartConsole.....	175
Troubleshooting VRRP	175
General Configuration Considerations	175
Firewall Policies.....	176
Monitored-Circuit VRRP in Switched Environments	176
Maintenance.....	177
Licenses	177
Configuring Licenses - WebUI	177
Configuring Licenses - CLI (cplic).....	178
License Activation	186
Snapshot Image Management.....	187
Snapshot Prerequisites	188
Working with Snapshot Management - WebUI.....	189
Working with Snapshot Management - CLI (snapshot)	190
Download SmartConsole.....	191
Download SmartConsole - WebUI.....	191
Hardware Health Monitoring	191
Showing Hardware Health Monitoring Information - WebUI.....	191
Showing Hardware Monitoring Information - CLI (sysenv)	192
Showing Hardware Information - CLI (show asset).....	192
Monitoring RAID Synchronization	194
Showing RAID Information - WebUI.....	194
Showing RAID Information - CLI	194
Shutdown	194
Shutting Down - WebUI.....	194
Shutting Down - CLI (halt, reboot)	195
System Configuration Backup.....	195
Backing Up and Restoring the System - WebUI	195
Backing Up and Restoring the System - CLI (Backup).....	196
Configuring Scheduled Backups - WebUI	197
Configuring Scheduled Backups - CLI (backup-scheduled)	198
Working with System Configuration - CLI (configuration).....	200
Emergendisk.....	201
Creating the Emergendisk Removable Device	201
Bootting from the Emergendisk Removable Device.....	202
Resetting the Administrator Password.....	202
Irrecoverably Erasing Data using DBAN	203
CPUSE	204

Configuring a CPUSE Policy - WebUI	204
Configuring CPUSE Mail Notifications - WebUI.....	205
Configuring CPUSE - WebUI.....	206
Reviewing CPUSE – clish.....	207
CLI Procedures - CPUSE	209

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

Gaia CPUSE

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

Introduction to the WebUI

In This Section:

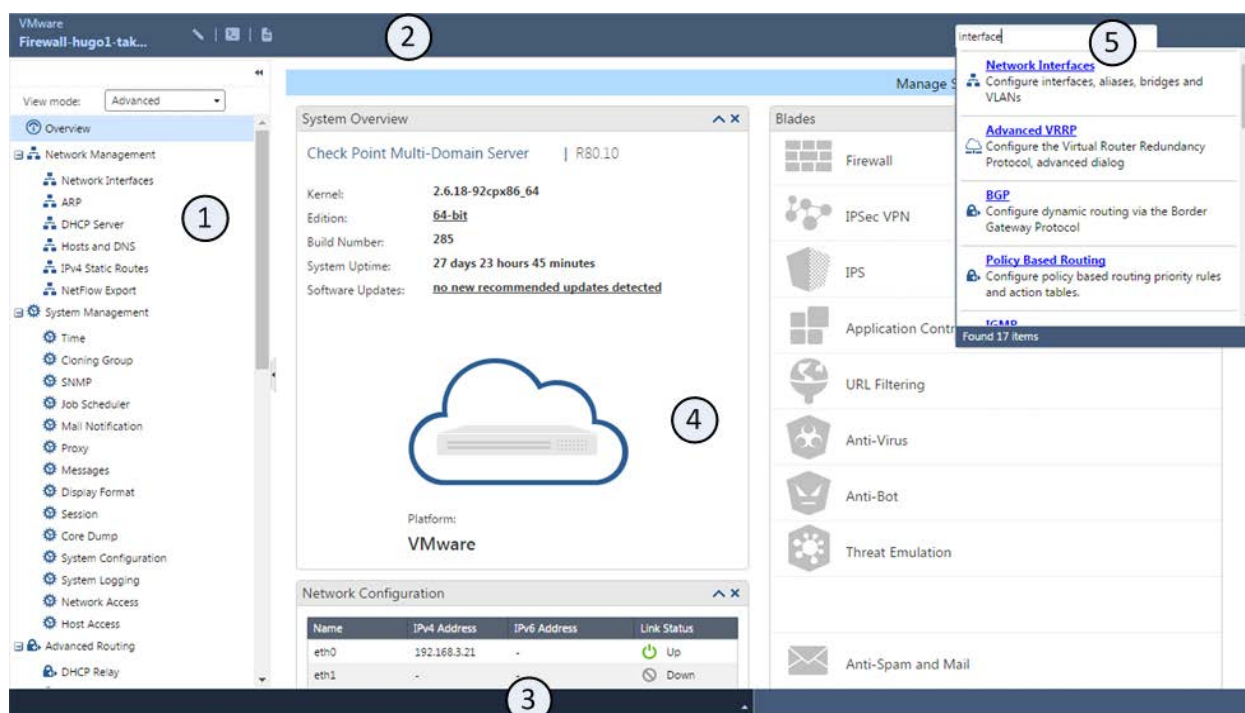
WebUI Overview	11
Logging in to the WebUI	12
Using the Interface Elements	13

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

WebUI Overview

- The Gaia WebUI 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 go to <https://<Device IP Address>>.
- Browser Support - Internet Explorer, Firefox, Chrome and Safari.
- Powerful Search Engine - Makes it easy to find features or functionality to configure.
- Easy Operation - Two operating modes. 1) Simplified mode which shows only basic configuration options. 2) Advanced mode which shows all configuration options. You can easily change modes.
- Web-Based Access to Command Line - Clientless access to the Gaia CLI directly from your browser.

The WebUI 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 WebUI

Logging in

To log in to the WebUI:

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

Logging out

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

Working with the Configuration Lock

Only one user can have Read/Write access to Gaia configuration settings at a time. All other users can log in with Read-Only access to see configuration settings, as specified by their assigned roles (on page 133).

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

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

To override a configuration lock in the WebUI:

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

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

Using the Interface Elements

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

Toolbar Accessories

You can use these toolbar icons to do these tasks:

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

Search Tool

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

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

Navigation Tree

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

- **Basic** - Shows some standard pages
- **Advanced** (Default) - Shows all pages

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

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

Status Bar

The status bar, located at the bottom of the window, shows the result of the last configuration operation. To see a history of the configuration operations during the current session, click the **Expand**  icon.

Configuration Tab

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

Monitoring Tab

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

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

System Information Overview

In This Section:

Showing System Overview Information - WebUI	15
Showing System Overview Information - CLI	16
Changing System Edition	17

This chapter shows you how to see system information using the WebUI and some CLI commands.

Showing System Overview Information - WebUI

The **Overview** page shows status widgets.

The screenshot shows the Check Point Security Gateway WebUI Overview page. The page is divided into two main sections: System Overview and Network Configuration.

System Overview

Check Point Security Gateway | R80.10

Kernel: 2.6.18-92cp86_64
Edition: 64-bit
Build Number: 6
System Uptime: 27 days 2 hours 39 minutes
Software Updates: no new recommended updates detected

Platform: VMware

Network Configuration

Name	IPv4 Address	IPv6 Address	Link Status
eth0	192.168.3.24	-	Up
eth1	-	-	Down
lo	127.0.0.1	-	Up

Blades

- Firewall
- IPSec VPN
- IPS
- Application Control
- URL Filtering
- Anti-Virus
- Anti-Bot
- Threat Emulation
- Threat Extraction
- Anti-Spam and Mail
- Data Loss Prevention

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

Widget	Description
System Overview	System information, including: • Installed product • Product version number • Kernel build • Product build • Edition (32 bit or 64 bit) • Platform on which Gaia is installed • Computer serial number (if applicable)
Blades	Installed Software Blades. Those that are enabled in SmartConsole are colored. Those that are not enabled are grayed out.
Network Configuration	Interfaces, their status and IP addresses
Memory Monitor	Graphical display of memory usage
CPU Monitor	Graphical display of CPU usage

To add a widget to the page: Scroll down to the bottom of the page, click **Add Widget** and select a widget to show.

To move a widget: Click its title bar and drag it to the desired location.

Showing System Overview Information - CLI

You can use these commands to show system status.

uptime

Description Show how long the system has been running

Syntax `show uptime`

Parameters None

version

Description Show the name and versions of the 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
<code>all</code>	Shows all system information.
<code>os build</code>	The Gaia build number.
<code>os edition</code>	The Gaia edition (32-bit or 64-bit).
<code>os kernel</code>	The Gaia kernel build number.
<code>product</code>	The Gaia version.

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

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

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

1. Run `set edition default 64-bit`
2. Run `save config`
3. Reboot



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

To see which edition is running:

- Go to the WebUI **System Overview** pane. The edition shows in the **System Overview** widget.
- OR: Run `show version os edition`

Changing System Edition

Gaia automatically starts in the 32 bit edition after an upgrade and for open servers that have less than the minimum RAM as described in the Release Notes.

You can change the system to 32-bit or 64-bit using the `set edition` command.

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

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

```
set edition 64-bit
save config
reboot
```



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

Introduction to the Command Line Interface

In This Section:

Saving Configuration Changes	18
Commands and Features	18
Command Completion	20
Command History	20
Command Line Movement and Editing	22
Obtaining a Configuration Lock	22
32 and 64-bit Gaia Editions	23
Environment Commands	24
Expert Mode	26
User Defined (Extended) Commands	27

This chapter gives an introduction to the Gaia command line interface (CLI). The default shell of the CLI is called `clish`.

To use the CLI:

1. Connect to the platform using one of these options:
 - From SmartConsole ("Opening Gaia WebUI and Gaia command line" on page 38).
 - Using a command-line connection (SSH or a console) over a TCP/IP network.
2. Log in using a user name and password.
Immediately after installation, the default user name and password are `admin` and `admin`.

Saving Configuration Changes

When you change the OS configuration with the CLI, changes are applied immediately to the running system only. To have the changes survive a reboot, you must run: `save config`

Commands and Features

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

operation feature parameter

The most common operations are `add`, `set`, `show`, `delete`

Main operations	Description
add	Adds a new value to the system.
set	Sets a value in the system.

Main operations	Description
<code>show</code>	Shows a value or values from the system.
<code>delete</code>	Deletes a value from the system.

Other operations	Description
<code>save</code>	Saves the configuration changes made since the last save operation.
<code>reboot</code>	Restart the system.
<code>halt</code>	Turns the computer off.
<code>quit</code>	Exits from the CLI.
<code>exit</code>	Exits from the shell.
<code>Start</code>	Starts a transaction. Puts the CLI into transaction mode. All changes made using commands in transaction mode are applied at once or none of the changes are applied based on the way transaction mode is terminated.
<code>commit</code>	Ends transaction by committing changes.
<code>rollback</code>	Ends transaction by discarding changes.
<code>expert</code>	Enter the expert shell. Allows low-level access to the system, including the file system.
<code>ver</code>	Shows the version of the active Gaia image.
<code>revert</code>	Revert the database.
<code>help</code>	Get help on navigating the CLI and some useful commands.

To see the commands you have permissions to run: `show commands`

To see a list of all features: `show commands feature <TAB>`

To see all commands for a specific feature: `show commands feature <featureName>`

To see all commands for an operation of a feature: `show commands [op <name>] [feature <name>]`

To see all operations: `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 the CLI prompt, press Q.

Command Completion

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

Press ...	To do this...
<TAB>	Complete or fetch the keyword. For example: <pre>Gaia> set in<TAB> inactivity-timeout - Set inactivity timeout interface - Displays the interface related parameters Gaia> set in</pre>
<SPACE> <TAB>	Show the arguments that the command for that feature accepts. For example: <pre>Gaia> set interface <SPACE> <TAB> eth0 eth1 lo Gaia> set interface</pre>
<ESC><ESC>	See possible command completions. For example: <pre>Gaia> 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 } Gaia> set inter</pre>
?	Get help on a feature or keyword. For example: <pre>Gaia> set interface <?> interface: {show/add/delete} interface "interface-name" Gaia> set interface</pre>
UP/DOWN arrow	Browse the command history.
LEFT/RIGHT arrow	Edit command.
Enter	Run a command string. The cursor does not have to be at the end of the line. You can usually abbreviate the command to the smallest number of unambiguous characters.

Command History

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

Command	Description
↓	Recall previous command.
↑	Recall next command.
history	Show the last 100 commands.
!!	Run the last command.
!nn	Run a specific previous command: The nn command.
!-nn	Run the nnth previous command. For example, entering !-3 runs the third from last command.
!str	Run the most recent command that starts with str.
!\?str\?	Run the most recent command containing str. The trailing ? may be omitted if str is followed immediately by a new line.
!!:s/str1/str2	Repeat the last command, replacing str1 with str2.

Command Reuse

You can combine word designators with history commands to refer to specific words used in previous commands. Words are numbered from the beginning of the line with the first word being denoted by 0. 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`, `interfaces` is word 1.

Word Designator	Meaning
0	The operation word.
n	The nth word.
^	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 the following modifiers, each preceded by a colon:

Modifier	Meaning
p	Print the new command but do not execute

Modifier	Meaning
s/str1/str2	Substitute new for the first occurrence of old in the word being referred to.
g	Apply changes over the entire command. Use this modified in conjunction with s, as in gs/str1/str2.

Command Line Movement and Editing

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

These are the keystroke combinations you can use:

Keystroke combination	Meaning
Alt-D	Delete next word.
Alt-F	Go to the next word.
Ctrl-Alt-H	Delete the previous word.
Ctrl-shift_	Repeat the previous word.
Ctrl-A	Move to the beginning of the line.
Ctrl-B	Move to the previous character.
Ctrl-E	Move to the end of the line.
Ctrl-F	Move to the next character.
Ctrl-H	Delete the previous character.
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.

Obtaining a Configuration Lock

Only one user can have Read/Write access to Gaia configuration settings at a time. All other users can log in with Read-Only access to see configuration settings, as specified by their assigned roles (on page 133).

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

to override their lock. If you:

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

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

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

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

Syntax

- `lock database override`
- `unlock database`

Comments Use these commands with caution. The admin whose write access is revoked does not receive notification.

Configuring Configuration Lock Behavior

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

Description Configures and shows the state of the configuration lock

Syntax

```
set config-lock {off | on [timeout <seconds>] override
show {config-lock | config-state}
```

Parameters

Parameter	Description
off on	Turns the configuration lock on and off. When you turn config-lock on, the default timeout value is 300 seconds.
timeout	Enables config-lock for the specified interval in seconds (5-900).

Comments

- `set config-lock on override` is identical to `lock database override`
- `set config-lock off` is identical to `unlock database`

32 and 64-bit Gaia Editions

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

For more on supported platforms and kernels, see the R80.10 Release notes
<http://supportcontent.checkpoint.com/solutions?id=sk111841>.

Note - The open server hardware must support 64-bit for the Edition feature to work.

Description

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

Syntax

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

Comments

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

To see which edition is running:

- Go to the WebUI **System Overview** pane. The edition shows in the **System Overview** widget.
- On the command line, run: `show version os edition`

Environment Commands

Description

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

Syntax

To show the client environment

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

To set the client environment

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

To save the client environment permanently

```
save clienv
```

Parameters

Parameter	Description
<code>config-lock {on off}</code>	Default value of the <code>clish config-lock</code> parameter. If set to <code>on</code> , <code>clish</code> will lock the configuration when invoked, otherwise continue without a configuration lock. When the configuration is locked by <code>clish</code> , no configuration changes are possible in WebUI, until the lock is released.
<code>debug {0-6}</code>	Debug level. Predefined levels are: • 0 - (Default) Do not debug, display error messages only • 5 - Show <code>confd</code> requests and responses • 6 - Show handler invocation parameters and results
<code>echo-cmd {on off}</code>	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. The default is <code>off</code> .
<code>on-failure {continue stop}</code>	Action performed on failure: • <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 {pretty structured xml}</code>	Command line output format (" Client Environment Output Format " on page 25). The default is <code>pretty</code> .
<code>prompt <prompt_string></code>	Command prompt string. A valid prompt string can consist of any printable characters and a combination of these variables: • <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 I. • <code>%U</code> - Replaced with the Username To set the prompt back to the default, use the keyword <code>default</code> .
<code>rows <row_number></code>	Number of rows to show in your terminal window. If the window size is changed, the number of rows will also change, unless the value is set to 0 (zero).
<code>syntax-check {on off}</code>	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

These are the output formats that CLI supports:

- **Pretty**

Output is formatted to be clear. For example, output of the command `show user admin` in

pretty mode would look like this:

Uid	Gid	Home Dir.	Shell	Real Name
0	0	/home/admin	/etc/cli.sh	n/a

- **Structured**

Output is delimited by semi-colons. For example, output of the command `show user admin` in structured mode would look like this:

```
Uid;Gid;Home Dir.;Shell;Real Name;
0;0;/home/admin;/etc/cli.sh;;
```

- **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>/etc/cli.sh</Shell>
<Real_Name></Real_Name>
</Row>
</System_User>
</RESPONSE>
</CMDRESPONSE>
```

Expert Mode

The default shell of the CLI is called `clish`. `clish` is a restrictive shell (role-based administration controls the number of commands available in the shell). While the use of `clish` is encouraged for security reasons, `clish` does not give access to low level system functions. For low level configuration, use the more permissive `expert` shell.

- To use the expert shell, run: `expert`
- To exit the expert shell and return to `clish`, run: `exit`

Note - If a command is supported in `clish`, it is not possible to run it in expert mode.

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

Expert- Password

A password protects the expert shell against unauthorized access. The expert password can be changed using the `expert-password` feature.

Description: Use this command to set the expert password by plain text or MD5 salted hash. Use the MD5 salted hash option when upgrading or restoring using backup scripts.

- Syntax:**
- `set expert-password`
 - `set expert-password hash VALUE`

Parameters

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

Example

```
gw> 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):
gw> save config
```

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

User Defined (Extended) Commands

Description

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

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

You can do role based administration (RBA) with extended commands by assigning extended commands to roles and then assigning the roles to users or user groups.

Syntax

To show all extended commands

```
show extended commands
```

To show the path and description of a specified extended command

```
show command VALUE
```

To add an extended command

```
add command VALUE path VALUE description VALUE
```

To delete an extended command

```
delete command VALUE
```

Parameters

Parameter	Description
command	Name of the extended command
path	Path of the extended command
description	Description of the extended command

Example

To add the `free` command to the `systemDiagnosis` role and assign a user with that role:

1. To add the `free` command, run

```
add command free path /usr/bin/free description "Display amount of free and used memory in the system"
```
2. Save the configuration. Run

```
save config
```
3. Log out of Gaia and log in again.
4. To add the `free` command to the `systemDiagnosis` role, run

```
add rba role systemDiagnosis domain-type System readwrite-features ext_free
```
5. To assign user `john` with the `systemDiagnosis` role, run

```
add rba user john roles systemDiagnosis
```

Configuring Gaia for the First Time

In This Section:

Running the First Time Configuration Wizard in WebUI	29
Running the First Time Configuration Wizard in CLI	29

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

Running the First Time Configuration Wizard in WebUI

To configure Gaia and the Check Point products on it for the first time, using WebUI, refer to the *R80.10 Installation and Upgrade Guide*

<http://downloads.checkpoint.com/dc/download.htm?ID=54829>.

Running the First Time Configuration Wizard in CLI

You can configure Gaia system and the Check Point products on it for the first time using the CLI `config_system` command.



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.

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

1. Run this command in Expert mode: `config_system --config-string <string of parameters and values>`

A configuration string must consist of *parameter=value* pairs, separated by &. The whole string must be enclosed between quotation marks. For example:

```
"hostname=myhost&domainname=somedomain.com&timezone='America/Indiana/Indianapolis'&ftw_sic_key=aaaa&install_security_gw=true&gateway_daip=false&install_ppak=true&gateway_cluster_member=true&install_security_managment=false"
```

For more information on valid parameters and values, see `config_system` (on page 30).

2. Reboot the system.

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

1. Run this command in Expert mode: `config_system -f <file_name>`
2. Reboot the system.

If you do not have a configuration file, you can create a configuration template and fill in the parameter values as necessary. Before you run the First Time Configuration Wizard, you can validate the configuration file you created.

To create a configuration file:

1. Create a template file: `config_system -t <file_name>`
2. Open the file you created in a text editor and edit all parameter values as necessary.
3. Save the updated configuration file.

To validate a configuration file:

Run this command in Expert mode: `config_system --config-file <file_name> --dry-run`

config_system

Run `config_system` command in expert mode.

Description

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

Syntax

To list the command options:

```
config_system --help
```

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

```
config_system -f|--config-file <filepath>
```

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

```
config_system -s|--config-string <string>
```

To create a First Time Wizard Configuration file template in a specified path:

```
config_system -t|--create-template <path>
```

To verify that the First Time Configuration file is valid:

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

To list configurable parameters:

```
config_system -l|--list-params
```

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

Note - The parameters can change from version to version. Run `config_system --help` to see currently available parameters.

Parameters

Parameter	Description	Valid values
<code>install_security_gw</code>	Installs Security Gateway, if set to <code>true</code> .	• <code>true</code> • <code>false</code>

Parameter	Description	Valid values
install_ppak	Installs Performance Pack, if set to true. Must be set to true, if install_security_gw is set to true.	• true • false
gateway_daip	Enables or disables dynamic IP gateway.	• true • false Note - must be set to false if ClusterXL or Security Management Server is enabled.
gateway_cluster_member	Enables or disables ClusterXL.	• true • false
install_security_management	Installs Security Management Server, if set to true.	• true • false
install_mgmt_primary	Makes the installed Security Management Server the primary one. The install_security_management must be set to true.	• true • false Note - can only be set to true, if the install_mgmt_secondary is set to false.
install_mgmt_secondary	Makes the installed Security Management Server a secondary one. The install_security_management must be set to true.	• true • false Note - can only be set to true, if the install_mgmt_primary is set to false.
install_mds_primary	Makes the installed Security Management Server the primary Multi-Domain Server. The install_security_management must be set to true.	• true • false Note - can only be set to true, if the install_mds_secondary is set to false.

Parameter	Description	Valid values
<code>install_mds_secondary</code>	Makes the installed Security Management Server a secondary Multi-Domain Server. The <code>install_security_management</code> must be set to <code>true</code> .	<code>true</code> <code>false</code> Note - can only be set to <code>true</code> , if the <code>install_mds_primary</code> is set to <code>false</code> .
<code>install_mlm</code>	Installs Multi-Domain Log Server, if set to <code>true</code> .	<code>true</code> <code>false</code>
<code>install_mds_interface</code>	Specifies Multi-Domain Server management interface.	Name of the interface exactly as it appears in the device configuration. Examples: <code>eth0</code> , <code>eth1</code>
<code>mgmt_admin_name</code>	Sets management administrator's username. Must be provided if <code>install_security_management</code> is set to <code>true</code> .	A string of alphanumeric characters.
<code>mgmt_admin_passwd</code>	Sets management administrator's password. Must be provided if <code>install_security_management</code> is set to <code>true</code> .	A string of alphanumeric characters.
<code>mgmt_gui_clients_radio</code>	Specifies management WebUI clients that can connect to the Security Management Server.	- IPv4 address of a host <code>any</code> <code>range</code> <code>network</code>
<code>mgmt_gui_clients_first_ip_field</code>	Specifies the first address of the range, if <code>mgmt_gui_clients_radio</code> is set to <code>range</code> .	IPv4 address of a host.
<code>mgmt_gui_clients_last_ip_field</code>	Specifies the last address of the range, if <code>mgmt_gui_clients_radio</code> is set to <code>range</code> .	IPv4 address of a host.

Parameter	Description	Valid values
<code>mgmt_gui_clients_ip_field</code>	Specifies the network address, if <code>mgmt_gui_clients_radio</code> is set to <code>network</code> .	IPv4 address of a network.
<code>mgmt_gui_clients_subnet_field</code>	Specifies the netmask, if <code>mgmt_gui_clients_radio</code> is set to <code>network</code> .	A number from 0 to 32.
<code>ftw_sic_key</code>	Sets a secure Internal Community key, if <code>install_security_management</code> is set to <code>false</code> .	A string of alphanumeric characters.
<code>admin_hash</code>	Sets administrator's password.	A string of alphanumeric characters, enclosed between single quotation marks.
<code>iface</code>	Interface name (optional).	Name of the interface exactly as it appears in the device configuration. Examples: <code>eth0</code> , <code>eth1</code>
<code>ipstat_v4</code>	Turns static IPv4 configuration on, when set to <code>manually</code> .	<code>manually</code> <code>off</code>
<code>ipaddr_v4</code>	Sets IPv4 address of the management interface.	IPv4 address.
<code>masklen_v4</code>	Sets IPv4 mask length for the management interface.	A number from 0 to 32.
<code>default_gw_v4</code>	Specifies IPv4 address of the default gateway.	IPv4 address.
<code>ipstat_v6</code>	Turns static IPv6 configuration on, when set to <code>manually</code> .	<code>manually</code> <code>off</code>
<code>ipaddr_v6</code>	Sets IPv6 address of the management interface.	IPv6 address.
<code>masklen_v6</code>	Sets IPv6 mask length for the management interface.	A number from 0 to 128.
<code>default_gw_v6</code>	Specifies IPv6 address of the default gateway.	IPv6 address.

Parameter	Description	Valid values
hostname	Sets the name of the local host (optional).	A string of alphanumeric characters.
domainname	Sets the domain name (optional).	Fully qualified domain name. Example: <code>somedomain.com</code>
timezone	Sets the area/region (optional).	The value must be enclosed between single quotation marks. Examples: 'America/New_York', 'Asia/Jerusalem'
ntp_primary	Sets the IP address of the primary NTP server (optional).	IPv4 address.
ntp_secondary	Sets the IP address of the secondary NTP server (optional).	IPv4 address.
primary	Sets the IP address of the primary DNS server (optional)	IPv4 address.
secondary	Sets the IP address of the secondary DNS server (optional)	IPv4 address.
tertiary	Sets the IP address of the tertiary DNS server (optional)	IPv4 address.
download_info	Downloads Check Point Software Blade contracts and other important information, if set to <code>true</code> (Best Practice - optional, but highly recommended). For more information, see sk94508 http://supportcontent.checkpoint.com/solutions?id=sk94508 .	• <code>true</code> • <code>false</code>
upload_info	Uploads data that helps Check Point provide you with optimal services, if set to <code>true</code> (Best Practice - optional, but highly recommended). For more information, see sk94509 http://supportcontent.checkpoint.com/solutions?id=sk94509 .	• <code>true</code> • <code>false</code>

Centrally Managing Gaia Device Settings

In This Section:

Overview of the Gateways & Servers View	35
Managing Gaia Devices in SmartConsole	35

Overview of the Gateways & Servers View

The SmartConsole Gateways & Servers view lets you manage and monitor the Check Point Security Gateways. It lets you manage all the gateways from one place and do actions on multiple gateways at the same time. In the **Gateways & Servers** view, you can:

- Create and configure Security Gateways for all supported platforms
- Edit gateways properties
- Run command line scripts on the gateways
- Open the Gaia WebUI and Gaia CLI shell
- Monitor and receive notifications on the gateways status
- Do backup and restore operations
- Examine recent management tasks done on the gateways. The tasks show in the Task tab in the bottom section of SmartConsole.

The Gateways & Servers view has configurable **Display Columns**:

- **General** - General properties of the Security Gateway
- **Health** - The condition of the Security Gateway
- **Traffic** - Details about the Security Gateway throughput and the actions which the Security Gateway enforced on the packets
- **Access Control** - Information on the Access Control policy installed on the Security Gateway
- **Threat Prevention** - Information about the Threat Prevention policy installed on the Security Gateway
- **Management** - Management related information, such as management Software Blades
- **License** - Information about the status of the license installed on the Security Gateway

Managing Gaia Devices in SmartConsole

Running Command Scripts

You can manually enter and run a command line script on the selected Gaia Security Gateways. This feature is useful for scripts that you do not have to run on a regular basis.

To run a one time script:

1. In the **Gateways & Servers** view, right-click the object you want to run scripts on.
2. Select **Scripts > One Time Script**.
3. The **Run One Time Script** window opens.
Note - For a cluster object, select the member you want to run the script on.
4. Enter the command in the **Script Body** text box or load the complete command from a text file.
5. Click **Run**.

Note - You can run a one-time script on multiple gateways or servers at the same time.

Understanding One-Time Scripts

If you specify a script:

- By default, the maximum size of a script is: 8kb.
- 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 a repository.

To run a Repository script:

1. In the Gateways & Servers, right-click the Security Gateways or Security Management Servers you want to run scripts on.
2. Select **Scripts > Scripts Repository**.
The **Scripts Repository** window opens.
3. Do one of these options:
 - Select a 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 gateways or servers at the same time.
- For a cluster object, the script will run automatically on all 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 regularly back up your system. 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 gateway for the first time, you must publish the changes made on the gateway before you do a system backup operation.

To back up the system:

1. Right-click the Security Gateway or Security Gateways you want to back up.
2. Select **Actions > System Backup**.
The **System Backup** window opens.
3. Select the backup location:
 - The **Backup server defined for this gateway** - To define a backup server for this gateway, double-click the gateway, and go to **Network Management > System Backup**
 Or
 - Enter the details of the backup server

Note - The path to the backup directory must start and end with (/)
For example: /ftroot/backup/
or just (/) for the root directory of the server.
The file name must be according to this convention:
backup_<name of gateway object>_<date of backup>.tgz
4. Click **OK**.
The status of the backup operation shows in **Tasks**.
5. When the task is complete, double-click the entry to see the file path and name of the backup file.

Notes:

- This name is necessary to do a system restore.
- You can do backup on multiple gateways at the same time.
- When you backup a cluster, the system does backup on all members.

Restoring the System

To restore the system:

1. Right-click the Security Gateway or Security Gateways you want to restore.
2. Select **Actions > System Restore**.
The **System Restore** window opens.
3. Enter the required information.
Note - If you cannot find the name of the file in **Tasks**, or did not save the file name after you completed the backup process:
 - a) Right-click the Security Gateway.
 - b) Select **Actions > Open Shell**.
 - c) On the gateway, run the clish command: `show backup logs`.

d) Find the name of the compressed backup file.

The file is named according to this convention:

backup_<name of gateway object>_<date of backup>.tgz

4. Click **OK**.

- Connectivity to the gateway is lost
- The gateway automatically reboots

5. **Install Policy.**

The status of the restore operation shows in **Tasks** tab.

Opening Gaia WebUI and Gaia command line

From SmartConsole, you can open a command line window on the gateway or open the gateway WebUI. You can select the command line or the WebUI from the right-click menu of a gateway, or from the **Actions** button.

To open a command line window on the gateway:

1. Right-click the Security Gateway.
2. Select **Actions > Open Shell**.
 - Log in with your Gaia credentials.
 - The Open Shell uses public key authentication.
 - For a cluster object, select the member you want to connect to.

A command line window opens.

To open a gateway WebUI:

1. Right-click the Security Gateway.
2. Select **Actions > Open WebUI**.

Note - For a cluster, select the member for which you want to open the WebUI.

The WebUI opens in the default browser.

The URL is taken from the **Gateway Properties > Platform Portal** page.

Network Management

In This Section:

Network Interfaces	39
ARP	62
DHCP Server	64
Hosts and DNS	68
IPv4 Static Routes	72
IPv6 Static Routes	77
Netflow Export	80
Performance Optimization	83

This chapter includes configuration procedures and examples for network management.

Network Interfaces

Gaia supports these network interface types:

- Ethernet physical interfaces.
- Alias (Secondary IP addresses for different interface types).
- VLAN
- Bond
- Bridge
- Loopback
- 6in4 tunnel
- PPPoE



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

Interface Link Status

You can see the status of physical and logical interfaces in the WebUI or the CLI.

To see interface status using the WebUI:

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

Link Status	Description
Down (grey)	The physical interface is disabled (Down).
No link (red)	The physical interface is enabled (up), but Gaia cannot find a network connection.

Link Status	Description
Up (green)	The physical interface is enabled (up) and connected to the network.

To see interface status using the CLI, run `show interfaces all`

Physical Interfaces

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

Gaia automatically identifies physical interfaces (NICs) installed on the computer. You cannot add or delete a physical interface using the WebUI or the CLI. You cannot add, change or remove physical interface cards while the Gaia computer is running.

To add or remove an interface card:

1. Turn off the computer.
2. Add, remove or replace the interface cards.
3. Start the computer.

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

Configuring Physical Interfaces - WebUI

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

To configure a physical interface:

1. In the navigation tree, select **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. On the **IPv4** tab, do one of these:
 - Select **Obtain IPv4 address automatically** to get the IP address from the DHCP server.
 - Enter the IP address and subnet mask in the applicable fields.
5. On the **IPv6** tab, do one of these:
 - Select **Obtain IPv6 address automatically** to get the IP address from the DHCP server.
 - Enter the IP address and mask length in the applicable fields.
6. On the **Ethernet** tab, configure the link speed and duplex setting, and then do one of these:
 - Select **Auto Negotiation** to automatically configure the link speed and duplex setting.
 - Select a link speed and duplex setting from the list.
7. 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.
8. Enter a different Maximum Transmission Unit (MTU) value (minimum value=68 - default=1500).

Configuring Physical Interfaces - CLI (interface)

Description

Configure physical interfaces

Syntax

```
set interface <IF>
    ipv4-address <IP>
        mask-length <Mask>
        subnet-mask <Mask>
    ipv6-address <IP> mask-length <Mask>
    ipv6-autoconfig <on | off>
    comments <Text>
    mac-addr <MAC>
    mtu <MTU setting>
    state <on | off>
    link-speed <Speed_Duplex>
    auto-negotiation <on | off>
```

```
show interfaces all
```

Parameters

Parameter	Description
interface	Configures a physical or virtual interface
ipv4-address ipv6-address	Assigns the IPv4 or IPv6 address
ipv6-autoconfig	If on, automatically gets the IPv6 address from the DHCP
mask-length	Configures IPv4 or IPv6 subnet mask length using CIDR (/xx) notation
subnet-mask	Configures IPv4 subnet mask using dotted decimal notation
comments	Adds free text comments to an interface definition
mac-addr	Configures the interface hardware MAC address
mtu	Configure the Maximum Transmission Unit size for an interface
state	Sets interfaces status to on (enabled) or off (disabled).
link-speed	Configures the interface link speed and duplex status
auto-negotiation	Configures automatic negotiation of interface link speed and duplex settings - on (enabled) or off (disabled)
<IP>	IPv4 or IPv6 address
<IF>	Interface name
<Mask>	Interface net mask in dotted decimal or CIDR (/xx) notation as applicable
<MAC>	Manually enter the applicable hardware address

Parameter	Description
<MTU Setting>	Integer greater or equal to 68 (Default = 1500)
<Speed_Duplex>	Enter the link speed in Mbps and duplex status using one of these values: 10M/half 10M/full 100M/half 100M/full 1000M/full 10000M/full

Example

```
set interface eth2 ipv4-address 40.40.40.1 subnet-mask 255.255.255.0

set interface eth2 mtu 1500
set interface eth2 state on
set interface eth2 link-speed 1000M/full
```

Comments

There are some command options and parameters that you cannot do using the WebUI.



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

Aliases

Interface aliases let you assign more than one IPv4 address to physical or virtual interfaces (bonds, bridges, VLANs and loopbacks). This section shows you how to configure an alias using the WebUI and the CLI.

Configuration using the WebUI

To configure an interface alias using the WebUI:

1. In the navigation tree, select **Network Management > Network Interfaces**.
2. Click **Add > Alias**. To change an existing alias interface, select an interface and then click **Edit**.
3. In the **Add** (or **Edit**) **Alias** window, select **Enable** to set the alias interface status to UP.
4. On the **IPv4** tab, enter the IPv4 address and subnet mask.
5. On the **Alias** tab, select the interface to which this alias is assigned.
You cannot change the interface for an existing alias definition.

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.

To delete an interface alias:

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

Configuring Aliases - CLI (interface)

Description

Configure an alias to a physical interface.

Syntax

```
add interface <IF> alias <IP>/<Mask>
delete interface <IF> alias <Alias IF>
```

Parameters

Parameter	Description
<IP>	IPv4 address
<IF>	Interface name
<Mask>	IPv4 subnet mask length using CIDR (/xx) notation
<Alias IF>	Interface alias name in the format <IF>:XX, where XX is the automatically assigned sequence number.

Example

```
add interface eth1 alias 10.10.99.1/24
delete interface eth1 alias eth1:2
```

Comments

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.

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

VLAN Interfaces

You can configure virtual LAN (VLAN) interfaces on Ethernet interfaces. VLAN interfaces let you configure subnets with a secure private link to gateways and management servers using your existing topology. With VLAN interfaces, you can multiplex Ethernet traffic into many channels using one cable.

This section shows you how to configure VLAN interfaces using the WebUI and the CLI.

Configuring VLAN Interfaces - WebUI

To configure a VLAN interface using the WebUI:

1. In the WebUI navigation tree, select **Network Management > Network Interfaces**.
2. Click **Add > VLAN**. To change an existing VLAN interface, select an interface and then click **Edit**.
3. In the **Add** (or **Edit**) **VLAN** window, select the **Enable** option to set the VLAN interface to UP.
4. **IPv4** and **IPv6** tabs, enter the IP addresses and subnet information as necessary. You can optionally select the **Obtain IP Address automatically** option.
5. On the **VLAN** tab, enter or select a **VLAN ID** (VLAN tag) between 2 and 4094.
6. In the **Member Of** field, select the physical interface related to this VLAN.



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

Configuration Using the CLI

This section is a reference for the VLAN interface commands.

Description

Use these commands to configure bridge interfaces.

Syntax

```
add interface <IF> vlan <VLAN ID>
set interface <IF> <VLAN ID>
    ipv4-address <IP> mask-length <Length>|subnet-mask<Mask>
    ipv6-address <IP> mask-length <Length>
    ipv6-autoconfig
delete interface <IF> vlan <VLAN ID>
```

Parameters

Parameter	Description
interface	configure an interface
ipv4-address	Assign an IPv4 address
ipv6-address	Assign an IPv6 address
ipv6-autoconfig	Automatically configure an IPv6 address
on	Enable automatic configuration
off	Disable automatic configuration
<IF>	Physical interface related to this VLAN
<VLAN ID>	VLAN identifier (integer range 2-4094)
<IP>	IP address (IPv4 or IPv6)

Parameter	Description
<Length>	Mask length (integer value)

Example

```
add interface vlan eth1

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

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

delete interface eth1 vlan 99
```

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

CLI Procedures

To add a new VLAN interface:

Run `add interface <IF Name> vlan <VLAN ID>`

- <IF Name> - Physical interface associated with this VLAN
- <VLAN ID> - VLAN ID (VLAN tag)

Example:

```
add interface eth1 vlan 10
```

To add IP addresses to a VLAN interface:

Run:

```
set interface <IF Name>.<VLAN ID> ipv4-address <IPv4 Address> [ipv6-address <IPv6 Address>]
```

- <IF Name> - Physical interface associated with this VLAN
- <VLAN ID> - VLAN ID (VLAN tag)
- <IPv4 Address> - Interface IPv4 address and the subnet in CIDR notation (xxx.xxx.xxx.xxx/xx)
- <IPv6-address> - Interface IPv6 address and the prefix (only if you are using IPv6)

Examples:

```
set interface eth1.99 ipv4-address 99.99.99.1 subnet-mask 255.255.255.0
set interface eth1.99 ipv6-address 209:99:1 mask-length 64
```

To delete a VLAN Interface:

Run:

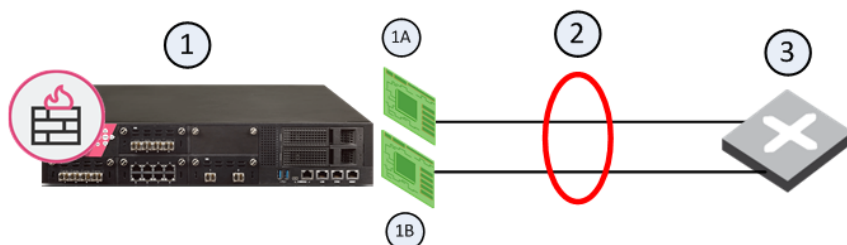
```
delete interface <IF Name> vlan <VLAN ID>
```

Example:

```
delete interface eth1 vlan 10
```

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 No.	Description
1	Security Gateway
1A	Interface 1
1B	interface 2
2	Bond Interface
3	Router

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

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

- **High Availability (Active/Backup)**: Gives redundancy when there is an interface or a link failure. This strategy also supports switch redundancy. High Availability works in **Active/Backup** mode - Interface Active/Standby mode. When an active slave interface is down, the connection automatically fails over to the primary slave interface. If the primary slave interface is not available, the connection fails over to a different slave interface.
- **Load Sharing (Active/Active)**: Slave interfaces are active simultaneously. Traffic is distributed among the slave interfaces to maximize throughput. Load Sharing does not support switch redundancy. You can configure load sharing to use one of these modes:
 - **Round Robin** - Selects the active slave interface sequentially.
 - **802.3ad** - Dynamically uses active slaves to share the traffic load. This mode uses the LACP protocol, which fully monitors the interface between the gateway and a switch.
 - **XOR** - Selects the algorithm for slave selection based on the TCP/IP layer.

Configuring Bond Interfaces - WebUI

To configure a bond interface using the WebUI:

1. Make sure that the slave interfaces do not have IP addresses.

2. On the WebUI **Network Interfaces** page, click **Enable**.
3. For a new bond interface, select **Add > Bond**. For an existing Bond interface, double-click the bond interface.
4. Select the **Enable** option to activate the bond interface.
5. On the **IPv4** and **IPv6** tabs (optional), enter the IP address information.
6. On the **Bond** tab, select or enter a **Bond Group** name. This parameter is an integer between 1 and 1024.
7. Select slave interfaces from the **Available Interfaces** list and then click **Add**.
8. Select an **Operation Mode** (**Round Robin** is the default).
9. On the **Advanced** tab, set the **Monitor Interval** to the frequency of requests to send to the monitor interface, to confirm that a slave interface is up. The valid range is 1-5000 ms and the default is 100 ms.
10. Set the Down Delay and Up Delay to the time to wait after the monitor request, before an action is taken.
11. Select the **Primary Interface** (for Active/Backup bonds only).
12. Select the **Transmit Hash Policy** (XOR or 802.3ad). Set the algorithm for interface selection according to the specified TCP/IP layer. Valid values are **layer2** (uses XOR of the physical interface MAC address) and **layer3+4** (users upper layer protocol data).
13. Select the **LACP Rate**. Set the Link Aggregation Control Protocol packet transmission rate. Valid values are **slow** (every 30 seconds) and **fast** (every 1 second).

Configuring Bond Interfaces - CLI

In the CLI, bond interfaces are known as **bonding groups**. Make sure the interfaces of the bond do not already have IP addresses.

Important: After you run a CLI command to add, configure, or delete an object, run the `save config` command to keep settings after reboot.

To create a bond interface with the CLI:

1. Create the bond interface ("[Creating or Deleting a Bond Interface](#)" on page 48).
2. Define the slave interfaces ("[Defining Interfaces](#)" on page 49) and set them to the UP State.
3. Set the bond operating mode ("[Defining the Bond Operating Mode](#)" on page 49).
4. Define other bond parameters: primary interface ("[Defining the Primary Slave Interface](#)" on page 49), media monitoring ("[Defining the Media Monitoring Interval](#)" on page 50), delay rate ("[Defining the UP and Down Delay Times](#)" on page 50).

Link Aggregation - CLI (bonding)

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

Syntax

```
{add | delete} bonding group <bondID> interface <IFName>
```

```
set bonding [group <bondID>] [primary <IFName>] [mi-interval <ms>] [up-delay <ms> | down-delay <ms>] [mode {round-robin | active-backup | xor [xmit-hash-policy {layer2 | layer3+4}]} | 8023AD [lacp-rate {slow | fast}]]]
```

```
show bonding group {<bondID> | groups}
```

Parameters

Parameter	Description
bondID	ID of bond, an integer between 1 and 1024
IFName	Name of interface to add to the bond
primary	Name of primary interface in the bond
mii-interval	Frequency that the system polls the Media Independent Interface (MII) to get status
up-delay down-delay	Waiting time to confirm the interface status before taking the specified action (0-5000 ms, default = 200 ms)
mode	Bond operating mode (" Defining the Bond Operating Mode " on page 49)
lacp-rate	Link Aggregation Control Protocol packet transmission rate: - slow - LACPDU packet sent every 30 seconds - fast - LACPDU packet sent every second
xmit-hash-policy	Algorithm for interface selected by TCP/IP layer

Example

```
set bonding group 666 20 eth2
show bonding groups
```

Output

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

Creating or Deleting a Bond Interface

To add a new bond interface:

```
add bonding group <bondID>
```

Example:

```
add bonding group 777
```

To delete a bond interface:

1. Remove all interfaces from the bond.
2. Run: `delete bonding group <bondID>`

Defining the Bond Operating Mode

Define how interfaces are activated in a bond:

- **round-robin** - Interfaces activated in order by ID (default)
- **active-backup** - On active interface down, failover to primary interface first, and to other interfaces if primary is down
- **xor** - Interface activation by TCP/IP layer (layer2 or layer3+4).
You can set the LACP packet transmission rate for **xor** mode or **8023AD** mode. After you set one of these Load Sharing modes, enter this option: `lacp-rate {slow | fast}` where **slow** is every 30 seconds, and **fast** is every one second.
- **8023AD** - Link Aggregation Control Protocol load shares traffic by dynamic interface activation, with full interface monitoring between gateway and switch. In this mode only, you can set the algorithm for interface selection, according to the specified TCP/IP layer:
`xmit-hash-policy {layer2 | layer3+4}`

To define the bond operating mode:

```
set bonding group <BondID> mode <mode> [option]
```

Example:

```
set bonding group 777 mode xor xmit-hash-policy layer3+4
```

Defining Interfaces

A bond interface typically contains between two and eight slave interfaces. This section shows how to add and remove a slave interface. The slave interface must not have IP addresses assigned to it.

To add a slave interface to a bond:

```
add bonding group <bondID> interface <IFName>
```

Example:

```
add bonding group 777 interface eth4
```



Note - Do not change the bond state manually. This is done automatically by the bonding driver.

To delete a slave interface from a bond:

```
delete bonding group <bondID> interface <IFName>
```

Example:

```
delete bonding group 777 interface eth4
```



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

Defining the Primary Slave Interface

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



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

To define the primary slave interface:

```
set bonding group <bondID> mode active-backup primary <IFName>
```

Example

```
add bonding group 777 interface eth4
set bonding group 777 mode active-backup primary eth4
```

Defining the Media Monitoring Interval

This sets the frequency of requests sent to the Media Independent Interface (MII) to confirm that a slave interface is up. The valid range is 1-5000 ms. The default is 100 ms.

To configure the monitoring interval:

```
set bonding group <bondID> mii-interval <ms>
```

Example:

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

To disable monitoring:

```
set bonding group <bondID> mii-interval 0
```

Defining the UP and Down Delay Times

This parameter defines the waiting time, in milliseconds, to confirm the slave interface status before taking the specified action. Valid values are 0 to 5000 ms. The default is 200 ms.

To configure the UP and Down delay times:

```
set bonding group <bondID> down-delay <ms>
set bonding group <bondID> up-delay <ms>
```

Example:

```
set bonding group 777 down-delay 500
```

Defining Load Sharing Parameters

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

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

To set the LACP rate:

```
set bonding group <bondID> lacp-rate {slow | fast}
```

Example: set bonding group 777 mode 8023AD lacp-rate slow

To set the Transmit Hash Policy:

```
set bonding group <bondID> xmit-hash-policy <layer>
```

Example: set bonding group 777 mode xor xmit-hash-policy layer2

Making Sure that Link Aggregation is Working

To make sure that a Link Aggregation is working for a bond interface, run this command in expert mode:

```
cat /proc/net/bonding/<bondID>
```

Example with output:

```
cat /proc/net/bonding/bond666
Ethernet Channel Bonding Driver: v3.2.4 (January 28, 2008)

Bonding Mode: fault-tolerance (active-backup)
Primary Slave: None
Currently Active Slave: eth2
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 100
Down Delay (ms): 200

Slave Interface: eth2
MII Status: up
Link Failure Count: 2
Permanent HW addr: 00:50:56:94:11:de
```

Bridge Interfaces

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

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

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

You can configure bridge mode with one gateway or with a cluster. The bridge functions without an assigned IP address. Bridged Ethernet interfaces (including aggregated interfaces) to work like ports on a physical bridge. You can configure the topology for the bridge ports in SmartConsole. There is a separate network or group object that represents the networks or subnets that connect to each port.

Notes:

- Gaia does not support Spanning Tree Protocol (STP) bridges.
- A bonded interface (slave) cannot be a bridge interface.

Check Point supports bridge interfaces that implement native, Layer-2 bridging. The bridge interfaces send traffic with Layer-2 addressing. On the same device, you can configure some interfaces as bridge interfaces, while other interfaces work as layer-3 interfaces. Traffic between bridge interfaces is inspected at Layer-2. Traffic between two Layer-3 interfaces, or between a bridge interface and a Layer-3 interface is inspected at Layer-3.

Configuring Bridge Interfaces - WebUI

To configure a bridge interface in the WebUI:

1. In the WebUI navigation tree, select **Network Interfaces**.
2. Click **Add > Bridge**, or select an interface and click **Edit**.
The **Add** (or **Edit**) **Bridge** window opens.
3. On the **Bridge** tab, enter or select a **Bridge Group** ID (unique integer between 1 and 1024).
4. Select the interfaces from the **Available Interfaces** list and then click **Add**.
5. Click the **IPv4** or **IPv6** tabs, and then enter the IP addresses and subnet.
Or click **Obtain IP Address automatically**.
6. Click **OK**.

Bridging group commands

This is a quick reference for bridge interface commands.

Description

Use these commands to configure bridge interfaces.

Syntax

```
{show | add | delete} bridging group <Group ID> [interface <interface>]
```

Parameters

Parameter	Description
<i>Group ID</i>	ID of bridging group
<i>interface</i>	Interface name

Configuring Bridge Mode with the CLI

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

To see the interfaces of an existing bridge:

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

Where *Group ID* is the unique identifier of the bridge, an integer between 0 and 1024

To create a new bridging group:

```
add bridging group <Group ID> [interface <Bridge Interface Name>]
```

To add an interface to the bridging group:

```
add bridging group <Group ID> interface <Physical interface Name>
```

Run this command one time for each physical interface.

To remove an interface from the bridging group:

```
delete bridging group <Group ID> interface <Physical interface Name>
```

Run this command one time for each physical interface.

To delete a bridging group:

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

To add or change a bridge interface IP address:

- IPv4: `set interface <Bridge interface Name> ipv4-address <IP> subnet-mask <Mask>`
- IPv6: `set interface <Bridge interface Name> ipv6-address <IP> mask-length <Prefix>`

Examples:

```
add bridging group 56 interface eth1
set interface br1 ipv6-address 3000:40::1 mask-length 64
```

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

Loopback Interfaces

You can define a virtual loopback interface by assigning an IPv4 or IPv6 address to the `lo` (local) interface. This can be useful for testing purposes or as a proxy interface for an unnumbered interface. This section shows you how to configure a loopback interface using the WebUI and the CLI.

Configuring Loopback Interfaces - WebUI

To configure a loopback interface using the WebUI:

1. In the navigation tree, select **Interface Management > Network Interfaces**.
2. Click **Add > Alias**. To change an existing loopback interface, select an interface and then click **Edit**.
3. In the **Add** (or **Edit**) window, select **Enable** to set the loopback interface status to UP.
4. On the **IPv4** tab, enter the IPv4 address and subnet mask.
5. On the **IPv6** tab, enter the IPv6 address and mask length.

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

To delete an interface alias:

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

Configuring Loopback Interfaces - CLI (interface)

Description

Configure loopback interfaces.

Syntax

```
add interface lo loopback <IP>/<Mask>
delete interface lo loopback <IF>
```

Parameters

Parameter	Description
loopback	Configures a loopback interface.
lo	You must use the <code>lo</code> (local interface) keyword to define a loopback interface.
<IP>	IPv4 or IPv6 address.
<Mask>	IPv4 subnet mask or IPv6 mask length using CIDR [/xx] notation.
<IF>	Loopback interface name (loopXX)

Example

```
add interface lo loopback 10.10.99.1/24
add interface lo loopback 2010:10:99::1/64
delete interface lo loopback loop01
```

Comments

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

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

VPN Tunnel Interfaces

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

The VPN tunnel and its properties are defined by the VPN community that contains the two gateways. You must define the VPN community and its member Security Gateways before you can create a VTI. To learn more about Route Based VPN, see *Route Based VPN* in the *R80.10 VPN Site to Site Administration Guide*

http://supportcontent.checkpoint.com/documentation_download?ID=53104.

The procedure for configuring a VTI includes these steps:

1. Make sure that the IPsec VPN Software Blade is enabled on the applicable Security Gateways.
2. Create and configure the Security Gateways.
3. Define a VPN community in SmartDashboard ("Defining the VPN Community" on page 55) that includes the two peer Security Gateways.

4. Make Route Based VPN the default option ("[Making Route Based VPN the Default Option](#)" on page 55). Do this procedure one time for each Security Management Server.
5. Define the VTI ("[Configuring VPN Tunnel Interfaces](#)" on page 56) using the WebUI or CLI.
6. Define Route Based VPN Rules ("[Defining Directional Matching VPN Rules](#)" on page 58).
7. Save the configuration and install the policy.

Defining the VPN Community

You must define the VPN Community and add the member Security Gateways to it before you configure a VPN Tunnel Interface. This section includes the basic procedure for defining a Site to Site VPN Community. To learn more about VPN communities and their definition procedures, see the *R80.10 VPN Site to Site Administration Guide*

http://supportcontent.checkpoint.com/documentation_download?ID=53104.

To define a VPN Community for Site to Site VPN:

1. In SmartConsole, click the VPN Communities tab  in the navigation tree.
2. Right-click **Site To Site** and select **New Site To Site > Meshed** or **Star**.
3. In the **Community Properties** window **General** tab, enter the VPN community name.
4. Select **Accept all encrypted traffic**.
This option automatically adds a rule to encrypt all traffic between gateways in a VPN community.
5. On the **Participating Gateways** tab, select member gateways from the list.
For star communities, use the **Center Gateways** and **Satellite Gateways** tabs to do this.
6. Configure other community parameters as necessary.
7. Save your configuration to the database.

Making Route Based VPN the Default Option

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

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

To Define an empty group:

1. In the SmartConsole navigation tree, right-click **Groups** and then select **Groups > Simple Group**.
2. In the **Group Properties** window, enter a group name in the applicable field.
Do not add members to this group.

To make Route Based VPN the default choice:

1. In SmartConsole, double-click the applicable Security Gateway.
2. In the **Gateway** window, click **Topology**.
3. In the **VPN Domain** section, select **Manually define** and then select the empty group.

Do these steps for each Security Gateway.

Configuring VPN Tunnel Interfaces

You can configure the VPN Tunnel Interfaces using Gaia WebUI or CLI.

Configuring VPN Tunnel Interfaces - WebUI

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

To configure a VPN Tunnel Interface:

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

Configuring VPN Tunnel Interfaces - CLI (vpn tunnel)

This section shows the CLI commands used to add or delete VPN Tunnel Interfaces.

Description

Add or delete a VPN Tunnel Interface (VTI)

Syntax

```
add vpn tunnel <Tunnel ID>
    type numbered local <Local IP> remote <Remote IP> peer <Peer IP>
    type unnumbered peer <Peer ID> dev <IF>
```

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

Parameters

Parameter	Description
type numbered	Defines a numbered VTI that uses a specified, static IPv4 addresses for local and remote connections.
type unnumbered	Defines an unnumbered VTI that uses the interface and the remote peer name to get addresses.
local	Defines the local peer IPv4 address (numbered VTI only).
remote	Defines the remote peer IPv4 address (numbered VTI only).

Parameter	Description
peer	Remote peer name as defined in the VPN community. You must define the two peers in the VPN community before you can define the VTI. The Peer ID is an alpha-numeric character string.
dev	Defines the interface (unnumbered VTI only)
<Tunnel ID>	Unique tunnel name (integer from 1 to 99) Gaia automatically adds the prefix 'vpnt' to the tunnel name Example: vnpt10
<Local IP>	Local peer IPv4 address (numbered VTI only) in dotted decimal format
<remote IP>	Remote peer IPv4 address (numbered VTI only) in dotted decimal format
<Peer ID>	Remote peer name as defined in the VPN community. You must define the two peers in the VPN community before you can define the VTI. The Peer ID is an alpha-numeric character string.
<IF>	Local peer interface name (unnumbered VTI only)

Example

```
add vpn tunnel 20 type numbered local 10.10.10.1 remote 20.20.20.1 peer MyPeer
add vpn tunnel 10 type unnumbered peer MyPeer dev eth1
delete vpn tunnel 10
```

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

CLI Configuration Procedures for VPN Tunnel Interfaces

To add a numbered VPN Tunnel Interface:

Run:

```
add vpn tunnel <Tunnel ID> type numbered local <Local IP> remote <Remote IP>
peer <Peer ID>
```

- **<Tunnel ID>** - Unique tunnel name (integer from 1 to 99)
Gaia automatically adds the prefix 'vpnt' to the tunnel name
- **type numbered** - Defines a **numbered** VTI that uses a specified, static IPv4 addresses for local and remote connections
- **local <Local IP>** - Local peer IPv4 address (numbered VTI only) in dotted decimal format
- **remote <Remote IP>** - Remote peer IPv4 address (numbered VTI only) in dotted decimal format

- **peer <Peer ID>** - Remote peer name as defined in the VPN community. You must define the two peers in the VPN community before you can define the VTI. The Peer ID is an alpha-numeric character string.

To add an unnumbered VPN Tunnel Interface:

Run:

```
add vpn tunnel <Tunnel ID> type unnumbered local peer <Peer ID>
```

- **<Tunnel ID>** - Unique tunnel name (integer from 1 to 99)
Gaia automatically adds the prefix 'vpnt' to the tunnel name
- **type unnumbered** - Defines an **unnumbered** VTI that uses the interface and the remote peer name to get addresses
- **peer <Peer ID>** - Remote peer name as defined in the VPN community. You must define the two peers in the VPN community before you can define the VTI. The Peer ID is an alpha-numeric character string.
- **dev <IF>** - Local peer interface name (unnumbered VTI only)

To Delete a VPN Tunnel Interface

Run:

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

- **<Tunnel ID>** - Unique tunnel name (integer from 1 to 99)
Gaia automatically adds the prefix 'vpnt' to the tunnel name

Defining VPN Rules

To make sure that your security rules work correctly with Route Based VPN traffic, you must add directional matching conditions and allow OSPF traffic. This section includes procedures for configuring security rules to do this.

Defining Directional Matching VPN Rules

This section contains the procedure for defining directional matching rules. Directional matching is necessary for Route Based VPN when a VPN community is included in the VPN column in the rule. This is because without bi-directional matching, the rule only applies to connections between a community and an encryption domain (Domain Based Routing).

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

The directional rule must contain these directional matching conditions:

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

MyIntranet is the name of a VPN Community. **Internal_Clear** refers to all traffic from IP addresses to and from the specified VPN community.

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



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

To enable VPN directional matching:

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

To define a VPN directional matching rule:

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

Defining Rules to Allow OSPF Traffic

One advantage of Route Based VPN is the fact that you can use dynamic routing protocols to distribute routing information between Security Gateways. The OSPF (Open Shortest Path First) protocol is commonly used with VTIs. This section shows you how to allow OSPF traffic in a VPN community.

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

To Allow OSPF traffic for a VPN Community:

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

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

Completing the VTI Configuration

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

To complete the VTI configuration:

1. Save the configuration to the database.
2. Install the policy to the gateways.
3. Make sure that the VTI tunnel and the rules are working correctly.

CLI Reference (interface)

This section summarizes the CLI `interface` command and its parameters.

Description

Add, delete and configure interface properties.

Syntax

```
add interface <IF>
    6in4 <Tunnel ID> remote <IP> ttl <Time>
    6to4 <Tunnel ID> ttl <Time>
    alias <IP>
    loopback <IP>
    vlan <VLAN ID>
delete interface <IF>
    6in4 <Tunnel ID>
    6to4 <Tunnel ID>
    alias <IP>
    ipv4-address <IP>
    ipv6-address <IP>
    ipv6-autoconfig
    loopback <IP>
    vlan <VLAN ID>
set interface <IF>
    ipv4-address <IP>
        mask-length <Mask>
        subnet-mask <Mask>
    ipv6-address <IP> mask-length <Mask>
    ipv6-autoconfig <on | off>
    comments <Text>
    mac-addr <MAC>
    mtu <MTU setting>
    state <on | off>
    link-speed <Speed Duplex>
```

auto-negotiation <on | off>

Parameters

Parameter	Description
interface	Configures a physical or virtual interface
6in4	Configures a 6in4 tunnel for IPv6 traffic over an IPv4 network
6to4	Configures a 6to4 tunnel for IPv6 traffic over an IPv4 network
remote	Sets the remote IP address for a 6in4 or 6to4 tunnel
ttl	Sets the time-to-live value for a 6in4 or 6to4 tunnel
alias	Assigns more than one IP addresses to a physical interface (IPv4 only)
loopback	Assigns an IP address to a logical loopback interface. This can be useful as a proxy for an unnumbered interface.
vlan	Assigns a VLAN tag to an existing physical interface to create a logical subnet.
ipv4-address ipv6-address	Assigns the IPv4 or IPv6 address
ipv6-autoconfig	If on, automatically gets the IPv6 address from the DHCP
mask-length	Configures IPv4 or IPv6 subnet mask length using CIDR (/xx) notation
subnet-mask	Configures IPv4 subnet mask using dotted decimal notation
comments	Adds free text comments to an interface definition
mac-addr	Configures the interface hardware MAC address
mtu	Configure the Maximum Transmission Unit size for an interface
state	Sets interfaces status to on (enabled) or off (disabled).
link-speed	Configures the interface link speed and duplex status
auto-negotiation	Configures automatic negotiation of interface link speed and duplex settings - on (enabled) or off (disabled)
<Tunnel ID>	Unique tunnel identifier (Integer in the range 2-4094)
<IP>	IPv4 or IPv6 address
<IF>	Interface name
<Time>	TTL time in seconds in the range 0-255 (default = 0)

Parameter	Description
<VLAN ID>	Integer in the range 2-4094
<Mask>	Interface net mask in dotted decimal or CIDR [/xx] notation as applicable
<MAC>	Manually enter the applicable hardware address
<MTU Setting>	Integer greater or equal to 68 (Default = 1500)
<Speed>	Enter the link speed in Mbps and duplex status using one of these values: 10M/half 10M/full 100M/half 100M/full 1000M/full 10000M/full

Example

See the interface configuration section

Comments

There are some command options and parameters that you cannot do using the WebUI.

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- WebUI

To show dynamic ARP entries

1. In the WebUI, go to the **Network Management > ARP** page.
2. Click the **Monitoring** tab.

To show static ARP entries

1. In the WebUI, go to the **Network Management > ARP** page.
2. Click the **Configuration** tab.

To change Static and dynamic ARP parameters

1. In the WebUI, go to the **Network Management > ARP** page.

2. In the **Configuration** tab, **ARP Table Settings** section:

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

Default: 4096, Range: 1024-16384

Note – Make sure to configure a value large enough to accommodate at least 100 dynamic entries, in addition to the maximum number of static entries.

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

Default: 60 (seconds), Range: 60-86400 (24 hours)

To add a static ARP entry

1. In the WebUI, go to the **Network Management > ARP** page.
2. In the **Configuration** tab, **Static ARP Entries** section, click **Add**.
3. Enter the **IP Address** of the static ARP entry and the **MAC Address** used when forwarding packets to the IP address.
4. Click **OK**.

To delete a Static ARP entry

1. In the WebUI, go to the **Network Management > ARP** page.
2. In the **Configuration** tab, **Static ARP Entries** section, select a Static ARP entry
3. Click **Remove**.

To flush all dynamic ARP entries

1. In the WebUI, go to the **Network Management > ARP** page.
2. In the **Monitoring** tab, click **Flush All**.

Configuring ARP - CLI (arp)

Description

Commands to configure the Address Resolution Protocol (ARP)

Syntax

To add a static arp entry

```
add arp static ipv4-address VALUE macaddress VALUE
```

To delete static and dynamic arp entries

```
delete arp dynamic all
delete arp static ipv4-address VALUE
```

To set arp parameters

```
set arp table validity-timeout VALUE
set arp table cache-size VALUE
```

To show arp parameters

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

Parameters

Parameter	Description
static	Configured static arp entries
dynamic	Configured dynamic arp entries
ipv4-address	IP Address of a static ARP entry. Range: Dotted-quad ([0-255].[0-255].[0-255].[0-255]). Default: No Default
macaddress	The hardware address used when forwarding packets to the given IP address. Range: Six hexadecimal octets separated by colon. Default: No Default
table validity-timeout	This is the time, in seconds, to keep resolved dynamic ARP entries. If the entry is not referred to and is not used by traffic before the time elapses, it is deleted. Otherwise, a request will be sent to verify the MAC address. Default: 60 (seconds), Range: 60-86400 (24 hours)
table cache-size	This is the maximum number of entries in the ARP cache. Default: 4096, Range: 1024-16384 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.

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

DHCP Server

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

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

1. To define a DHCP subnet on a Gaia device interface:
 - a) Enable DHCP 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 hosts.
2. Define additional DHCP subnets on other Gaia interfaces, as needed.
3. Enable the DHCP server process.
4. Configure the network hosts to use the DHCP server.

Configuring a DHCP Server- WebUI

To allocate DHCP parameters to hosts

1. In the tree view, 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.
4. In the **Subnet** tab, enter the **Network IP Address** of the interface. Click **Get from interface** to do this automatically.
5. Enter the **Subnet mask**.
6. In the **Address Pool** section, click **Add** and define the range of IPv4 addresses that the server assigns to hosts.
7. Optional: Define a **Default Lease** in seconds, for host IPv4 addresses. This applies only if clients do not request a unique lease time. If you do not enter a value, the configuration default is 43,200 seconds.
8. Optional: Define a **Maximum 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.
9. Optional: Click the **Routing & DNS** tab to define routing and DNS parameters for hosts:
 - **Default Gateway**. The IPv4 address of the default gateway for the network hosts
 - **Domain Name**. The domain name of the network hosts. For example, `example.com`.
 - **Primary DNS Server**. The DNS server that the network hosts use to resolve hostnames.
 - **Secondary DNS Server**. The DNS server that the network hosts use to resolve hostnames if the primary server does not respond.
 - **Tertiary DNS Server**. The DNS server that the network hosts use to resolve hostnames if the primary and secondary servers do not respond.
10. Click **OK**.
11. Optional: Define DHCP subnets on other Gaia interfaces, as needed.

12. In the main **DHCP Server** page, select **Enable DHCP Server**.

13. Click **Apply**.

The DHCP server on Gaia is now configured and enabled.

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

Configuring a DHCP Server - CLI (dhcp)

DHCP Server commands allow you to configure the Gaia device as DHCP server for network hosts.

Syntax

To create DHCP Server subnets:

```
add dhcp server subnet VALUE
    netmask VALUE
    include-ip-pool start VALUE end VALUE
    exclude-ip-pool start VALUE end VALUE
```

To change DHCP Server subnet configurations:

```
set dhcp server subnet VALUE
    enable
    disable
    include-ip-pool VALUE enable
    include-ip-pool VALUE disable
    exclude-ip-pool VALUE enable
    exclude-ip-pool VALUE disable
    default-lease VALUE
    max-lease VALUE
    default-gateway VALUE
    domain VALUE
    dns VALUE
```

To delete DHCP Server subnets:

```
delete dhcp server subnet VALUE
    exclude-ip-pool VALUE
    include-ip-pool VALUE
```

To enable or disable the DHCP Server process:

```
set dhcp server
    disable
    enable
```

To view DHCP Server configurations

```
show dhcp server
    all
    status
    subnet VALUE ip-pools
    subnets
```

Parameters

Parameter	Description
subnet VALUE	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 VALUE	The IPv4 subnet mask in CIDR notation. For example, 24
start VALUE	The IPv4 address that starts the allocated IP Pool range. For example 192.0.2.20
end VALUE	The IPv4 address that ends the allocated IP Pool range. For example 192.0.2.90
include-ip-pool VALUE	The range of IPv4 addresses to include in the IP pool. For example 192.0.2.20-192.0.2.90
exclude-ip-pool VALUE	The range of IPv4 addresses to exclude from the IP pool. For example: 192.0.2.155-192.0.2.254
enable	Enable the DHCP Server subnet, or the DHCP Server process (depending on the context).
disable	Disable the DHCP Server subnet, or the DHCP Server process (depending on the context).
default-lease VALUE	The default lease in seconds, for host IPv4 addresses. Applies only if clients do not request a unique lease time. If you do not enter a value, the default is 43,200 seconds.
max-lease VALUE	The maximum 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 VALUE	The IPv4 address of the default gateway for the network hosts
domain VALUE	The domain name of the network hosts. For example, example.com.
dns VALUE	The DNS servers that the network hosts will use to resolve hostnames. Optionally, specify a primary, secondary and tertiary server in the order of precedence. For example 192.0.2.101, 192.0.2.102, 192.0.2.103
all	All DHCP server configuration settings.
subnets	DHCP Server subnet configuration settings.

subnet VALUE ip-pools	The IP pools in the DHCP Server subnet, and their status: Enabled or Disabled.
status	The status of the DHCP Server process: Enabled or disabled.

Example

```
gw-9403be> show dhcp server all
```

Output

```
DHCP Server Enabled
DHCP-Subnet 192.0.2.0
  State           Enabled
  Net-Mask        24
  Maximum-Lease   86400
  Default-Lease   43200
  Domain          example.com
  Default Gateway 192.0.2.103
  DNS             192.0.2.101, 192.0.2.102, 192.0.2.103
  Pools (Include List)
    192.0.2.20-192.0.2.90      : enabled
    192.0.2.120-192.0.2.150   : disabled
  Pools (Exclude List)
    192.0.2.155-192.0.2.254   : enabled
DHCP-Subnet 192.0.2.155
  State           Disabled
  Net-Mask        24
  Maximum-Lease   86400
  Default-Lease   43200
  Pools (Include List)
    192.0.2.10-192.0.2.99     : enabled
DHCP-Subnet 192.0.2.200
  State           Disabled
  Net-Mask        24
  Maximum-Lease   86400
  Default-Lease   43200
```

Hosts and DNS

Host Name

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

Configuring Host Name - WebUI

To show the host name

The host name is in the header of the WebUI.

To change the host name

1. Open the **Network Management > Host and DNS** page.
2. In the **System Name** section, enter the

- **Host Name.** The network name of the Gaia device.
- **Domain Name** (optional). For example, `example.com`.

Configuring Host Name - CLI (hostname)

Description

Use this group of commands to configure the host name of your platform.

Syntax

```
set hostname VALUE
show hostname
```

Host Addresses

You should add host addresses for systems that will communicate frequently with the system. You can:

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

Configuring Hosts- WebUI

To add a static host entry

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

To edit a static host entry

1. Go to the **Network Management > Hosts and DNS** page.
2. In the **Hosts** section, select a host and click **Edit**.
3. Edit the
 - **Host Name**
 - **IPv4 address**
 - **IPv6 address**

To delete a static host entry

1. Go to the **Network Management > Hosts and DNS** page.
2. In the **Hosts** section, select a host and click **Delete**.

Configuring Hosts - CLI (host)

Description

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

Syntax

To add a host name and address:

```
add host name VALUE ipv4-address VALUE
add host name VALUE ipv6-address VALUE
```

To edit the name and IPv4 or IPv6 address of a host:

```
set host name VALUE ipv4-address VALUE
set host name VALUE ipv6-address VALUE
```

To delete a host name and address:

```
delete host name VALUE ipv4
delete host name VALUE ipv6
```

To show an IPv4 or IPv6 host address:

```
show host name VALUE ipv4
show host name VALUE ipv6
```

To show all IPv4 or IPv6 hosts:

```
show host names ipv4
show host names ipv6
```

Parameters

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

Domain Name Service (DNS)

Gaia uses the Domain Name Service (DNS) to translate host names into IP addresses. To enable DNS lookups, you must enter the primary DNS server for your system. You can also enter secondary and tertiary DNS servers. When the system resolves host names, it consults the primary name server. If a failure or time-out occurs, the system consults the secondary name server, and if necessary, the tertiary.

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

Configuring DNS - WebUI

To configure the DNS Server for the Gaia computer:

1. In the WebUI, go to the **Network Management > Hosts and DNS** page.
2. In the **System Name** section, enter the **Domain Name**. For example, `example.com`.
3. In the **DNS** Section, enter the:

DNS Suffix. The name at the end of all DNS searches if they fail. By default, it must be the local domain name.

A valid domain name suffix is made up of subdomain strings separated by periods. Subdomain strings must begin with an alphabetic letter and can consist only of alphanumeric characters and hyphens. The domain name syntax is described in RFC 1035 (modified slightly in RFC 1123). **Note -** Domain names that are also valid numeric IP addresses, for example 10.19.76.100, though syntactically correct, are not permitted.

For example, if you set the DNS Suffix to `example.com` and try to ping some host `foo` (with `ping foo`), and `foo` cannot be resolved, then the resolving computer tries to resolve `foo.example.com`.

- a) IPv4 address or IPv6 of the **Primary DNS Server**. The server which resolves host names. This must be a host which runs a DNS server.
- b) (Optional) IPv4 or IPv6 address of the **Secondary DNS Server**. The server which resolves host names if the primary server does not respond. This must be a host which runs a DNS server.
- c) (Optional) IPv4 or IPv6 address of the **Tertiary DNS Server**. The server which resolves host names if the primary and secondary servers do not respond. This must be a host which runs a DNS server.

Configuring DNS - CLI (*dns*)

Description

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

Syntax

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

```
set dns primary VALUE
set dns secondary VALUE
set dns tertiary VALUE
set dns suffix VALUE
```

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

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

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

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

delete dns suffix

Parameters

Parameter	Description
primary VALUE	The server which resolve host names. This must be a host which runs a DNS server. An IPv4 or IPv6 address.
secondary VALUE	The server which resolves host names if the primary server does not respond. This must be a host which runs a DNS server. An IPv4 or IPv6 address.
tertiary VALUE	The server which resolves host names if the primary and secondary servers do not respond. This must be a host which runs a DNS server. An IPv4 or IPv6 address.
suffix VALUE	The name at the end of all DNS searches if they fail. By default, it must be the local domain name. A valid domain name suffix is made up of subdomain strings separated by periods. Subdomain strings must begin with an alphabetic letter and can contain only alphanumeric characters and hyphens. The domain name syntax is described in RFC 1035 (modified slightly in RFC 1123). Note: Domain names that are also valid numeric IP addresses, for example 10.19.76.100, though syntactically correct, are not permitted. For example, if you set the DNS Suffix to <code>example.com</code> and try to ping some host <code>foo</code> (by running <code>ping foo</code>), and <code>foo</code> cannot be resolved, then the resolving computer will try to resolve <code>foo.example.com</code> .

IPv4 Static Routes

A static route defines the destination and one or more paths (next hops) to get to that destination. You define static routes manually using the WebUI or the `set static-route` command from the CLI.

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 IP address.
- Route type:
 - **Normal** - Accepts and sends packets to the specified destination.
 - **Reject** - Drops packets and sends an error message to the traffic source.
 - **Black hole** - Drops packets but does not send an error message.
- Next-hop gateway type:
 - **Address** - Identifies the next hop gateway by its IP address.

- **Logical** - Identifies the next hop gateway by the interface that connects to it. Use this option only if the next hop gateway has an unnumbered interface.
- Gateway identifier - IP address or interface name.
- 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 CLI to configure the rank.

Configuring IPv4 Static Routes - WebUI

You can configure static routes one at a time or use the Batch Mode to configure many routes simultaneously.

To configure one static route at a time:

1. In the WebUI navigation tree, select **IPv4 Static Routes**.
2. In the **IPv4 Static Routes** pane, click **Add**
or
Select a route and click **Edit** to change an existing route.
3. In the **Add (or Edit) Destination Route** window, enter the IPv4 address and subnet mask.
4. Select the **Next Hop Type**.
 - **Normal** - Accepts and sends packets to the specified destination.
 - **Reject** - Drops packets and sends an error message to the traffic source.
 - **Black Hole** - Drops packets but does not send an error message.
5. Click **Add gateway** or double-click an existing gateway.
6. For new interfaces only, select an interface type.
 - **Normal** - Identifies the destination gateway by its IP address.
 - **Network Interface** - Identifies the next hop gateway by the interface that connects to it. Use this option only if the next hop gateway has an unnumbered interface. This option is known as a logical interface in the CLI.
7. **Optional:** Select **Local Scope**. Defines a static route with a link-local scope. Use this setting on a cluster member when the ClusterXL Virtual IP address is in a different subnet than the physical interface address. This allows the cluster member to accept static routes on the subnet of the Cluster Virtual address.
8. **Optional:** Select **Ping** to send periodic ICMP packets to the route destination.
This action makes sure that the connection is alive. If no answer is returned, the route is deleted from the routing table.
9. **Optional:** Enter or select a **Rank**.
This is a route priority value to use when there are many routes to a destination that use different routing protocols. The route with the lowest rank value is selected. Default = 0.
10. In the **Add (or Edit) Interface gateway** window, enter the IP address or interface name.
11. Select a **Priority** between 1 and 8. The priority sets the order for the selection of the next hop among many gateways. 1 (default) is the highest priority and 8 is the lowest. This parameter is required.

Configuring Many Static Routes at Once

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



Note - You cannot configure a network (logical) interface using this option.

To add many static routes at once:

1. In the WebUI navigation tree, select **Static Routes**.
2. In the **Static Routes** pane, click **Add Multiple Static Routes**.
3. In the **Add Multiple Routes** window, select the **Next Hop Type**.
 - **Normal** - Accepts and sends packets to the specified destination
 - **Reject** - Drops packets and sends an error message to the traffic source
 - **Black Hole** - Drops packets but does not send an error message

4. Add the routes in the text box, using this syntax:

`<Destination IP>/<Mask length> <Next Hop IP> [<Comment>]`

default - Use this as an alternative to the default route IP address

Destination IP - Destination IP address using dotted decimal notation

Mask length - Net mask using slash (/xx) notation

Next Hop IP - Next hop gateway IP address using dotted decimal notation

Comment - Optional free text comment

Examples:

`default 192.0.2.100 192.0.2.1 "Default Route"`

`192.0.2.200 192.0.2.18`

5. Click **Apply**.

The newly configured more static routes show in the list of Static Routes in the **Static Routes** page.



Note - The text box shows entries that contain errors with messages at the top of the page.

6. Correct errors and reload the affected routes.
7. Click the **Monitoring** tab to make sure that the routes are configured correctly.

Configuring Static Routes - CLI (static-route)

You only use the `set` operation with the `static-route` command, even when adding or deleting a static route.

Description

Add, change or delete an IPv4 static route.

Syntax

```
set static-route <Destination>
```

```
    nexthop gateway address <GW IP> [priority <P Value>] on|off
```

```
    nexthop gateway logical <GW IF> [priority <P Value>] on|off
```

```
    nexthop blackhole
```

```
    nexthop reject
```

```
    scopelocal on
```

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

```
set static-route <Destination> rank <0-255>
```

Parameters

Parameter	Description
<code>nexthop</code>	Defines the next hop path, which can be a <code>gateway</code> , <code>blackhole</code> or <code>reject</code> .
<code>gateway</code>	Accepts and sends packets to the specified destination.
<code>blackhole</code>	Drops packets, but does not send an error message.
<code>reject</code>	Drops packets and sends an error message to the traffic source.
<code>address</code>	Identifies the next hop gateway by its IP address.
<code>logical</code>	Identifies the next hop gateway by the interface that connects to it. Use this option only if the next hop gateway has an unnumbered interface.
<code>priority</code>	Assigns a path priority if there are many different paths. The available path with the lowest priority value is selected.
<code>on</code>	Adds the specified route or next hop.
<code>off</code>	Deletes the specified route or next hop. If you specify a next hop, only the specified path is deleted. If no next hop is specified, the route and all related paths are deleted.
<code>rank</code>	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>nexthop</code> keyword with no other parameters.
<code>scope local</code>	Defines a static route with a link-local scope. Use this setting on a cluster member when the ClusterXL Virtual IP address is in a different subnet than the physical interface address. This lets the cluster member accept static routes on the subnet of the Cluster Virtual address.
<code><Destination></code>	Destination IP address using dotted decimal/mask length (slash) notation. You can use the <code>default</code> keyword instead of an IP address when referring to the default route.
<code><GW IP></code>	Gateway IP address in dotted decimal notation in dotted decimal format without a net mask.
<code><GW IF></code>	Name of the interface that connects to the next hop gateway.
<code><P Value></code>	Priority. An integer between 1 and 8 (default=1).

Parameter	Description
<Rank Value>	Rank. An integer between 0 and 255 (default=0).

Example

```
set static-route 192.0.2.100 nexthop gateway address 192.0.2.155 on
set static-route 192.0.2.100 nexthop gateway address 192.0.2.18 off
set static-route 192.0.2.0/24 off
set static-route 192.0.2.100 nexthop blackhole
set static-route 192.0.2.0/24 rank 2
```

Comments

There are no add commands for the static-route feature. To show static routes, run `show route static`

CLI Procedures

This section includes some basic procedures for managing static routes using the CLI.

To show static routes, run

```
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
```

To add a static route, run:

```
set static-route <Destination> nexthop gateway <GW IP> on
set static-route <Destination> nexthop gateway <GW IF> on
```

Destination - Destination IP address.

GW IP - Next hop gateway IP address.

GW IF - Interface that connects to the next hop.

Example:

```
set static-route 192.0.2.100 nexthop gateway address 192.0.2.10 on
set static-route 192.0.2.100 nexthop gateway logical 192.0.2.10 on
```

To add a static route with paths and priorities, run:

```
set static-route <Destination> nexthop gateway <GW ID> priority <P Value>
```

Destination - Destination IP address

GW IP - Next hop gateway IP address

P Value - Integer between 1 and 8 (default =1)

Run this command for each path, assigning a priority value to each. You can define two or more paths using the same priority to specify a backup path with equal priority.

Examples:

```
set static-route 192.0.2.100 nexthop gateway address 192.0.2.10 on
priority 1
```

```
set static-route 192.0.2.100 nexthop gateway address 192.0.2.10 on
priority 1
```

```
set static-route 192.0.2.0/24 nexthop gateway logical eth4 on priority 2
```

```
set static-route 192.0.2.0/24 nexthop gateway logical eth5 on priority 3
```

To add a static route where packets are dropped, run:

```
set static-route <Destination> nexthop reject
set static-route <Destination> nexthop blackhole
```

Destination - Destination IP address.

Reject - Drops packets and sends an error message to the traffic source.

Blackhole - Drops packets but does not send an error message.

Examples:

```
set static-route 192.0.2.0/24 nexthop reject
```

or

```
set static-route 192.0.2.0/24 nexthop blackhole
```

To delete a route and all related paths, run:

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

Destination - Destination IP address.

Example:

```
set static-route 192.0.2.0/24 off
```

To delete a path only, run:

```
set static-route <Destination> nexthop gateway <GW ID> off
```

Destination - Destination IP address.

GW ID - Next hop gateway IP address or interface name.

Example:

```
set static-route 192.0.2.10 nexthop gateway address 192.0.2.100 off
```

IPv6 Static Routes

Configuring IPv6 Static Routes - WebUI

You can configure IPv6 static routes one at a time.

To configure one static route at a time:

1. In the WebUI navigation tree, select **IPv6 Static Routes**.
2. In the **IPv6 Static Routes** pane, click **Add**
or
Select a route and click **Edit** to change an existing route.
3. In the **Add** (or **Edit**) **Destination Route** window, enter the IPv6 address and prefix (default = 64).
4. Select the **Next Hop Type**.
 - **Normal** - Accepts and sends packets to the specified destination.

- **Reject** - Drops packets and sends an error message to the traffic source.
 - **Black Hole** - Drops packets but does not send an error message.
5. Click **Add Gateway** or double-click an existing gateway.
 6. In the **Add** (or **Edit**) **Gateway** window, enter the IP address or interface name.
 7. Select a **Priority** between 1 and 8. The priority defines the sequence for selecting the next hop among many gateways. 1 is the highest priority and 8 is the lowest. This parameter is required.

Configuring IPv6 Static Routes - CLI (set ipv6 static-route)

Use `set ipv6 static-route` to add, change, or delete IPv6 static routes.

Syntax

```
> set ipv6 static-route <source_ip> nexthop gateway <gw_ip> [priority <p_val>] on|off [interface <gw_if> [priority <p_val>]] on
> set ipv6 static-route <source_ip> nexthop [<gw_ip>] blackhole|reject|off
```

Syntax	Description
gateway	Defines the next hop path.
<source_ip>	Defines the source IPv6 IP address and subnet.
<gw_ip>	Identifies the next hop gateway by its IP address.
<gw_if>	Identifies the next hop gateway by the interface that connects to it. Use this option only if the next hop gateway has an unnumbered interface.
priority	Assigns a path priority when there are many different paths. The available path with the lowest priority value is selected. The gateway with the lowest priority value is selected.
interface	Identifies the next hop gateway by the interface that connects to it. Use this option only if the next hop gateway has an unnumbered interface.
<p_val>	Priority value for a route or interface. Valid values are integers between 1 and 8. Default = 1
on	Enables the specified route or next hop.
off	Deletes the specified route or next hop. If you specify a next hop, only the specified path is deleted. If no next hop is specified, the route and all related paths are deleted.
blackhole	Drops packets but does not send an error message.
reject	Drops packets and sends an error message to the traffic source.

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

Troubleshooting

Symptoms

- You cannot configure the VPN Software Blade.
- This message shows: VPN blade demands gateway's IP address corresponding to the interface's IP addresses

Cause

IPv6 is active, but the main IPv6 address is not configured.

Solution

Configure the main IPv6 address in **General Properties**.

CLI Procedures - IPv6 Static Routes

This section includes some basic procedures for managing static routes using the CLI.

To show IPv6 static routes, run

```
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
```

To add an IPv6 static route, run:

```
set ipv6 static-route <Destination> nexthop gateway <GW IP> on
set ipv6 static-route <Destination> nexthop gateway <GW IP> interface
<GW IF> on
```

Destination - Destination IPv6 address.

GW IP - Next hop gateway IPv6 address.

GW IF - Next hop gateway interface name.

Example:

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

To add an IPv6 static route with paths and priorities, run:

```
set static-route <Destination> nexthop gateway <GW ID> priority <P Value>
```

Destination - Destination IP address.

GW IP - Next hop gateway IP address.

P Value - Integer between 1 and 8 (default =1)

Run this command for each path, assigning a priority value to each. You can define two or more paths using the same priority to specify a backup path with equal priority.

Example:

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

To add an IPv6 static route where packets are dropped, run:

```
set ipv6 static-route <Destination> nexthop reject
set ipv6 static-route <Destination> nexthop blackhole
```

Destination - Destination IP address.

Reject - Drops packets and sends an error message to the traffic source.

Blackhole - Drops packets, but does not send an error message.

Examples:

```
set ipv6 static-route 3100:192::0/64 nexthop reject
or
set ipv6 static-route 3100:192::0/64 nexthop blackhole
```

To delete an IPv6 route and all related paths, run:

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

Destination - Destination IP address.

Example:

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

To delete a path only, run:

```
set static-route <Destination> nexthop gateway <GW IP> off
```

Destination - Destination IP address.

GW IP - Next hop gateway IP address or interface name.

Example:

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

Netflow Export

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

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

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

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

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

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

Notes:

- The IP addresses and TCP/UDP ports reported by NetFlow are the ones on which it expects to receive traffic. Therefore, for NATted connections, one of the two directions of flow is reported with the NATted address.
- If SecureXL is not enabled or not working, NetFlow packets are not sent.

- NetFlow sends the connection records after the connections have terminated. If the system is idle or the connections are long-lasting, you may have to wait to see NetFlow packets.

Flow Records

You can configure Gaia to export flow records using NetFlow Versions 5 or 9. (Version 9 is specified in RFC 3954.) Regardless of which export format you choose, Gaia exports values for the following fields:

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

Configuring Netflow Export - WebUI

To configure NetFlows using the WebUI:

1. Open the **Network Management > NetFlow Export** page of the WebUI.
2. Click **Add**.
3. Enter the required data.

Netflows Data to Prepare for each collector:

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

Configuring Netflow Export - CLI (netflow)

To add a collector:

```
add netflow collector ip VALUE port VALUE [srcaddr VALUE export-format VALUE]
```

To delete a collector:

```
delete netflow collector [for-ip VALUE [for-port VALUE]]
```

To change settings of a collector:

```
set netflow collector [for-ip VALUE [for-port VALUE]]
    export-format VALUE
    srcaddr VALUE
```

```
set netflow collector [for-ip VALUE]
    port VALUE
```

```
set netflow collector
    ip VALUE
```

Parameter	Description
ip VALUE	The IPv4 address to which NetFlow packets are sent. This is mandatory.
port VALUE	The UDP port number on which the collector is listening. This is mandatory. There is no default or standard port number for NetFlow.
srcaddr VALUE	Optional: The IPv4 address of the NetFlow packets source. This must be an IP address of the local host. The default (which is recommended) is an IP address from the network interface on which the NetFlow traffic is going out.
export-format VALUE	The NetFlow protocol version to send: 5 or 9 . Each has a different packet format. The default is 9 .
for-ip VALUE for-port VALUE	The for-ip and for-port parameters specify the collector that the command operates on. If you only have one collector configured, you do not need these parameters. If you have two or three collectors with different IP addresses, use for-ip . If you have two or three collectors with the same IP address and different UDP ports, you must use for-ip and for-port to identify the one you want to work on.

Monitoring NetFlow Configuration

To see NetFlow configurations:

```
show netflow all
show netflow collector [for-ip VALUE [for-port VALUE]]
show netflow collector [for-ip VALUE [for-port VALUE]]
    export-format
    srcaddr
show netflow collector [for-ip VALUE] port
show netflow collector ip
```

Performance Optimization

Use Performance Optimization to get best results for performance tests on multi-core appliances and open servers. CoreXL, Performance Pack and Multi-Queue technologies are used to get best results.

How is performance measured?

There are different ways of measuring performance:

- **Packet Rate** – How many packets the gateway can forward per second. Usually measured with 64 bytes UDP packets.
- **Throughput** – How many bits the gateway can forward per second. Measured using large packets, usually 1518 byte packets.
- **TCP Session Rate** – How many connections can be opened and closed per second.

Performance Optimization Terms and Concepts

SecureXL - A Check Point patented open interface that offloads security processing to optimized hardware or software processing units. Makes it possible to get multi-gigabit Firewall and VPN performance on Security Gateways.

Performance Pack – A Check Point software product that uses SecureXL technology to increase the speed of IPv6 and IPv4 traffic. It is installed on a gateway, and gives significant performance improvements for Security Gateways.

Connection Templates - A mechanism that is used by SecureXL acceleration devices to improve session rates by opening connections more quickly. When a connection is opened, the Firewall offloads to the acceleration device a *template* for this connection type. The template increases the throughput of connections between the same IP addresses, same destination port, same protocol and same interfaces, starting the first packet.

CoreXL - A Check Point performance-enhancing technology for Security Gateways on multi-core (CPU) processing platforms. It enhances performance by letting the processing cores do multiple tasks at the same time. It provides almost linear scalability of performance for each processing core.

Multi-Queue

Multi-Queue improves the performance of SecureXL acceleration on multi-core Security Gateways. Traffic entering a network interface card (NIC) traffic queue is:

- Accelerated by Performance Pack or
- Directed to a CoreXL core that processes traffic that is not accelerated, because it must be inspected by Software Blades.

By default, each network interface has one traffic queue that is handled by one CPU at a time.

Multi-Queue lets you configure more than one traffic queue for each network interface. This means more than one CPU can be used for acceleration.

Configuring Performance Optimization - WebUI

This page shows in the WebUI for R76 and higher appliances and open servers with:

- More than 6 cores (CPUs), and
- Interfaces that support Multi-Queue: igb (1 Gigabit/s) and ixgbe (10 Gigabit/s) interfaces.

To configure Performance Optimization

1. Choose one of these options
 - **Optimize for Software Blades** - Best Software Blades performance. Most cores are assigned to CoreXL instances. Select if you enabled more blades than the Firewall Blade and the VPN Blade.
 - **Optimize for Session Rate** - Best session rate for template connections. Up to 4 cores are assigned to Performance Pack. Recommended Multi-Queue interface configuration is applied.
 - **Optimize for Packet Rate and Throughput** - Best small or large packet accelerated throughput. Up to 6 cores are assigned to Performance Pack. Recommended Multi-Queue Interface configuration is applied.
 - **Custom** - Assign cores to Performance Pack and CoreXL using the **Core Split** slider. This is the equivalent of the **Configure Check Point CoreXL** option in `cpconfig` and the `cpmq` configuration utility.
2. Click **Apply**.
3. Reboot.

Core Split

Shows how the cores on the Security Gateway are used for each **Performance Optimization** option.

Multi-Queue

You cannot configure Multi-Queue if you select **Optimize for Software Blades**.

1. Select a **Performance Optimization** option.
In the **Multi-Queue** section of the page, interfaces that
 - Support Multi-Queue are shown. Other interfaces (Management, Synchronization and on board interfaces) do not show.
 - Are recommended for enabling Multi-Queue are selected. These are interfaces which are Up and have a link.
2. To change the settings, select or clear interfaces.
3. Click **Apply**.
4. Reboot.

To see the association of interfaces to cores, run the command:

- `sim affinity -l` for interfaces that are not configured with Multi-Queue.
- `cpmq get -v` for interfaces that are configured with Multi-Queue.

To learn about CoreXL and Multi-Queue, see the *R80.10 Performance Tuning Administration Guide* <http://downloads.checkpoint.com/dc/download.htm?ID=54765>.

Configuring Performance Optimization - CLI (cpconfig)

To configure CoreXL for performance optimization:

1. Run `cpconfig`
2. Select
(10) Configure Check Point CoreXL

You can see the total number of CPUs (cores) and edit the number of cores with enabled firewall instances.

The number of cores used by Performance Pack = The number of CPUs - The number of firewall instances.



Note - In the WebUI, this is equivalent to the **Performance Optimization** option **Custom**.

To configure Multi-Queue for performance optimization:

To see the association of interfaces to cores, run the command `sim affinity -l`.

To learn about CoreXL and Multi-Queue, see the *R80.10 Performance Tuning Administration Guide* <http://downloads.checkpoint.com/dc/download.htm?ID=54765>.

System Management

In This Section:

Time	86
Cloning Groups	90
SNMP	99
Job Scheduler	111
Mail Notification	114
Messages	115
Session	116
Core Dumps	117
System Configuration	119
System Logging	120
Network Access	123
Configuring the WebUI Web server	123
Host Access	125

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

Time

All Security Gateways, Security Management Servers and cluster members must synchronize their system clocks. This is important for these reasons:

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

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

- Network Time Protocol (NTP).
- Manually, using the WebUI or the CLI.

Network Time Protocol (NTP)

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

NTP runs as a background client program on a client computer. It sends periodic time requests to specified servers to synchronize the client computer clock. **Best Practice** - Configure more than one NTP server for redundancy.

Setting the Time and Date - WebUI

To set time and date automatically using NTP:

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

To set the system time and date:

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

To set the time zone:

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

Configuring NTP - CLI (ntp)

NTP

Description

Use this command to configure and troubleshoot the Network Time Protocol (NTP).

Syntax

To monitor and troubleshoot your NTP implementation:

```
show ntp active
show ntp current
show ntp servers
```

To add a new NTP server:

```
set ntp active [On|Off]
set ntp server primary VALUE version VALUE
set ntp server secondary VALUE version VALUE
```

To delete an NTP server:

```
delete ntp server <IP>
```

Parameters

Parameter	Description
active	Shows the active NTP server or Enables or disables NTP. Valid values are On or Off.
current	Shows the host name or IP address of the NTP server you are using now.
primary	Set the host name or IP address of the primary NTP server.
secondary	The host name or IP address of the secondary NTP server.
version	The version number of the NTP server (from 1 to 4).
server	Keyword that identifies the NTP server.

Example

```
show ntp servers
```

Output

IP Address	Type	Version
pool.ntp.org	Primary	4

Comments

Server-Specifies the host name or IP address of the time server from which your system synchronizes its clock. The specified time server does **not** synchronize to the local clock of your system.

Version-The version number Specifies which version of NTP to run. **Best Practice** - Check Point recommends that you run version 3.

Showing the Time & Date - CLI (clock)**Clock****Description**

Show current system date and time

Syntax

```
show clock
```

Parameters

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

Example

```
show clock
```

Output

Thu Oct 6 15:20:00 2011 IST

Setting the Date - CLI (date)

Date

Description

Set the system date.

Syntax

```
set date <date>
```

```
show date
```

Parameters

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

Example

```
set date 2012-08-10
```

Setting the Time - CLI (Time)

Time

Description

Set the system time in HH:MM:SS format.

Syntax

```
set time <time of day>
```

```
show time
```

Parameters

Parameter	Description
<time of day>	The current system time in HH:MM:SS format

Example

```
show time
```

output

```
12:03:54
```

Setting the Time Zone - CLI (timezone)

Time Zone

Description

Show and Set the system time zone.

Syntax

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

Note: The spaces before and after the '/' character are important.

```
show timezone
```

Parameters

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

Example

```
set timezone America / Detroit
```

Cloning Groups

A Cloning Group is a collection of Gaia gateways that synchronize their OS configurations and settings for a number of these shared features:

- SNMP
- Banner Messages
- Job Scheduler
- DNS
- System Logging
- Host Access Control
- Proxy Settings
- Host Address Assignment
- NTP
- Password Policy
- Time
- Network Access
- Display Format
- Mail Notification
- Inactivity Timeout
- Users and Roles
- Static Routes
- DHCP Relay
- IPv6 DHCP Relay
- BGP
- IGMP

- PIM
- Static Multicast Routes
- RIP
- RIPng
- OSPF
- IPv6 OSPF
- Route Aggregation
- Inbound Route Filters
- Route Redistribution
- Route Map
- Routing Options
- Policy Based Routing
- Scheduled Backups

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

You can:

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

Note - a VRRP Cluster has to be manually defined.

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

Configuring Cloning Groups - WebUI

Cloning Groups are configured from the gateway WebUI.

To create a new Cloning Group:

1. Open the Gaia gateway WebUI.
2. In **System Management > Cloning Group**, click **Start Cloning Group Creation Wizard**.
The **Cloning Group Creation Wizard** opens.
3. Select **Create a new Cloning Group**.
The **New Gaia Cloning Group** window opens.
 - Enter a name for the Cloning Group

- Select an IP address for synchronizing settings between member gateways. Select an address on a secure internal network.
 - Enter a password for the administration account (*cadmin*). This password is necessary to:
 - Manage the Cloning Group
 - Add other gateways to the Cloning Group
 - Create encrypted traffic between members of the Cloning Group
4. In the **Shared Features** screen, select features to clone to other members of the group.
Pay attention to which features you want to clone. For example, you might not want to clone static routes to gateways that are members of a cluster.
 5. Click **Next** for the **Wizard Summary** and then click **Finish**.

To manage the Cloning Group:

1. Sign out of the WebUI
2. Sign in *to the same WebUI* using the *cadmin* account and password.
(Alternatively, log in to the gateway command line using the *cadmin* credentials.)
Important - No unique URL or IP address is needed to access the Cloning Group WebUI or cli command line. Use the URL or IP address of the member 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 WebUI of each member are grayed out.

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

To manage a Cloning Group as an assigned administrator:

1. Open WebUI on a Cloning Group member gateway.
2. Click **Group Mode**.
The gateway switches to Cloning Group management mode.

To join a Cloning Group:

1. Open the Gaia gateway WebUI.
2. In **System Management > Cloning Group**, click **Start Cloning Group Creation Wizard**.
The **Cloning Group Wizard** opens.
3. Select **Join an existing Cloning Group**.
4. The **Join Existing Cloning Group** window opens.
 - Enter the IP address of a remote member of the Cloning Group.
 - Select an IP address for synchronizing the settings between gateways. Select a secure internal address.

- Enter the password of the Cloning Group administration account (*cadmin*). (The same password you entered when creating the group.) The cadmin password:
 - Lets you log in to the cadmin account
 - Is used to create authentication credentials for members during synchronization

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

To create a Cloning Group that follows ClusterXL:

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

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

1. Open the Gaia WebUI.
2. In **System Management > Cloning Group**, click **Start Cloning Group Creation Wizard**.
The **Cloning Group Creation Wizard** opens.
3. Select **Cloning Group follows ClusterXL**.
 - Enter the Cloning Group name.
 - Enter a password for the Cloning Group administration account (*cadmin*).
4. Click **Next** for the **Wizard Summary** and then click **Finish**.
5. Repeat steps 1-4 for all members of the cluster.

Configuring Cloning Groups - CLI (Cloning Groups)

Cloning Groups can also be managed in clish command line interface. When run from the cadmin account, these commands apply to all members of the group.

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

To create the first Cloning Group member in manual mode:

1. Set the cloning group mode to manual
2. Set the cloning group local-ip
3. Set the cloning group password
4. Set the cloning group state to: on
5. Optional: set a name for the Cloning Group

To add other gateways to the Cloning Group in manual mode:

On each of those gateways:

1. Set the cloning group mode to manual
2. Set the cloning group local ip
3. Set the cloning group password
4. Run the `join cloning group` command to join the group

To create Cloning Group members in ClusterXL mode:

On all member gateways:

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

To set up a Cloning Group:

Run this command: `set cloning-group {local-ip <IPv4_address> | mode <manual|cluster-xl> | name <Cloning Group_name> | password | state <on|off>}`

Parameter	Description
<code>local-ip <IPv4_address></code>	The IPv4 address used to synchronize shared features between members of the Cloning Group.
<code>mode <manual cluster-xl></code>	The mode determines whether the Cloning Group is manually defined or through ClusterXL.
<code>name <Cloning Group_name></code>	Name of the Cloning Group.
<code>password</code>	Password for the administrator's (cadmin) account, used to access the Cloning Group configuration in the CLI or WebUI. When prompted, enter and confirm the password.
<code>state on off</code>	Turns the Cloning Group feature on or off. If you select <code>off</code> , the gateway is removed from the Cloning Group.

To add Shared Features

Run this command: `add cloning-group shared-feature <feature>`

Parameter	Description
feature	The name of the feature to be synchronized between the members of the Cloning Group: • aggregate • bgp • bootp • cron • dns • hosts • igmp • inboundfilters • time • ntp • message • ospf • ospf3 • password-controls • mailrelay • display-format • http • net-access • users-and-roles • syslog • proxy • host-access • pbr • pim • redistribution • rip • routemap • routingoptions • static • static-mroute • snmp

To delete Shared Features

Run this command: `delete cloning-group shared feature <feature>`

Parameter	Description
feature	The name of the feature to be deleted from the list of shared features: • aggregate • bgp • bootp • cron • dns • hosts • igmp • inboundfilters • time • ntp • message • ospf • ospf3 • password-controls • mailrelay • display-format • http • net-access • users-and-roles • syslog • proxy • host-access • pbr • pim • redistribution • rip • routemap • routingoptions • static • static-mroute • snmp

To join a Cloning Group:

Run this command: `join cloning-group remote-ip <IPv4_address>`

Parameter	Description
IPv4_address	The IPv4 address of a member of the Cloning Group. Note - This option is not available if you are logged into the cadmin account.

To remove a member from a Cloning Group:

On the member gateway, run this command: `leave cloning-group`

To remove an inaccessible Cloning Group member:

Run this command: `delete cloning-group disconnected-member <member_IP>`

Parameter	Description
member_IP	The IPv4 address of the Cloning Group member that became inaccessible.

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



Notes -

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

To view Cloning Group Attributes:

Run this command: `show cloning-group {local-ip | members | mode | name | shared-feature | state | status}`

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

To re-synchronize a Cloning Group:

On a member gateway, run this command: `re-synch cloning-group`

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

To turn on the Cloning Group management mode:

Run this command: `set cloning-group-management <on|off>`

Parameter	Description
on off	on - Turns the Cloning Group management mode on off - Turns the Cloning Group management mode off

Creating Cloning Groups using the CLI

You can create Cloning Groups in manual mode and in ClusterXL mode.

To create the first Cloning Group member in manual mode:

1. Set the cloning group mode to manual
2. Set the cloning group local-ip
3. Set the cloning group password
4. Set the cloning group state to: on
5. Optional: set a name for the Cloning Group

To add other gateways to the Cloning Group in manual mode:

On each gateway:

1. Set the cloning group mode to manual
2. Set the cloning group local ip
3. Set the cloning group password
4. Run the `join cloning group` command to join the group

To create Cloning Group members in ClusterXL mode:

On all member gateways:

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

SNMP

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

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

To view detailed information about each MIB that the Check Point implementation supports:

MIB	Location
Standard MIBs	/usr/share/snmp/mibs
Check Point MIBs	\$CPDIR/lib/snmp
Check Point Gaia trap MIBs (GaiaTrapsMIB)	/etc/snmp

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



Warning - If you use SNMP, it is recommended that you change the community strings for security purposes. If you do not use SNMP, disable SNMP or the community strings.

SNMP, as implemented on Check Point platforms enables an SNMP manager to monitor the device using `GetRequest`, `GetNextRequest`, `GetBulkRequest`, and a select number of traps. The Check Point implementation also supports using `SetRequest` to change these attributes: `sysContact`, `sysLocation`, and `sysName`. You must configure read-write permissions for set operations to work.

SNMP on Check Point platforms, supports SNMP v1, v2, and v3.

Use Gaia to run these tasks:

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

V3 - User-Based Security Model (USM)

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

The system uses the MD5 hashing algorithm to supply authentication and integrity protection and DES to supply encryption (privacy). **Best Practice** - Use authentication and encryption. You can use them independently by specifying one or the other with your SNMP manager requests. The Gaia system responds accordingly.

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

Enabling SNMP

The SNMP daemon is disabled by default. If you choose to use SNMP, enable and configure it according to your security requirements. At minimum, you must change the default community string to something other than public. It is also advised to select SNMPv3, rather than the default v1/v2/v3, if your management station supports it.



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

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

SNMP Agent Address

An agent address is a specified IP address at 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 `GaiaTrapsMIB.mib` in the `/etc/snmp` directory.

Gaia supports these types of traps:

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.

Type of Trap	Description
configurationSave	Notifies when a permanent change to the system configuration occurs.
lowDiskSpace	Notifies when space on the system disk is low. This trap is sent if the disk space utilization in the / partition has reached 80 percent or more of its capacity.
powerSupplyFailure	Notifies when a power supply for the system fails. This trap is supported only on platforms with two power supplies installed and running.
fanFailure	Notifies when a CPU or chassis fan fails.
overTemperature	Notifies when the temperature rises above the threshold.
highVoltage	Notify if one of the voltage sensors exceeds its maximum value.
lowVoltage	Notify if one of the voltage sensors falls below its minimum value.
raidVolumeState	Notify if the raid volume state is not optimal. This trap works only if RAID is supported on the Gaia appliance or computer. To make sure that RAID monitoring is supported, run the command <code>raid_diagnostic</code> and confirm that it shows the RAID status.

Configuring SNMP - WebUI

To enable SNMP:

1. In the tree view, click **System Management > SNMP**.
2. Select **Enable SNMP Agent**.
3. In **Version** drop down list, select the version of SNMP to run:
 - **1/v2/v3 (any)**
Select this option if your management station does not support SNMPv3.
 - **v3-Only**
Select this option if your management station supports v3. SNMPv3 provides a higher level of security than v1 or v2.
4. In **SNMP Location String**, enter a string that contains the location for the system. The maximum length for the string is 128 characters. That includes letters, numbers, spaces, special characters. For example: **Bldg 1, Floor 3, WAN Lab, Fast Networks, Speedy, CA**
5. In **SNMP Contact String**, enter a string that contains the contact information for the device. The maximum length for the string is 128 characters. That includes letters, numbers, spaces,

special characters. For example: John Doe, Network Administrator, (111) 222-3333

6. Click **Apply**.

To set an SNMP agent interface (Version R77.10 and higher):

1. In the tree view, click **System Management > SNMP**.

The SNMP Addresses table shows the applicable interfaces and their IP addresses.

2. Select the header row checkbox to select all or select individual interfaces.



Note - If no agent addresses are specified, the SNMP protocol responds to requests from all interfaces.

To set an SNMP agent address (Version R77 and earlier):

1. In the tree view, click **System Management > SNMP**.

The SNMP Addresses table shows the applicable interfaces and their IPv4 addresses.

2. Select the header row checkbox to select all or select individual IPv4 addresses.



Note - If no agent addresses are specified, the SNMP protocol responds to requests from all interfaces.

To configure the community strings:

1. In the **V1/V2 Settings** section, in **Read Only Community String**, set a string other than **public**. This is a basic security precaution that you must always use.

2. [Optional]. Set a **Read-Write Community String**.



Warning - Set a read-write community string only if you have reason to enable set operations, and if your network is secure.

To add a USM user:

1. In the tree view, click **System Management > SNMP**.

2. Below V3 - User-Based Security Model (USM), click **Add**. The **Add New USM User** window opens.

3. In **User Name**, The range is 1 to 31 alphanumeric characters with no spaces, backslash, or colon characters. This can be the same as a user name for system access.

4. In **Security Level**, select from the drop down list:

- **authPriv**—The user has authentication and privacy pass phrases and can connect with privacy encryption.
- **authNoPriv**—The user has only an authentication pass phrase and can connect only without privacy encryption.

5. In User Permissions, select the privileges for the user:

- **Read-only**
- **Read-write**

6. In **Authentication Protocol**, select:

- **MD5**
- **SHA1**

The default is **MD5**.

7. In **Authentication Pass Phrase**, enter a password for the user that is between 8 and 128 characters in length.
8. In **Privacy Protocol**, select:
 - **DES**
 - **AES**
 The default is **DES**.
9. In **Privacy Pass Phrase**, enter a pass phrase that is between 8 and 128 characters in length. Used for protection against disclosure of SNMP message payloads.
10. Click **Save**. The new user shows in the table.

To delete a USM user

1. In the tree view, click **System Management > SNMP**.
2. Below V3 - User-Based Security Model (USM), select the user and click **Remove**. The **Deleting USM User Entry** window opens.
3. The window shows this message: **Are you sure you want to delete "username" entry?** Click **Yes**.

To edit a USM user:

1. In the tree view, click **System Management > SNMP**.
2. Below V3 - User-Based Security Model (USM), select the user and click **Edit**. The **Edit USM User** window opens.
3. In the window you can change the **Security Level**, **User Permissions**, the **Authentication Passphrase**, or the **Privacy Passphrase**.
4. Click **Save**.

To enable or disable trap types:

1. In the tree view, click **System Management > SNMP**.
2. In the **Enabled Traps** section, click **Set**. The **Add New Trap Receiver** window opens.
 - To enable a trap: Select from the **Disabled Traps** list, and click **Add>**
 - To disable a trap: Select from the **Enabled Traps** list, and click **Remove>**
3. Click **Save**.
4. Add a USM user. You must do this even if using SNMPv1 or SNMPv2. In **Trap User**, select an SNMP user.
5. In **Polling Frequency**, specify the number of seconds between polls.
6. Click **Apply**.

To configure trap receivers (management stations):

1. In the tree view, click **System Management > SNMP**.
2. In the **Trap Receivers Settings** section, click **Add**. The **Add New Trap Receiver** window opens.
3. In **IPv4 Address**, enter the IP address of a receiver.
4. In **Version**, Select the Trap SNMP Version for the trap receiver from the drop down menu.
5. In **Community String**, enter the community string for the specified receiver.
6. Click **Save**.

To edit trap receivers:

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

To delete trap receivers:

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

Configuring SNMP - CLI (snmp)

Description

Use These commands to configure SNMP

Syntax

Enable SNMP

Set Commands:

```
set snmp agent VALUE
set snmp agent-version VALUE
set snmp location VALUE
set snmp contact VALUE
```

Show Commands:

```
show snmp agent
show snmp agent-version
show snmp location
show snmp contact
```

Delete Commands:

```
delete snmp location
delete snmp contact
```

SNMP Agent

Add commands:

```
add snmp interface <IF_name>
add snmp address <IP_address>
```

Set Commands:

```
set snmp community VALUE read-only
set snmp community VALUE read-write
```

Show Commands:

```
show snmp address
```

```
show snmp community
```

Delete Commands:

```
delete snmp address VALUE
delete snmp community VALUE
```

v3 USM User Settings

Add Commands:

- `add snmp usm user VALUE security-level authNoPriv`

This opens an interactive dialog to enter a password and optionally an authentication protocol. You can use a hashed password or a non-hashed password.

These are all the `authNoPriv` commands:

```
add snmp usm user VALUE security-level authNoPriv auth-pass-phrase VALUE
add snmp usm user VALUE security-level authNoPriv auth-pass-phrase-hashed
VALUE
```

```
add snmp usm user VALUE security-level authNoPriv auth-pass-phrase VALUE
authentication-protocol VALUE
```

```
add snmp usm user VALUE security-level authNoPriv auth-pass-phrase-hashed
VALUE authentication-protocol VALUE
```

- `add snmp usm user VALUE security-level authPriv`

This opens an interactive dialog to enter an authentication password and a privacy password, and optionally a privacy protocol or a privacy protocol and an authentication protocol. You can use hashed passwords or non-hashed passwords.

These are all the `authPriv` commands:

```
add snmp usm user VALUE security-level authPriv auth-pass-phrase VALUE
privacy-pass-phrase VALUE
```

```
add snmp usm user VALUE security-level authPriv auth-pass-phrase-hashed
VALUE privacy-pass-phrase-hashed VALUE
```

```
add snmp usm user VALUE security-level authPriv auth-pass-phrase VALUE
privacy-pass-phrase VALUE privacy-protocol VALUE
```

```
add snmp usm user VALUE security-level authPriv auth-pass-phrase-hashed
VALUE privacy-pass-phrase-hashed VALUE privacy-protocol VALUE
```

```
add snmp usm user VALUE security-level authPriv auth-pass-phrase VALUE
privacy-pass-phrase VALUE privacy-protocol VALUE
authentication-protocol VALUE
```

```
add snmp usm user VALUE security-level authPriv auth-pass-phrase-hashed
VALUE privacy-pass-phrase-hashed VALUE privacy-protocol VALUE
authentication-protocol VALUE
```

Best Practice - For commands that include `auth-pass-phrase` or `privacy-pass-phrase` or both, use the hashed commands. Get the hashed password by running: `show configuration snmp`

Set Commands:

- `set snmp usm user VALUE security-level authNoPriv`

This opens an interactive dialog to enter a password and an optionally an authentication protocol.

These are all the authNoPriv commands:

```
set snmp usm user VALUE security-level authNoPriv
auth-pass-phrase VALUE
```

```
set snmp usm user VALUE security-level authNoPriv auth-pass-phrase VALUE
authentication-protocol VALUE
```

- `set snmp usm user VALUE security-level authPriv`

This opens an interactive dialog to enter an authentication password and a privacy password, and optionally a privacy protocol or a privacy protocol and an authentication protocol. You can use hashed passwords or non-hashed passwords.

These are all the authPriv commands:

```
set snmp usm user VALUE security-level authPriv auth-pass-phrase VALUE
privacy-pass-phrase VALUE
```

```
set snmp usm user VALUE security-level authPriv auth-pass-phrase VALUE
privacy-pass-phrase VALUE privacy-protocol VALUE
```

```
set snmp usm user VALUE security-level authPriv auth-pass-phrase VALUE
privacy-pass-phrase VALUE privacy-protocol VALUE
authentication-protocol VALUE
```

```
set snmp usm user VALUE usm-read-only
```

```
set snmp usm user VALUE usm-read-write
```

Show Commands:

```
show snmp usm user VALUE
show snmp usm users
```

Delete Commands:

```
delete snmp usm user VALUE
```

SNMP Traps

Add Commands:

```
add snmp traps receiver VALUE version v1 community VALUE
add snmp traps receiver VALUE version v2 community VALUE
add snmp traps receiver VALUE version v3
```

Set Commands:

```
set snmp traps receiver VALUE version v1 community VALUE
set snmp traps polling-frequency VALUE
set snmp traps receiver VALUE version v2 community VALUE
set snmp traps receiver VALUE version v3
set snmp traps trap VALUE disable
set snmp traps trap VALUE enable
set snmp traps trap-user VALUE
```

Show Commands:

```
show snmp traps enabled-traps
show snmp traps polling-frequency
show snmp traps receivers
show snmp traps trap-user
```

Delete Commands:

```
delete snmp traps polling-frequency
delete snmp traps receiver VALUE
delete snmp traps trap-user
```

Parameters

Parameter	Description
snmp agent	on or off to enable or disable.
snmp agent-version	any or v3-Only
location	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
contact	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
snmp address	For version R77 and earlier: Interface IP address. If you do not select one at which the SNMP Agent listens and responds to requests, it responds to requests from all interfaces.
snmp interface	For version R77.10 and higher: Interface name. If you do not select one at which the SNMP Agent listens and responds to requests, it responds to requests from all interfaces.
community <c_name> read-only	For SNMP v1 and v2 only. Enter a unique community name as a string value for read-only actions. The community name works like a password to identify and validate SNMP requests. The default community name is public . Best Practice - We recommend that you assign community names based on industry-standard password conventions.
community <c_name> read-write	For SNMP v1 and v2 only. Enter a unique community name as a string value for read-write actions. The community name works like a password to identify and validate SNMP requests. The default community name is public . Best Practice - We recommend that you assign community names based on industry-standard password conventions.
usm user	The range is 1 to 31 alphanumeric characters with no spaces, backslash, or colon characters. This can be the same as a user name for system access.
authNoPriv	The user has only an authentication pass phrase and can connect only without privacy encryption. A user is always created with read-only privilege. This can be changed using the command set snmp usm user <name> <usm-read-only / usm-read-write>

authPriv	The user has authentication and privacy pass phrases and can connect with privacy encryption. A user is always created with read-only privilege. This can be changed using the command <code>set snmp usm user <name> <usm-read-only / usm-read-write></code>
auth-pass-phrase	A password for the user that is between 8 and 128 characters in length.
auth-pass-phrase-hashed	A hashed password which is the output of the command <code>show configuration snmp</code>
privacy-pass-phrase	A pass phrase that is between 8 and 128 characters in length. Used for protection against disclosure of SNMP message payloads.
privacy-pass-phrase-hashed	A hashed password which is the output of the command <code>show configuration snmp</code>
usm users	All USM users
traps receiver	IP address selected to receive traps sent by the agent.
community	Set a string
traps trap	The trap name
polling-frequency	The polling frequency in seconds. Default is 20 seconds.
trap-user	The user which generates the traps.

Example

```
show snmp traps enabled-traps
```

Output

```
authorizationError
```

Comments

- CLI only displays the enabled traps. For all trap types, see table in Configuring SNMP - WebUI (on page 102)Example.
- In auth-pass-phrase and privacy-pass-phrase, notice the different options for regular and hashed pass phrase:
auth-pass-phrase and auth-pass-phrase-hashed
privacy-pass-phrase and privacy-pass-phrase-hashed

Interpreting Error Messages

This section lists and explains certain common error status values that can appear in SNMP messages. Within the PDU, the third field can include an error-status integer that refers to a specific problem. The integer zero (0) means that no errors were detected. When the error field is anything other than 0, the next field includes an error-index value that identifies the variable, or object, in the variable-bindings list that caused the error.

The following 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 displays and logs the appropriate message.

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

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

Variable-bindings element	Description
<code>value</code>	Value that is associated with each object instance; 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 referred to 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 a `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 use WebUI to access cron and schedule regular jobs. You can configure the jobs to run at the dates and times that you specify, or at startup.

Configuring Job Scheduler - WebUI

To schedule jobs:

1. In the tree view, click **System Management > Job Scheduler**.
2. Click **Add**. The **Add A New Scheduled Job** window opens.
3. In **Job Name**, enter the name of the job. Use alphanumeric characters only, and no spaces.
4. In **command to Run**, enter the name of the command. The command must be a UNIX command.
5. Below **Schedule**, select the frequency (**Daily, Weekly, Monthly, At startup**) for this job. Where relevant, enter the **Time** of day for the job, in the 24 hour clock format.
6. Click **OK**. The job shows in the Scheduled Jobs table.
7. In **E-mail Notification**, enter the email to receive the notifications.



Note - You must also configure a Mail Server ("[Configuring Mail Notification - WebUI](#)" on page 114).

8. Click **Apply**.

To delete scheduled jobs

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

To edit the scheduled jobs:

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

Configuring Job Scheduler - CLI (cron)

Description

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

You can define an email address to which the output of the scheduled job will be sent.

Syntax

To add scheduled jobs:

```
add cron job VALUE command VALUE recurrence daily time VALUE
add cron job VALUE command VALUE recurrence monthly month VALUE days VALUE time VALUE
add cron job VALUE command VALUE recurrence weekly days VALUE time VALUE
add cron job VALUE command VALUE recurrence system-startup
```

To delete scheduled jobs:

```
delete cron all
delete cron job VALUE
delete cron mailto
```

To change existing scheduled jobs:

```
set cron job VALUE command VALUE
set cron job VALUE recurrence daily time VALUE
set cron job VALUE recurrence monthly month VALUE days VALUE time VALUE
set cron job VALUE recurrence weekly days VALUE time VALUE
set cron job VALUE recurrence system-startup
set cron mailto VALUE
```

To monitor and troubleshoot the job scheduler configuration:

```
show cron job VALUE command
show cron job VALUE recurrence
show cron jobs
show cron mailto
```

Parameters

Parameter	Description
job	The name of the job.
command	The name of the command.
recurrence daily time	To specify a job for once a day, enter recurrence daily time, and the time of day, in the 24 hour clock format. For example: 14:00.
recurrence monthly month	To specify a job for once a month, enter recurrence monthly month, and the specific months. Each month by number, and separate by commas. For example: for January through March, enter 1,2,3
recurrence weekly days	To specify a job for once a week, enter recurrence weekly, and the day by number, when 0 is Sunday and 6 is Saturday.
recurrence system-startup	Specify a job that will run at every system startup.
days	When the recurrence is weekly: To specify the days, enter the day by number: 0 is Sunday and 6 is Saturday. When the recurrence is monthly: To specify the days, enter the day by number: 1 to 31. Separate several days with commas. For example: for Monday and Thursday enter 1,4
time	To specify the time, enter the time in the twenty four hour clock format. For example: 14:00.
mailto	To specify a mail recipient, enter the email address. One email address per command. You must also configure a mail server (" Configuring Mail Notification - CLI (mail-notification) " on page 114).

Comments

Only Show commands provide an output.

Mail Notification

Mail notifications (also known as Mail Relay) allow you to send email from the Security Gateway. You can send email interactively or from a script. The email is relayed to a mail hub that sends the email to the final recipient.

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

Gaia supports these mail notification features:

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

Gaia does not support these mail notification features:

- Incoming email.
- Mail transfer protocols other than outbound SMTP.
- Telnet to port 25.
- Email accounts other than admin or monitor.

Configuring Mail Notification - WebUI

To configure mail notifications recipient:

1. In the tree view, click **System Management** > **Mail Notification**.
2. In The **Mail Server** field, enter the server. For example: mail.example.com
3. In the **User Name** field, enter the user name. For example: user@mail.example.com
4. Click **Apply**.

Configuring Mail Notification - CLI (mail-notification)

Description

Use this group of commands to configure mail notifications.

Syntax

To configure the mail server and user that receive the mail notifications:

```
set mail-notification server VALUE
set mail-notification username VALUE
```

To view the mail server and user configurations:

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

Parameters

Parameter	Description
server	The IP address or hostname of the mail server to receive mail notifications. For example: mail.company.com
username	The username on the mail server that receives the admin or monitor mail notifications. For example: user@mail.company.com

Example

```
show mail-notification server
```

Output

```
Mail notification server: mail.company.com
```

Messages

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

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

Configuring Messages - WebUI

To configure messages:

1. In the tree view, 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 messages.
5. Click **Apply**.

Configuring Messages - CLI (message)

Description

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

Syntax and Examples

To define a new banner message or message of the day:

```
set message banner <on|off> msgvalue <banner>
set message motd <on|off> msgvalue <message>
```

Examples:

```
set message banner on msgvalue "This system is private and confidential"
set message motd on msgvalue "Hi all- no changes allowed today"
```

To enable or disable the banner message:

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

To enable or disable the message of the day:

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

To show the messages:

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

To show if the messages are enabled or disabled:

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

To delete the messages:

The `delete` command deletes the user defined message, not the default message. To prevent a message being shown, turn off the message.

1. Delete the configured message

```
delete message banner
delete message motd
```

This deletes the configured messages, and replace them with the default messages.

2. Disable the default messages:

```
set message banner off
set message motd off
```

To make multi-line banner message or message of the day:

You can add a line to an existing message. If you delete the message, all lines are deleted, and replaced with the default message. To add a line to an existing message:

```
set message banner on line msgvalue <message>
set message motd on line msgvalue <message>
```

Examples:

```
set message banner on line msgvalue Welcome
set message motd on line msgvalue "System maintenance today"
```

Session

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

Configuring the Session - WebUI

1. In the tree view, click **System Management > Session**.
2. Configure the **Inactivity Timeout** for the **Command Line Shell**.
3. Configure the **Inactivity Timeout** for the **WebUI**.

Configuring the Session - CLI (inactivity-timeout)

Description

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

Syntax

```
set inactivity-timeout VALUE
show inactivity-timeout
```

Parameters

Parameter	Description
inactivity-timeout	The inactivity timeout (in minutes) for the command line.

Core Dumps

A Gaia core dump consists of the recorded status of the working memory of the Gaia computer at the time that a Gaia process terminated abnormally.

When a process terminates abnormally, it produces a core file in the `/var/log/dump/usermode` directory.

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

Configuring Core Dumps - WebUI

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

To configure core dumps:

1. Open the **System Management > Core Dumps** page.
2. Configure the Core Dump parameters.
3. Click **Apply**.

Core Dump Parameters

Parameter	Description
Total space limit	The maximum amount of space that is used for core dumps. If space is required for a dump, the oldest dump is deleted. The per-process limit is enforced before the space limit. • Range: 1-99999 MB • Default: 1000 MB
Dumps per process	The maximum number of dumps that are stored for each process executable (program) file. A new dump overwrites the oldest dump. For example, if there are two programs "A" and "B", and the per-process limit is limit is 2. "A" terminates 1 time and "B" terminates 3 times. The dumps that remain are: 1 dump for program "A", and 2 dumps for program "B". Dump 3 for "B" is deleted because of the per-process limit. The per-process limit is enforced before the space limit. • Range: 1-99999 • Default: 2

Configuring Core Dumps -CLI (core-dump)

Description

Configure Gaia core dumps.

Syntax

To enable or disable core dumps:

```
set core-dump enable
set core-dump disable
```

To set the total space usage limit:

```
set core-dump total VALUE
```

To set the number of dumps per process:

```
set core-dump per_process VALUE
```

To show the total space usage limit:

```
show core-dump total
```

To show the number of dumps per process:

```
show core-dump per_process
```

Parameters

Parameter	Description
total VALUE	- The maximum amount of space that is used for core dumps. If space is required for a dump, the oldest dump is deleted. The per-process limit is enforced before the space limit. - Range: 1-99999 MB - Default: 1000 MB
per_process VALUE	- The maximum number of dumps that are stored for each process executable (program) file. A new dump overwrites the oldest dump. For example, if there are two programs "A" and "B", and the per-process limit is limit is 2. "A" terminates 1 time and "B" terminates 3 times. The dumps that remain are: 1 dump for program "A", and 2 dumps for program "B". Dump 3 for "B" is deleted because of the per-process limit. The per-process limit is enforced before the space limit. - Range: 1-99999 - Default: 2

System Configuration

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

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

Configuring IPv6 Support - WebUI

1. In the WebUI tree view, click **System Management > System Configuration**.
2. In the **IPv6 Support** area, click **On**.
3. Click **Apply**.

Configuring IPv6 Support - CLI

The IPv6-state feature configures IPv6 support.

Description

Use this command to enable or disable IPv6 support.

Syntax

```
set ipv6-state off
set ipv6-state on
show ipv6-state
```

Parameters

Parameter	Description
on off	Turns IPv6 support on or off.

System Logging

Configure the settings for the system logs, including sending them to a remote server. Make sure to configure the remote server to receive the system logs.

Configuring System Logging - WebUI

This section includes procedures for configuring system logging to remote servers using the WebUI.

To send system logs using the WebUI:

1. In the tree view, click **System Management > System Logging**.
2. Click **Add**.
The **Add Remote Server Logging Entry** window opens.
3. In **IP Address**, enter the IP address of the remote server.
4. In **Priority**, select the severity level of the logs that are sent to the remote server.
5. Click **OK**.

To edit system logging settings using the WebUI:

1. In the tree view, click **System Management > System Logging**.
2. Select the IP address of the remote server.
3. Click **Edit**.
The **Edit Remote Server Logging Entry** window opens.
4. Configure the **IP Address** and **Priority** settings.
5. Click **OK**.

To stop sending system logs using the WebUI:

1. In the tree view, click **System Management > System Logging**.
2. Select the IP address of the remote server.
3. Click **Delete**.
A confirmation window opens.
4. Click **Yes**.

Configuring System Logging - CLI (syslog)

Description

Configures system logging settings.

Syntax

To send system logs to a remote server:

```
add syslog log-remote-address <remote ip> level <severity>
```

To stop sending system logs to a remote server:

```
delete syslog log-remote-address <remote ip> level <severity>
```

To configure the file name of the system log:

```
set syslog filename <file>
```

To show the system logging settings:

```
show syslog all
      filename
      log-remote-addresses
```

Parameters

Parameter	Description
syslog	Configures the system logging.
log-remote-address	Configures remote IP address for system logging.
level	Filters a severity level for the system logging.
filename	Configures or shows the file name of the system log.
<remote ip>	IP address of remote computer.
<severity>	syslog severity level. These are the legal values: • emerg • alert • crit • err • warning • notice • info • debug • all
<file>	System log file name.

Example

```
add syslog log-remote-address 192.0.2.1 level all
set syslog filename system_logs
show syslog filename
```

Comments

There are some command options and parameters that you cannot do using the WebUI.

Configuring Log Volume - CLI (volume)

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



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

To show log partition usage, run:

Syntax

```
show volume logs
```

Output

```
Logical volume (logs) size:3.00GB, free:2.82GB
Free space for future backup images: 15.84GB
```

To enlarge the log partition, run:

Syntax

```
set volume VALUE size VALUE
```

Example

```
set volume logs size 4
```

Output

Prior to adding new storage to the file system, it is recommended to backup the system.

Note that during the process, all Check Point products will be shutdown.

```
Are you sure you want to continue?(Y/N)[N]
```

```
y
```

```
This operation may take several minutes...
```

Comments

- The new size for the logical volume is set in GB. In the above example, the volume will be resized from 3GB to 4GB.
- The new size must be a whole number.
- If the size of the new volume subtracts too much space from the space used to store backup images, this message shows: "The logical volume new size is out of range, should be smaller than <number> GB."
The system always reserves 6GB for backup images. This 6GB cannot be used to increase log volume. If necessary, enter a smaller number.
- The volume will be resized after the system reboots.

Redirecting Routed System Logging Messages

By default, Gaia sends the Routed syslog messages (for example, OSPF or BGP errors) to the /var/log/messages file. You can configure Gaia to send the Routed syslog messages to the /var/log/routed_messages file instead.

To redirect the Routed syslog messages using the WebUI:

1. Go to **Advanced Routing > Routing Options**.
2. Enable **Log Routed Separately**.

To redirect the RouteD syslog messages using clish:

1. Log in to Clish.
2. Run these commands:


```
HostName> set routedsyslog on
HostName> set routedsyslog maxnum <Number of files between 1 and 4294967295>
HostName> set routedsyslog size <Number of MB between 1 and 2047>
HostName> save config
```

For more information on the configurations in the WebUI and clish, see sk116436

<http://supportcontent.checkpoint.com/solutions?id=sk116436>.

Network Access

Telnet is not recommended for remote login because it is not secure. SSH, for example, provides much of the functionality of Telnet with good security. Network access to Gaia using Telnet is disabled by default. However, you can allow Telnet access.

Configuring Telnet Access - WebUI

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

Configuring Telnet Access - CLI (net-access)

Description

Allow or disallow network access using Telnet to the Gaia computer

Syntax

To allow or disallow Telnet access:

```
set net-access telnet on
set net-access telnet off
```

To show if Telnet access is allowed or disallowed:

```
show net-access telnet
```

Configuring the WebUI Web server

You can configure the server responsible for the Gaia WebUI using the web feature. The web feature consists of these commands:

- set web daemon-enable VALUE
- set web session-timeout VALUE
- set web ssl-port VALUE

- `show web daemon-enable`
- `show web session-timeout`
- `show web ssl-port`

Enabling the web daemon

Use this command to enable the web daemon:

Syntax `set web daemon-enable on | off`

Parameters

Parameter	Description
<code>daemon-enable VALUE</code>	on or off

Setting a web-session timeout

Use this command to define the time (in minutes) after which the HTTP session terminates.

Syntax `set web session-timeout VALUE`

Parameter	Description
<code>session-timeout VALUE</code>	The value entered here defines the amount of time after which the web server will terminate a HTTP session with the WebUI. Range: Integers between 1 and 1440 inclusive. Default: 20

Setting an SSL port

Use this command to define a port for SSL

Description Specifies the port number on which the WebUI can be accessed when using SSL-secured connections

Syntax `set web ssl-port VALUE`

Parameters

Parameter	Description
<code>ssl-port VALUE</code>	Integers between 1 and 65535 inclusive. Default: "443".

Comments 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.

Note: This setting does not affect non-SSL connections. Normally this should be left at 443. If you change the port number you will have to change the URL used to access the WebUI: from `https://hostname/` to `https://hostname:PORTNUMBER/`

Showing the state of the web daemon

Description	Use this command to show the state of the web daemon
Syntax	<code>show web daemon-enable</code>
Output	<pre>gw-gaia> show web daemon-enable WebDaemonEnable on</pre>

Showing the web session-timeout

Description	Use this command to show the state of the web session time-out
Syntax	<code>show web session-timeout</code>
Output	<pre>gw-gaia> show web session-timeout WebSessionTimeout 99</pre>

Showing the web SSL-port

Description	Use this command to show the web SSL-port
Syntax	<code>show web ssl-port</code>
Output	<pre>gw-gaia> show web ssl-port web-ssl-port 443</pre>

Host Access

The Allowed-Clients feature lets you specify hosts or networks that are allowed to connect to the WebUI or Command Line interface of the Gaia device.

Configuring Allowed Gaia Clients - WebUI

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

Configuring Allowed Gaia Clients - CLI (allowed-client)

Description

Use this command to configure remote access to the Gaia WebUI or CLI.

Syntax

```
add allowed-client host any-host
add allowed-client host ipv4-address VALUE
add allowed-client network ipv4-address VALUE mask-length VALUE
delete allowed-client host any-host
delete allowed-client host ipv4-address VALUE
delete allowed-client network ipv4-address VALUE
show allowed-client all
```

Parameters

Parameter	Description
ipv4-address VALUE	The IPv4 address of the allowed host
mask-length VALUE	The mask-length of the allowed network

Example

```
add allowed-client host any-host
```

Output

```
gw-gaia> add allowed-client host any-host
gw-gaia> show allowed-client all
Type          Address          Mask Length
```

Advanced Routing

Dynamic Routing is fully integrated into the Gaia WebUI and command-line shell. BGP, OSPF and RIP are supported.

Dynamic Multicast Routing is supported, with PIM (Sparse Mode (SM), Dense Mode (DM), Source-Specific Multicast (SSM), and IGMP.

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

User Management

In This Section:

Change My Password	128
Users	129
Roles	133
Password Policy	137
Authentication Servers	146
System Groups	156
GUI Clients	157

This chapter describes how to manage passwords, user accounts, roles, authentication servers, system groups, and Gaia WebUI clients.



Note - When a user logs in to Gaia, the WebUI navigation tree displayed and CLI 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 WebUI navigation tree or in the list of commands. If the user has read-only access to a feature, they can see the WebUI 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.

Change My Password - WebUI

To change your current user password:

1. In the tree view, click **User Management > Change My Password**.
2. In **Old Password**, enter your old password.
3. In **New Password** and in **Confirm New Password**, enter the new Password.
4. Click **Apply**.

Change My Password - CLI (selfpasswd)

Description

Change your own Gaia password, in an interactive dialog.

Syntax

`set selfpasswd`

Warning

It is not recommended to use
`set selfpasswd oldpass VALUE passwd VALUE`
 because the passwords are stored as plain text in the `command history`. Instead, use `set selfpasswd`

Users

Use the WebUI and CLI to manage user accounts. You can:

- Add users to your Gaia system.
- Edit the home directory of the user.
- Edit the default shell for a user.
- Give a password to a user.
- Give privileges to users.

These users are created by default and cannot be deleted:

- **admin** — Has full read/write capabilities for all Gaia features, from the WebUI and the CLI. 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 WebUI and the CLI, 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 WebUI and CLI by default. You must assign one or more roles before they can log in.



Note - 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 CLI), the user is equivalent to the Admin user and the roles assigned to that account cannot be modified.



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.

When you create a user you can add pre-defined roles (privileges) to the user. For more information, see "Role-Based Administration" ("[Roles](#)" on page [133](#)).



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 - WebUI

To see a list of all users

Choose **User Management > Users** in the navigation tree.

You can also see your username in the toolbar of the WebUI.

To add a user

1. Open the **User Management > Users** page.
2. Click **Add**
3. In the **Add User** page, enter the following:
 - **Login Name** - (1–31 characters),
 - **Home Directory** - for the new user. Must be subdirectory of /home
 - **Password**.
 - **Confirm Password**
4. Click **OK**

To delete a user

1. Open the **User Management > Users** page.
2. Select the User
3. Click **Delete**.

User Account Fields- WebUI

Item	Description
Login Name	Name used to identify the user. The valid characters are alphanumeric characters, dash (-), and underscore (_). Range: 1-32 characters
Real Name	User's real name or other informative label.
Home directory	This is the full Linux path name of a directory where the user will log in. The home directory for all users must be in /home.
Shell	• <code>/etc/cli.sh</code> - User can use the full Gaia CLI (clish). This is the default option. By default, some basic networking commands (such as ping) are also available. The <i>Extended Commands mechanism</i> makes it possible to add Linux commands that can be used. User can run <code>shell</code> to enter the bash shell. • <code>/bin/bash</code>, <code>/bin/csh</code>, <code>/bin/sh</code>, <code>/bin/tcsh</code> - Standard Linux shells. User can run <code>clish</code> to enter the clish shell. • <code>/usr/bin/scponly</code> - User can log in only with SCP, and transfer files to and from the system. No other commands are permitted. • <code>/sbin/nologin</code> - User is not allowed to log in.
Password	Use this field to enter a new password if you are changing it. Range: 6-128 characters. All printable characters are allowed. Note - If you use an asterisk (*) in a password, users with that password are unable to log in.

Item	Description
Reset Password	Change the user password. Important - After resetting the password, tell the user to immediately change their password in User Management > Change My Password .
Confirm Password	Re-enter the new password if you are changing it.
User must change password at next logon	Important - After selecting this option, tell the user to immediately change their password in User Management > Change My Password .
Access Mechanisms	Choose whether the user is able to access Gaia from the command line, from the WebUI, both, or neither.
Roles	Assign a role to the user. Define the roles in User Management > Roles .

Managing User Accounts - CLI (user)

Description

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

Syntax

To add a user account:

```
add user <username> uid <user_ID> homedir <dir>
```

To modify a user account:

```
set user <username> {force-password-change {1 | on | t | true | y | yes | 0  
| off | f | false | n | no} | gid <group_ID> | homedir <dir> | lock-out off  
| newpass <passwd> | password | password-hash <hash> | realname <name> | shell  
<login_sh> | uid <user_ID>}
```

To delete an existing user:

```
delete user <user_ID>
```

To view summary information about all users:

```
show users
```

To view information about a user

```
show user <username> [force-password-change {1 | on | t | true | y | yes |
0 | off | f | false | n | no} | gid <group_ID> | homedir <dir> | lock-out off
| realname <name> | shell <login_sh> | uid <user_ID>
```

Parameters

Parameter	Description
user <username>	Unique login username - an alphanumeric string, 1 to 32 characters long, that can contain dashes (-) and underscores (_), but not spaces.
force-password-change {yes no}	If set to yes, forces the user to change their password on the next login.
gid <group_ID>	Numeric ID (0-65535) for the primary group to which a user belongs. The default is 100. Use the group management commands to specify membership in other groups.
homedir <dir>	User's home directory, where the user is placed on login. Enter the full Linux path name, under /home/ directory, and without colon (:). If the directory does not already exist, it is created.
lock-out off	Unlock the user, if the user was locked-out. The password expiration date is adjusted, if necessary.
newpass <passwd>	Set a new password for the user. You will not be asked to verify the new password. The password you enter shows on the terminal command line in plain text and is also stored in the command history as plain text.
password	Set a password for the new user. The command runs in interactive mode. You must enter the password twice, to verify it. The password you enter will not be visible on the terminal command line.
password-hash <hash>	An encrypted representation of the password. The password is not visible as text on the terminal command line or in the command history. Use this option if you want to change passwords using a script. You can generate the hash version of the password using standard Linux hash generating utilities.
realname <name>	User description, most commonly user's real name - an alphanumeric string that can contain spaces. The default is the username with capitalized first letter.

Parameter	Description
<code>shell <login_sh></code>	User's command interpreter (shell), which is invoked when the user logs in. The default shell is <code>/etc/cli.sh</code> and lets the user use the full Gaia CLI (clish). By default, some basic networking commands (such as ping) are also available. The Extended Commands mechanism makes it possible to use Linux commands. <code>/bin/bash</code>, <code>/bin/csh</code>, <code>/bin/sh</code>, <code>/bin/tcsh</code> - Standard Linux shells. To switch to the clish shell, the user has to run the command <code>clish</code>. <code>/usr/bin/scponly</code> - User is allowed to log in only using SCP, and to transfer files to and from the system. No other commands are allowed. <code>/sbin/nologin</code> - User is not allowed to log in.
<code>uid <user_ID></code>	Unique user ID (Integer 0-65535), to identify permissions of the user. This parameter is optional. If a value is not specified, a sequential number is assigned automatically.

Comments

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

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 (WebUI or the CLI) are available to the user.



Note - When users log in to the WebUI, they see only those features that they have read-only or read/write access to. If they have read-only access to a feature, they can see the settings pages, but cannot change the settings.

Gaia includes these predefined roles:

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

You cannot delete or change the predefined roles.



Note - Do not define a new user for external users. An external user is one that is defined on an authentication server (such as RADIUS or TACACS) and not on the local Gaia system.

Configuring Roles - WebUI

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

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

To add new role or change an existing role:

1. Select **User Management > Roles** in the WebUI navigation tree.
2. To add a new role, click **Add** and enter a **Role Name**. The role name can be a combination of letters, numbers and the underscore (`_`) character, but must start with a letter.
3. To change permissions for an existing role, double-click the role.
4. In the **Add** or **Edit Role** window, click a feature (**Features** tab) or extended command (**Extended Commands** tab).
5. Select **None**, **Read Only** or **Read/Write** from the options menu.



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.

To delete a role:

1. Select **User Management > Roles** in the navigation tree.
2. Select a role to delete.
3. Click **Delete**.



Note - You cannot delete the **adminRole**, or **monitorRole** default roles.

You can assign many users to a role from the **Roles** window.

To assign users to a role:

1. Select **User Management > Roles** in the WebUI navigation tree.
2. Click **Assign Members**.
3. In the **Assign Members to Role** window:
 - a) Double-click a user in the **Available Users** list to add that user to the role.
 - b) Double-click a user in the **Users with Role** list to remove that user from the role.

You can assign the many roles to a user from the **Users** page. You must work with the **Users** page to define access mechanism permissions (Web and/or command line) for users. A

To assign roles and access mechanisms to a user:

1. Select **User Management > Users** in the WebUI navigation tree.
2. Double-click a user in the list.
3. In the **Edit User** window:
 - Double-click a role in the **Available Roles** list to assign that role to the user.
 - Double-click a role in the **Assigned Roles** list to remove that role from the user.
 - Select an **Access Mechanisms** permission (**Web** or **Command Line**) to let the user to work with it.
 - Clear an **Access Mechanisms** permission (**Web** or **Command Line**) to prevent the user from working with it.

Configuring Roles - CLI (rba)

Description

1. Add, change or delete role definitions.
2. Add or remove users to or from existing roles.
3. Add or remove access mechanism (WebUI or CLI) permissions for a specified user.

Syntax

```
add rba role <Name> domain-type System
    readonly-features <List>
    readwrite-features <List>
```

```
add rba user <User name> access-mechanisms [Web-UI | CLI]
add rba user <User Name> roles <List>
```

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

```
delete rba role <Name>
    readonly-features <List>
    readwrite-features <L
```

```
delete rba user <User Name> access-mechanisms [Web-UI | CLI]
delete rba user <User Name> roles <List>
```

Parameters

Parameter	Description
Role <Name>	Role name as a character string that contains letters, numbers or the underscore (_) character. The role name must with a letter.
Domain-type System	Reserved for future use.
readonly-fea tures <List>	Comma separated list of Gaia features that have read only permissions in the specified role. You can add read only and read write feature lists in the same command.
readwrite-fe atures <List>	Comma separated list of Gaia features that have read/write permissions in the specified role. You can add read only and read write feature lists in the same command.
user <User name>	User to which access mechanism permissions and roles are assigned.
roles <List>	Comma separated list of role names that are assigned to or removed from the specified user.
access-mecha nisms	Defines the access mechanisms that users can work with to manage Gaia. You can only specify one access mechanism at a time with this command.

Examples

```
add rba role NewRole domain-type System readonly-features
vpn,ospf,rba readwrite-features tag,
```

```
add rba user Paul access-mechanisms CLI,WebUI
add rba user Daly roles NewRole,adminRole
delete rba role NewRole
delete rba user Daly roles adminRole
```

Comments

- There is no set operation for this command.
- Use the `add` or `delete` operations to add and remove features from an existing role.
- Use `delete rba role` to delete an role.

CLI Procedures

To define a new role or add features to an existing role:

Run:

```
add rba role <Name> domain-type System readonly-features <List>
readwrite-features <List>
```

- `role <Name>` - Role name as a character string that contains letters, numbers or the underscore (`_`) character. The role name must with a letter.
- `readonly-features <List>` - Comma separated list of Gaia features that have read only permissions in the specified role.
- `readwrite-features <List>` - Comma separated list of Gaia features that have read/write permissions in the specified role.

To remove features from an existing role:

Run:

```
delete rba role <Name> readonly-features <List> readwrite-features <List>
```

- `role <Name>` - Role name as a character string that contains letters, numbers or the underscore (`_`) character. The role name must with a letter.
- `readonly-features <List>` - Comma separated list of Gaia features that have read only permissions in the specified role.
- `readwrite-features <List>` - Comma separated list of Gaia features that have read/write permissions in the specified role.

To assign or remove roles to a user:

Run:

```
add rba user <User Name> roles <List>
delete rba user <User Name> roles <List>
```

- `user <User name>` - User to which access mechanism permissions and roles are assigned.
- `roles <List>` - Comma separated list of role names that are assigned to or removed from the specified user.

To Assign or remove access mechanisms (WebUI or CLI) for a user:

Run:

```
add rba user <User name> access-mechanisms [Web-UI | CLI]
```

```
delete rba user <User Name> access-mechanisms [Web-UI | CLI]
```

- **user <User name>** - Comma separated list of role names that are assigned to or removed from the specified user.
- **Web-UI** - Add or remove permissions to use the WebUI.
- **CLI** - Add or remove permissions to use the Gaia CLI.

Password Policy

This section explains how to configure your platform to:

- Enforce creation of strong passwords.
- Monitor and prevent use of already used passwords.
- Force users to change passwords at regular intervals.

One of the important elements of securing your Check Point cyber security platform is to set user passwords and create a good *password policy*.

Note - The password policy does not apply to nonlocal users that authentication servers such as RADIUS manage their login information and passwords. Also, it does not apply to non-password authentication, such as the public key authentication supported by SSH.

To set and change user passwords, see Users and Change My Password (on page 128).

Password Strength

Strong, unique passwords that use a variety of character types and require password changes, are key factors in your overall cyber security.

Password History Checks

The *password history* feature prevents from users using a password they have used before when they change their password. The number of already used passwords that this feature checks against is defined by the *history length*. Password history check is enabled by default.

The password history check

- Applies to user passwords set by the administrator and to passwords set by the user.
- Does not apply to SNMPv3 USM user pass phrases.

These are some considerations when using password history:

- The password history for a user is updated only when the user successfully changes password. If you change the history length, for example: from ten to five, the stored passwords number does not change. Next time the user changes password, the new password is examined against all stored passwords, maybe more than five. After the password change succeeds, the password file is updated to keep only the five most recent passwords.
- Passwords history is only stored if the password history feature is enabled when the password is created.
- The new password is checked against the previous password, even if the previous password is not stored in the password history.

Mandatory Password Change

The *mandatory password change* feature requires users to use a new password at defined intervals.

Forcing users to change passwords regularly is important for a strong security policy. You can set user passwords to expire after a specified number of days. When a password expires, the user is forced to change the password the next time the user logs in. This feature works together with the password history check to get users to use new passwords at regular intervals.

The mandatory password change feature does not apply to SNMPv3 USM user pass phrases.

Deny Access to Unused Accounts

You can deny access to unused accounts. If there has been no successful login attempt in a set period of time, the user is locked out and cannot log in. You can also configure the allowed number of days of non-use before a user is locked-out.

Deny Access After Failed Login Attempts

You can deny access after too many failed login attempts. The user cannot log in for a configurable period of time. You can also allow access again after a user has been locked out. Also, 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- WebUI

1. In the tree view, click **User Management > Password policy**.
2. Configure the password policy options:
 - **Password Strength** (on page 138)
 - **Password History** (on page 139)
 - **Mandatory Password change** (on page 139)
 - **Deny Access to Unused Accounts** (on page 140)
 - **Deny Access After Failed Login Attempts** (on page 140)
3. Click **Apply**.

Password Strength

Parameter	Description
Minimum Password Length	The minimum number of characters in a user or an SNMP user password. Does not apply to passwords that were already set. • Range: 6-128 • Default: 6
Disallow Palindromes	A palindrome is a sequence of letters, numbers, or characters that can be read the same in each direction. • Default: Selected

Password Complexity	The required number of character types. Character types are: Upper case alphabetic (A-Z), Lower case alphabetic (a-z), Digits (0-9), Other (everything else). A value of "1" disables this check. Changes to this setting do not affect existing passwords. • Range: 1-4 • Default: 2
----------------------------	---

Password History

Parameter	Description
Check for Password Reuse	Check for reuse of passwords. 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. Enables or disables password history checking and password history recording, for all users. • Default: Selected.
History Length	The number of former passwords to keep and check against for each user. • Range: 1-1000. • Default: 10.

Mandatory Password Change

Parameter	Description
Password Expiration	The number of days for which a password is valid. After that time, the password expires. The count starts when the user changes their passwords. Users are required to change an expired password the next time they log in. If set to never, passwords do not expire. Does not apply to SNMP users. • Range: 1-1827 or Password never expire. • Default: Password never expire.
Warn users before password expiration	The number of days before the password expires that the user starts getting warned they will have to change it. A user that does not log in will not see the warning. • Range: 1-366. • Default: 7.

Lockout users after password expiration	Lockout users after password expiration. After a user's password has expired, they have this number of days to log in and change it. If they do change their password within that number of days they will be unable to log in: They are locked out. A value of never allows the user to wait as long as they want to change their password. The administrator can unlock a user that is locked out from the User Management > Users page. • Range: 1-1827, or Never • Default: Never lockout users after password expires
Force users to change password at first login after password was changed from Users page	Force users to change password at first login after their password was changed using the command <code>set user <username> password</code> or from the WebUI User Management > Users page. • Default: Not selected

Deny Access to Unused Accounts

Parameter	Description
Deny access to unused accounts	Deny access to unused accounts. If there has been no successful login attempt in a set period of time, the user is locked out and cannot log in. • Default: Not selected
Days of non-use before lock-out	Days of non-use before lock-out. The number of days in which a user has not (successfully) logged in before that user is locked out. This only takes effect if Deny access to unused accounts is selected. • Range: 30-1827 • Default: 365

Deny Access After Failed Login Attempts

Note - These configurations do not apply to the admin user. The admin user is not blocked irrespective of failed login attempts.

Parameter	Description
Deny access after failed login attempts	If the configured limit is reached, the user is locked out (unable to log in) for a configurable period of time. Warning: Enabling this leaves you open to a "denial of service" -- if an attacker issues unsuccessful login attempts often enough you will be locked out. Please consider the advantages and disadvantages of this option, in light of your security policy, before enabling it. • Default: Not selected

Maximum number of failed attempts allowed	This only takes effect if Deny access after failed attempts is enabled. The number of failed login attempts that a user is allowed before being locked out. After making that many successive failed attempts, future attempts will fail. When one login attempt succeeds, counting of failed attempts stops, and the count is reset to zero, • Range: 2-1000 • Default: 10
Allow access again after time	Allow access again after a user has been locked out (due to failed login attempts). The user is allowed access after the configured time if there have been no login attempts during that time). This setting only takes effect if Deny access after failed login attempts is selected. • Range: 60-604800 (seconds) • Default: 1200 (20 minutes) Examples: 60 - 1 minute 300 - 5 minutes 3600 - 1 hour 86400 - 1 day 604800 - 1 week

Configuring Password Policy- CLI (password-controls)

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

Password Strength

```
set password-controls
  min-password-length <6-128>
  palindrome-check <on |off>
  complexity <1-4>
```

Parameter	Description
min-password-length <6-128>	The minimum number of characters of a password that is to be allowed for users or SNMP users. Does not apply to passwords that have already been set. • Range: 6-128 • Default: 6

palindrome-check <on off>	A palindrome is a sequence of letters, numbers, or characters that can be read the same in each direction. On prevents passwords that are palindromes. • Range: On or Off. • Default: On
complexity <1-4>	The required number of character types. Character types are: Upper case alphabetic (A-Z), Lower case alphabetic (a-z), Digits (0-9), Other (everything else). A value of "1" effectively disables this check. Changes to this setting do not affect existing passwords. • Range: 1-4 • Default: 2

Password History

```
set password-controls
  history-checking <on|off>
  history-length <1-1000>
```

Parameter	Description
history-checking <on off>	Check for reuse of passwords. 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. Enables or disables password history checking and password history recording, for all users. • Range: On or Off. • Default: On
history-length <1-1000>	The number of former passwords to keep and check against for each user. • Range: 1-1000. • Default: 10.

Mandatory Password Change

```
set password-controls
  password-expiration <never, 1-1827>
  expiration-warning-days <1-366>
  expiration-lockout-days <never, 1-1827>
  force-change-when <no|password>
```

Parameter	Description
password-expiration <never, 1-1827>	The number of days for which a password is valid. After that time, the password expires. The count starts when the user changes their passwords. Users are required to change an expired password the next time they log in. If set to never, passwords do not expire. Does not apply to SNMP users. • Range: 1-1827 or never. • Default: never.
expiration-warning-days <1-366>	The number of days before the password expires that the user starts getting warned they will have to change it. A user that does not log in will not see the warning. • Range: 1-366. • Default: 7.
expiration-lockout-days <never, 1-1827>	Lockout users after password expiration. After a user's password has expired, they have this number of days to log in and change it. If they do change their password within that number of days they will be unable to log in: They are locked out. A value of never allows the user to wait as long as they want to change their password. The administrator can unlock a user that is locked out using the command <code>set user <username> lock-out</code>. • Range: 1-1827, or never • Default: never
force-change-when <no password>	Force users to change password at first login after their password was changed using the command <code>set user <username> password</code> or from the WebUI User Management > Users page. • Range: • no - Disables this functionality. • password - Forces users to change their password after their password was changed using the command <code>set user <username> password</code> or from the WebUI User Management > Users page. • Default: no

Deny Access to Unused Accounts

```
set password-controls
  deny-on-nonuse enable <off|on>
  deny-on-nonuse allowed-days <30-1827>
```

Parameter	Description
deny-on-nonuse enable <off on>	Deny access to unused accounts. If there has been no successful login attempt in a set period of time, the user is locked out and cannot log in. • Range: on/off • Default: off

deny-on-nonuse allowed-days <30-1827>	Days of non-use before lock-out. The number of days in which a user has not (successfully) logged in before that user is locked out. This only takes effect if set <code>password-controls deny-on-nonuse enable</code> is set to on. • Range: 30-1827 • Default: 365
--	---

Deny Access After Failed Login Attempts

```
set password-controls
  deny-on-fail allow-after <60-604800>
  deny-on-fail failures-allowed <2-1000>
  deny-on-fail enable <off|on>
```

Note - These configurations do not apply to the admin user. The admin user is not blocked irrespective of failed login attempts.

Parameter	Description
deny-on-fail enable <off on>	Deny access after too many failed login attempts. If the configured limit is reached, the user is locked out (unable to log in) for a configurable period of time. Warning: Enabling this leaves you open to a "denial of service" -- if an attacker issues unsuccessful login attempts often enough you will be locked out. Please consider the advantages and disadvantages of this option, in light of your security policy, before enabling it. • Range: on/off • Default: off
deny-on-fail failures-allowed <2-1000>	This only takes effect if set <code>password-controls deny-on-fail enable</code> is set to on. The number of failed login attempts that a user is allowed before being locked out. After making that many successive failed attempts, future attempts will fail. When one login attempt succeeds, counting of failed attempts stops, and the count is reset to zero, • Range: 2-1000 • Default: 10

deny-on-fail allow-after <60-604800>	Allow access again after a user has been locked out (due to failed login attempts). The user is allowed access after the configured time if there have been no login attempts during that time. This setting only takes effect if set password-controls deny-on-fail enable is set to on. • Range: 60-604800 (seconds) • Default: 1200 (20 minutes) Examples: 60 - 1 minute 300 - 5 minutes 3600 - 1 hour 86400 - 1 day 604800 - 1 week
deny-on-fail failures-allowed <2-1000>	This only takes effect if set password-controls deny-on-fail enable is set to on. The number of failed login attempts that a user is allowed before being locked out. After making that many successive failed attempts, future attempts will fail. When one login attempt succeeds, counting of failed attempts stops, and the count is reset to zero, • Range: 2-1000 • Default: 10

Monitoring Password Policy

Use these commands to view password Policy configuration

```
show password-controls
all
complexity
deny-on-fail allow-after
deny-on-fail enable
deny-on-fail failures-allowed
deny-on-nonuse allowed-days
deny-on-nonuse enable
expiration-lockout-days
expiration-warning-days
force-change-when
history-checking
history-length
min-password-length
palindrome-check
password-expiration
```

Example

```
> 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

Authentication Servers

You can configure Gaia to authenticate Gaia users even when they are not defined locally. This is a good way of centrally managing the credentials of multiple Security Gateways. To define non-local Gaia users, you define Gaia as a client of an authentication server.

Gaia supports these types of authentication servers:

RADIUS

RADIUS (Remote Authentication Dial-In User Service) is a client/server authentication system that supports remote-access applications. User profiles are kept in a central database on a RADIUS authentication server. Client computers or applications connect to the RADIUS server to authenticate users.

You can configure your Gaia computer to connect to more than one RADIUS server. If the first server in the list is unavailable, the next RADIUS server in the priority list connects.

TACACS

The TACACS+ (Terminal Access Controller Access Control System) authentication protocol users a remote server to authenticate users for Gaia. All information sent to the TACACS+ server is encrypted.

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

You can configure TACACS+ support separately for different services. The Gaia WebUI service is one of those for which TACACS+ is supported and is configured as the http service. When TACACS+ is configured for use with a service, Gaia contacts the TACACS+ server each time it needs to examine a user password. If the server fails or is unreachable, the user is authenticated via local password mechanism. If the user fails to authenticate via the local mechanism, the user is not allowed access.

Note - For TACACS authentication to work on a Virtual System, see the *VSX administration Guide* <http://downloads.checkpoint.com/dc/download.htm?ID=54764>.

Configuring RADIUS Servers - WebUI

To configure a RADIUS server:

1. In the tree view, click **User Management > Authentication Servers**.
2. In the **RADIUS Servers** section, click **Add**.
The **Add New RADIUS Server** window opens.
3. Enter the *RADIUS Server parameters*.
4. Click **OK**.
5. **Optional:** Select the **Network Access Server (NAS)** IP address.
6. **Optional:** Select the **Super User ID**.
7. Click **Apply**.

RADIUS Server Parameters

Parameter	Description
Priority	The RADIUS server priority is an integer between 0 and 999 (default=0). When there two or more RADIUS servers, Gaia connects to the server with the highest priority. Low numbers have the higher priority.
Host	RADIUS server host name or IP address (IPv4 or IPv6).
UDP Port	RADIUS server UDP port. The default port is 1812 as specified by the RADIUS standard. The range of valid port numbers is 1 to 65535. Warning - Firewall software frequently blocks traffic on port 1812. Make sure that you define a firewall rule to allow port 1812 traffic between the RADIUS server and Gaia.
Shared Secret	Shared secret used for authentication between the authentication server and the Gaia client. Enter the shared secret text string without a backslash. Make sure that the shared string defined on the Gaia client matches that which is defined on the authentication server. Some RADIUS servers have a maximum shared secret string length of 15 or 16 characters. See the documentation for your RADIUS server.
Timeout in Seconds	Optional: Enter the timeout period in seconds. The default value is 3. If there is no response after the timeout period, Gaia tries to connect to a different server.
Network Access Server (NAS)	Optional: An IP address of the Security Gateway interface. This parameter records the IP address that the RADIUS packet comes from. This address is stored in the RADIUS packet even when the packet goes through NAT or some other address translation, that changes the source IP of the packet. The NAS-IP-Address is defined in RFC2865 http://freeradius.org/rfc/rfc2865.html#NAS-IP-Address . If no NAS IP Address is chosen, the IPv4 address of the Gaia host is used.
Super User ID	Optional: The UID for the RADIUS super user. Select 0 or 96. If the UID is 0 there is no need to run the sudo command to get super user permissions (" Configuring RADIUS Servers for Non-Local Gaia Users " on page 150).

To edit a RADIUS server:

1. In the tree view, click **User Management > Authentication Servers**.
2. Select a RADIUS server.
3. Click **Edit**.

The **Edit RADIUS Server** window opens.

4. You can edit the **Host** name, **UDP port** number, **Shared secret**, and **Timeout**. You cannot change the **Priority**.
5. Click **OK**.

To delete a RADIUS server:

1. In the tree view, click **User Management > Authentication Servers**.
2. Select a RADIUS server from the table.
3. Click **Delete**.

The **Remove RADIUS Server** window opens.

4. Click **OK** to confirm.

Configuring RADIUS Servers - CLI (aaa)

Description

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

Syntax

To configure RADIUS for use in a single authentication profile:

```
add aaa radius-servers priority VALUE host VALUE [ port VALUE ]
    prompt-secret timeout VALUE
    secret VALUE timeout VALUE
```

To delete a RADIUS configuration:

```
delete aaa radius-servers
    priority VALUE
    NAS-IP
```

To change the configuration of a RADIUS entry:

```
set aaa radius-servers priority VALUE
    host VALUE
    new-priority VALUE
    port VALUE
    prompt-secret
    secret VALUE
    timeout VALUE
set aaa radius-servers
    super-user-uid VALUE
    NAS-IP VALUE
```

To view a list of all servers associated with an authentication profile:

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

To view the RADIUS server configuration:

```
show aaa radius-servers priority VALUE
  host
  port
  timeout
show aaa radius-servers
  super-user-uid
  NAS-IP
```

Parameters

Parameter	Description
priority	The RADIUS server priority is an integer between 0 and 999 (default=0). When there two or more RADIUS servers, Gaia connects to the server with the highest priority. Low numbers have the higher priority.
new-priority	The priority of the new RADIUS server
host	Host name or the IP address (IPv4 or IPv6) of the RADIUS server
port	UDP port on the RADIUS server. This value must match the port as configured on the RADIUS server. Typically this 1812 (default) or 1645 (non-standard but a commonly used alternative).
prompt secret	Shared secret (password) text string. The system prompts you to enter the value.
timeout	The number of seconds to wait for the server to respond. The default value 3 seconds.
secret	The shared secret used to authenticate the RADIUS server and the local client. You must define this value on your RADIUS server.
super-user-uid	The UID for the RADIUS super user. Select 0 or 96. If the UID is 0 there is no need to run the <code>sudo</code> command to get super user permissions (" Configuring RADIUS Servers for Non-Local Gaia Users " on page 150).
NAS-IP	An IP address of the Security Gateway interface. This parameter records the IP address that the RADIUS packet comes from. This address is stored in the RADIUS packet even when the packet goes through NAT or some other address translation, that changes the source IP of the packet. The NAS-IP-Address is defined in RFC2865 http://freeradius.org/rfc/rfc2865.html#NAS-IP-Address . If no NAS IP Address is chosen, the IPv4 address of the Gaia host is used.

Example

```
show aaa radius-servers priority 1 host
```

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 configure Gaia as a RADIUS Client

1. Define the role for the RADIUS client:
 - If no group is defined on the RADIUS server for the client, define the role:
radius-group-any
 - If a group is defined on RADIUS server for the client (group XXX, for example), define the role:
radius-group-XXX
2. Define the features for the role.

For instructions, see Roles (on page 133).



Note - Do not define a new user for external users. An external user is one that is defined on an authentication server (such as RADIUS or TACACS) and not on the local Gaia system.

Configuring RADIUS Servers for Non-Local Gaia Users

Non-local users can be defined on a RADIUS server and not in Gaia. When a non-local user logs in to Gaia, the RADIUS server authenticates the user and assigns the applicable permissions. You must configure the RADIUS server to correctly authenticate and authorize non-local users.



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

To configure a RADIUS server for non-local Gaia users

1. Copy the applicable dictionary file to your RADIUS server:

Steel-Belted RADIUS server

- a) Copy `/etc/radius-dictionaries/checkpoint.dct` to the server directory.
- b) Add the following lines to the `vendor.ini` file on RADIUS server (keep in alphabetical order with the other vendor products in this file):


```
vendor-product = Check Point Gaia
dictionary = nokiaipso
ignore-ports = no
port-number-usage = per-port-type
help-id = 2000
```
- c) Add to the `dictionary.dcm` file the line:


```
"@checkpoint.dct"
```

FreeRADIUS server

- d) Copy `/etc/radius-dictionaries/dictionary.checkpoint` (on Gaia) to `/etc/freeradius/` (on the RADIUS server).
- e) Add to `/etc/freeradius/dictionary` the line:


```
"$INCLUDE dictionary.checkpoint"
```

OpenRADIUS server

- f) Copy
`/etc/radius-dictionaries/dict.checkpoint`
 on Gaia to
`/etc/openradius/subdicts/`
 on the RADIUS server.
- g) Add the line
`$include subdicts/dict.checkpoint`
 to
`/etc/openradius/dictionaries`
 immediately after `dict.ascend`
2. Define the user roles.
 Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:
`CP-Gaia-User-Role = "role1,role2,..."`
 For example:
`CP-Gaia-User-Role = "adminrole, backuprole, securityrole"`
Note - Make sure the role names match the existing roles in the Gaia system.
3. Define the Check Point users that must have superuser access to the Gaia shell. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:
`CP-Gaia-SuperUser-Access = <0|1>`
 0 - This user cannot receive superuser permissions
 1 - This user can receive superuser permissions

To log in as a superuser

A user with super user permissions can use the Gaia shell to do system-level operations, including working with the file system. Super user permissions are defined in the Check Point Vendor-Specific Attributes.

Users that have a UID of 0 have super user permissions. They can run all the commands that the root user can run. Users that have a UID of 96 must run the `sudo` command to get super user permissions. The UIDs of all non-local users are defined in the file `/etc/passwd`

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

1. Log into the system using command line.
2. Enter expert mode to go to the Gaia shell.
3. Run
`sudo /usr/bin/su -`

The user now has superuser permissions

Configuring TACACS+ Servers - WebUI

To configure a TACACS+ server:

1. In the tree view, click **User Management > Authentication Servers**.
2. In the **TACACS+ Configuration** section, select **Enable TACACS+ authentication**.
3. Click **Apply**.

4. Configure one or more TACACS+ servers. In the **TACACS+ Servers** section, for each TACACS+ server:
 - a) Click **Add**.
The **Add new TACACS+ Server** window opens.
 - b) Configure the TACACS+ parameters.
 - c) Click **OK**.

TACACS+ Parameters

Parameter	Description
Priority	The priority of the TACACS+ server. Must be unique for this operating system. The priority is used to: - Determine the order in which Gaia makes contact with the servers. The server with the lowest priority number is first. For example, if three TACACS+ servers have a priority of 1, 5, and 10 respectively. Gaia makes contact with the servers in that order, and uses the first server that responds. - Identify the server in commands. A command with priority 1 applies to the server with priority 1.
Server	The TACACS+ server IPv4 address.
Shared Key	The shared secret used for authentication between the authentication server and the Gaia client. Enter the shared secret text string without a backslash. Make sure that the shared string defined on the Gaia client matches that which is defined on the authentication server.
Timeout in Seconds	The maximum number of seconds to wait for the server to respond.

To disable TACACS+ authentication:

1. In the tree view, click **User Management > Authentication Servers**.
2. In the **TACACS+ configuration** section, clear **Enable TACACS+ authentication**.
3. Click **Apply**.

To disable a TACACS+ server:

1. In the tree view, click **User Management > Authentication Servers**.
2. In the **TACACS+ Server** section, select a server.
3. Click **Delete**.

To make sure the logged in user is enabled for Tacacs+, run:

```
show tacacs_enable
```

Configuring TACACS+ Servers - CLI (aaa)

Description

Use the `aaa tacacs -servers` commands to configure one or more TACACS+ authentication servers.

Syntax

To add a TACACS+ server:

```
add aaa tacacs-servers priority VALUE server VALUE key VALUE timeout VALUE
```

To change the configuration of a TACACS+ server entry:

```
set aaa tacacs-servers priority VALUE
  key VALUE
  new-priority VALUE
  server VALUE
  timeout VALUE
set aaa tacacs-servers state VALUE
```

To delete TACACS+ server from the list of servers:

```
delete aaa tacacs-servers priority VALUE
```

To see the configuration of the TACACS+ servers

```
show aaa tacacs-servers
  list
  priority VALUE server
  priority VALUE timeout
  state
```

Parameters

Parameter	Description
priority VALUE	The priority of the TACACS+ server. Must be unique for this operating system. The priority is used to: • Determine the order in which Gaia makes contact with the servers. The server with the lowest priority number is first. For example, if three TACACS+ servers have a priority of 1, 5, and 10 respectively. Gaia makes contact with the servers in that order, and uses the first server that responds. • Identify the server in commands. A command with priority 1 applies to the server with priority 1. • Range: Integers 1 - 20 • Default: No default.
server VALUE	The TACACS+ server IPv4 address. • Default: No default.

key VALUE	The shared secret used for authentication between the authentication server and the Gaia client. Enter the shared secret text string without a backslash. Make sure that the shared string defined on the Gaia client matches that which is defined on the authentication server. • Range: Text strings, up to 256 characters, without any whitespace characters. • Default: No default.
timeout VALUE	The maximum number of seconds to wait for the server to respond. • Range: 1-60. • Default: 5
new-priority VALUE	The new priority.
state VALUE	Range: On - Enable TACACS+ authentication for all servers. Off - Disable TACACS+ authentication for all servers.
list	The list of TACACS+ servers that this system is configured to use.

Example

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

Configuring Gaia as a TACACS+ Client

Gaia acts as a TACACS+ client for Gaia users that are defined on the TACACS+ server and are not defined locally on Gaia. The admin user must define a role called TACP-0 for the TACACS+ users, and the features for the TACP-0 role.

Privilege Escalation

The Gaia admin user can define roles that make it possible for Gaia users to temporarily get higher privileges than their regular privileges. For example, Gaia user Fred needs to configure the firewall, but his role does not support firewall configuration. To configure the firewall, Fred uses his user name together with a password given him by the admin user. This password let him change role to one that allows him to configure the firewall.

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. N is a number from 1 to 15. The TACACS+ users can changes their own privileges by moving to another TACP-N role. To do this, the TACACS+ users need to get a password from the Gaia admin user.

To configure Gaia as a TACACS+ Client:

1. Connect to Gaia as the admin user.
2. Define the role TACP-0

3. Define the features for the role.
For instructions, see Roles (on page 133).
4. **Optional:** Define one or more roles with the name TACP-N where N is a number from 1 to 15, and define the features for each role.

To raise TACP privileges using the CLI:

1. Connect to Gaia CLI as a TACACS+ user.
2. Enter the username and password of the user.
After you are authenticated by the TACACS server, you will see the clish prompt. At this point you have the privileges of the TACP-0 role.
3. Run:
`tacacs_enable TACP-N`
Where N is the new TACP role (an integer from 1 to 15).
4. When prompted, enter the applicable password.

To go back to the TACP-0 role, press **Ctrl+D**.

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

```
show tacacs_enable
```

To raise privileges using the WebUI

1. Connect to Gaia WebUI as a TACACS+ user.
2. Enter the username and password of the user.
After you are authenticated by the TACACS server you have the privileges of the TACP-0 role.
3. To raise the privileges to the TACP-N role (N is a number from 1 to 15), click **Enable** at the top of the **Overview** page.
4. Enter the password for the user.

To go back to the TACP-0 role from a different TACP-N role, press **Ctrl+D** or enter **exit** at the command prompt. The user automatically exits the current shell and goes back to TACP-0.

Configuring TACACS+ Servers for Non-Local Gaia Users

You can define Gaia users on a TACACS server instead of defining them on the Gaia computer. Gaia users that are defined on a TACACS server are called non-local users. Cisco ACS servers are the most commonly used TACACS+ servers. For help with the configuration of a Cisco ACS server as a TACACS+ server for Gaia clients, see sk98733

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



Note - sk98733 <http://supportcontent.checkpoint.com/solutions?id=sk98733> is an example of best practices and not a replacement for the official Cisco documentation.

When a non-local user logs in to Gaia, the TACACS server authenticates the user and assigns the permissions to the user. You must configure the TACACS server to correctly authenticate and authorize non-local Gaia users.



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

System Groups

You can define and configure groups with Gaia as you can with equivalent Linux-based systems. This function is retained in Gaia for advanced applications and for retaining compatibility with Linux.

Use groups for these purposes:

- Specify Linux file permissions.
- Control who can log in through SSH.

For other functions that are related to groups, use the role-based administration feature, described in "Role-Based Administration" ("[Roles](#)" on page [133](#)).

All users are assigned by default to the `users` group. You can edit a user's primary group ID (using `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 - WebUI

To see a list of all groups:

Choose **User Management > System Groups** in the navigation tree.

To add a group:

1. In the **User Management > System Groups** page, click **Add**.
2. Enter the **Group Name**. 1-8 alphanumeric characters.
3. Enter a **Group ID** number.
Group ID ranges 0-99 and 65531-65535 are reserved for system use. (GID 0 is reserved for users with root permissions and GID 10 is reserved for the predefined `Users` groups). If you specify a value in the reserved ranges, an error message is displayed.
4. Click **OK**.

To add a member to a group:

1. In the **User Management > System Groups** page, select a group.
2. Click **Edit**.
3. Click **Add New Member**.
4. Select a user.
5. Click **OK**.

To delete a member from a group:

1. In the **User Management > System Groups** page, select the group.
2. Click **Edit**.
3. Select the member
4. Click **Remove Member**
5. Click **OK**

To delete a group:

1. In the **User Management > System Groups** page, select the group.
2. Click **Delete**.
3. Click **OK**.

Configuring System Groups - CLI (group)

Description

The commands in this section allow you to manage groups.

Syntax

To view existing group members:

```
show group VALUE
```

To see existing groups:

```
show groups
```

To set the Group ID:

```
set group VALUE gid VALUE
```

To add a group or a group member:

```
add group VALUE gid VALUE  
add group VALUE member VALUE
```

To delete a group or a group member

```
delete group VALUE member VALUE
```

Parameters

Parameter	Description
group VALUE	Name of group. 1-8 alphanumeric characters, Must be unique on your system.
gid VALUE	Numeric Group ID. Must be unique on your system. Note - Group ID ranges 0-99 and 65531-65535 are reserved for system use. (GID 0 is reserved for users with root permissions and GID 10 is reserved for the predefined Users groups). If you specify a value in the reserved ranges, an error message is displayed.
member VALUE	Name of an existing user. For example, <code>admin</code> or <code>monitor</code> .

GUI Clients

GUI Clients are trusted hosts from which Administrators are allowed to log in to the Security Management Server.

Security Management GUI Clients - WebUI

Define which GUI clients (SmartConsoles) can connect to the Security Management Server.

To configure the GUI clients:

1. In the tree view, click **User Management > GUI Clients**.

2. Click **Add**.

The **Add GUI Client** window opens.

3. Define the GUI clients (trusted hosts). These are the values:

- Any.

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.

- An IP address
- A network
- A range of addresses



Note - GUI clients can be deleted on the **User Management > GUI Clients** page.

GUI Clients - CLI (cpconfig)

1. Run: `cpconfig`.

A list of configuration options shows. For example:

Configuration Options:

- (1) Licenses and contracts
- (2) Administrator
- (3) GUI Clients
- (4) SNMP Extension
- (5) PKCS#11 Token
- (6) Random Pool
- (7) Certificate Authority
- (8) Certificate's Fingerprint
- (9) Disable Check Point SecureXL
- (10) Configure Check Point CoreXL
- (11) Automatic start of Check Point Products

2. Enter 3.

3. A list of hosts selected to be GUI clients, shows.

You can add or delete hosts, or create a new list.

New GUI clients can be added using these formats:

- IP address.
- Machine name.
- "Any" - Any IP without restriction.
- IP/Netmask - A range of addresses, for example 192.0.2.0/255.255.255.0
- A range of addresses - for example 192.0.2.10-192.0.2.16
- Wild cards (IP only) - for example 192.0.2.*

High Availability

In This Section:

VRRP	159
Configuring Monitored Circuit/Simplified VRRP	166
Configuring Advanced VRRP	171
Troubleshooting VRRP	175

VRRP

Virtual Routing Redundancy Protocol (VRRP) is a high-availability solution where two Gaia Security Gateways can provide backup for each other. Gaia offers two ways to configure VRRP:

- **Monitored Circuit/Simplified VRRP** - All the VRRP interfaces automatically monitor other VRRP interfaces
- **Advanced VRRP** - Every VRRP interface must be explicitly configured to monitor every other VRRP interface

Important - You cannot have a standalone deployment (Security Gateway and Security Management Server on the same computer) in a Gaia VRRP cluster.

Understanding VRRP

Virtual Router Redundancy Protocol (VRRP) provides dynamic failover of IP addresses from one router to another in the event of failure. This increases the availability and reliability of routing paths via gateway selections on an IP network. Each VRRP router has a unique identifier known as the Virtual Router Identifier (VRID) which is associated with at least one Virtual IP Address (VIP). Neighboring network nodes connect to the VIP as a next hop in a route or as a final destination. Gaia supports VRRP as defined in RFC 3768.

On Gaia, VRRP can be used with and without ClusterXL enabled. With ClusterXL enabled, the most common use case, VRRP supports a maximum of one VRID with one Virtual IP Address (VIP) for each interface. Also, only active/backup environments are supported and you must configure VRRP so that the same node is the VRRP master for all VRIDs. Therefore, you must configure each VRID to monitor every other VRRP-enabled interface. You must also configure *priority deltas* to allow a failover to the backup node when the VRID on any on interface does a failover.

With ClusterXL disabled, active/active environments can be deployed. You can configure two VRIDs on the same interface, with one VIP for each VRID. Only Static Routes are supported on the VRRP interfaces. Also, you must disable VRRP monitoring of the Firewall ("[Configuring Global Settings for VRRP](#)" on page 165).

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	Primary (active) member	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	Backup (standby) member	A redundant Security Gateway (Security Gateway) that is available to take over for the master in the event of a failure.
VRID	Cluster name	Unique Virtual Router identifier The VRID is the also last byte of the MAC address.
VIP	Cluster IP address	Virtual IP address assigned to a Virtual Router. VIPs are routable from internal and/or external network resources. The VIP is called Backup Address in the WebUI.
VMAC		Virtual MAC address assigned to a Virtual Router.
VRRP Transition	Failover	Automatic change over to a backup Security Gateway when the primary Security Gateway fails or is unavailable. The term 'failover' is used frequently in this guide.

VRRP Configuration Methods

You can configure VRRP using one of these methods:

- **Monitored Circuit/Simplified VRRP**

This method contains all of the basic parameters, and is applicable for most environments. It makes possible a complete node failover, by automatically monitoring all VRRP-enabled interfaces. You can configure only one VRID, which is automatically added to all the VRRP interfaces. If the VRID on any of the interfaces fails, the configured priority delta is decremented on the other interfaces to allow the backup node to take over as the VRRP master.

In the Gaia WebUI, configure Monitored Circuit/Simplified VRRP in the **High Availability > VRRP** section.

- **Advanced VRRP**

This method allows for different VRIDs to be configured on different interfaces. With ClusterXL enabled, you must configure each VRID to monitor every other VRRP interface. You must also

configure priority deltas that allow complete node failover. Advanced VRRP also makes it possible for a VRID to monitor interfaces that do not run VRRP. With ClusterXL disabled, active/active deployments are possible, and you can configure two VRIDs on each interface, with one VIP for each VRID ("[Internal Network Load Sharing](#)" on page 163).

In the Gaia WebUI, configure Advanced VRRP in the **High Availability > Advanced VRRP** section.

You cannot use the Monitored Circuit/Simplified and Advanced types together on the same Security Gateway.

How VRRP Failover Works

Each Virtual Router (VRRP Group) is identified by a unique *Virtual Router ID (VRID)*. A Virtual Router contains one *Master* Security Gateway and at least one *Backup* Security Gateway. The master sends periodic VRRP advertisements (known as *hello messages*) to the backups.

VRRP advertisements broadcast the operational status of the master to the backups. Gaia uses dynamic routing protocols to advertise the VIP of the Virtual Router (virtual IP address or backup address).

Notes:

- Gaia supports OSPF on VPN tunnels that terminate at a VRRP group.
- Active/passive VRRP environments are supported with ClusterXL enabled. If ClusterXL is not enabled, active/active environments can be deployed.
- Active/Active environments support only static Routes. Also, you must disable the monitoring of the Firewall by VRRP.

If the master or its interfaces fails, VRRP uses a priority algorithm to make the decision if failover to a backup is necessary. Initially, the master is the Security Gateway that has the highest defined priority value. You define a priority for each Security Gateway when you create a Virtual Router or change its configuration. If two Security Gateways have same priority value, the platform that comes online and broadcasts its VRRP advertisements first becomes the master.

Gaia also uses priorities to select a backup Security Gateway upon failover (when there is more than one 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 master. The *Priority Delta* value is a Check Point proprietary parameter that you define when configuring a Virtual Router. If you configure your system correctly, the effective priority will be lower than the backup gateway priority in the other Virtual Routers. This causes the problematic master to fail over for the other Virtual Routers as well.

Note- If the effective priority for the current master and backup are the same, the gateway with the highest IP address becomes the master.

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

In *Advanced VRRP*, the VRID is configured on each interface individually. Also, 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 backup state.

The monitoring of all VRRP-enabled interfaces by all VRIDs is important to avoid connection issues with asymmetric routes. For example, when an external interface fails, the master fails

over only for the external Virtual Router. The 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 master.

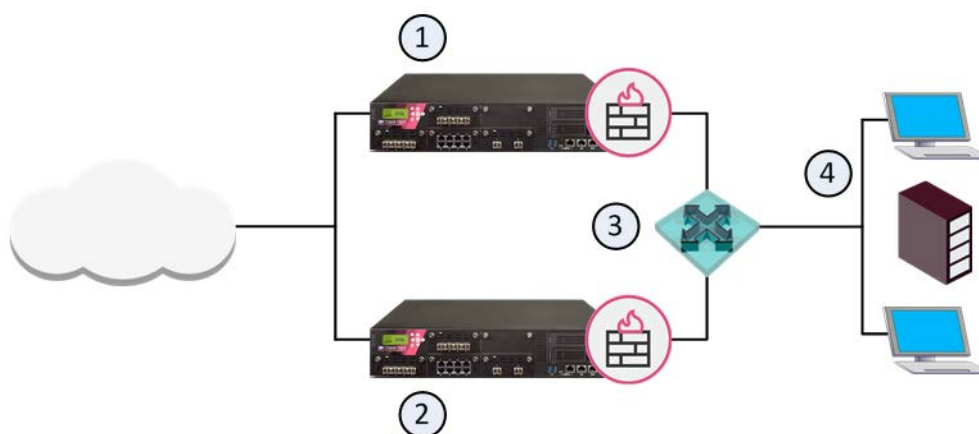
Another tool for avoiding asymmetric issues during transitions is the VRRP *interface delay* setting. Configure this when the Preempt Mode of VRRP has been turned off. This VRRP global setting is useful when the VRRP node with a higher priority is rebooted but must not preempt the existing VRRP master that is handling the traffic but is configured with a lower priority. Sometimes interfaces that come up take longer than the VRRP timeout to process incoming VRRP hello packets. The interface delay extends the time that VRRP waits to receive Hello packets from the existing master.

Typical VRRP Use Cases

This section shows examples of some use case VRRP environments.

Internal Network High Availability

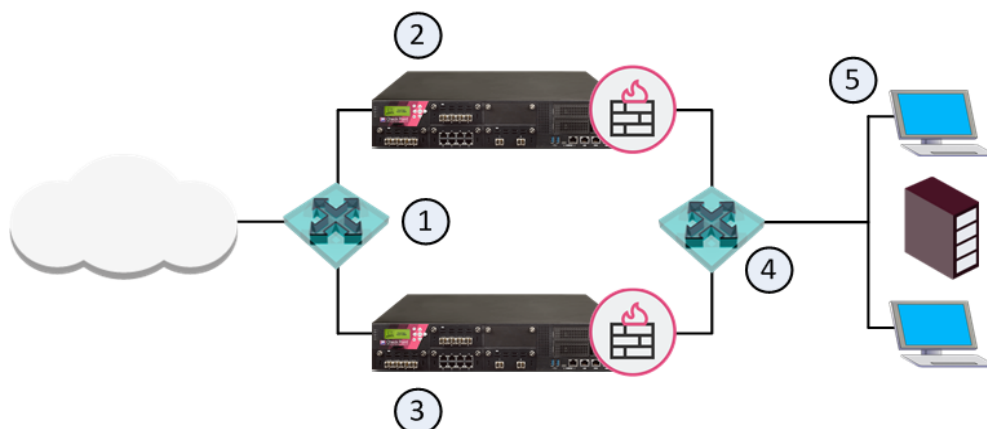
This is a simple VRRP high availability use case where Security Gateway 1 is the master and Security Gateway 2 is the backup. Virtual Router redundancy is available only for connections to and from the internal network. There is no redundancy for external traffic.



Item	Description
1	Master Security Gateway
2	Backup Security Gateway
3	Virtual Router VRID 5 - Virtual IP Address (Backup Address) is 192.168.2.5
4	Internal Network and hosts

Internal and External Network High Availability

This use case shows an example of an environment where there is redundancy for internal and external connections. Here, you can use one Virtual Routers for the two Security Gateways, for internal and for external connections. The internal and external interfaces must be on different subnets. Define one Security Gateway as the master and one as a backup.



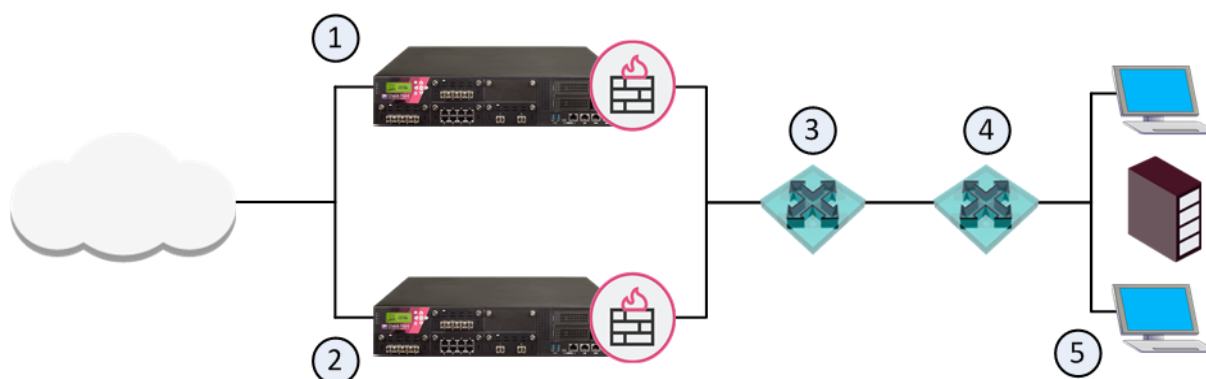
Item	Description
1	Virtual Router VRID 5. External Virtual IP Address (Backup Address) is 192.168.2.5
2	Master Security Gateway
3	Backup Security Gateway
4	Virtual Router VRID 5. Internal Virtual IP Address (Backup Address) is 192.168.3.5
5	Internal network and hosts

Internal Network Load Sharing

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

This configuration is supported with ClusterXL disabled. Only Static Routes are supported. The monitoring of the 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 master for VRID 5 and Security Gateway 2 is the backup. Security Gateway 2 is the master for VRID 7 and Security Gateway 1 is the 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	Master Security Gateway for VRID 5 and backup for VRID 7
2	Backup Security Gateway for VRID 5 and master for VRID7
3	Virtual Router, VRID 5 Virtual IP Address (Backup Address) is 192.168.2.5
4	Virtual Router, VRID 7 Virtual IP Address (Backup Address) is 192.168.2.7
5	Internal network and hosts

Preparing a VRRP Cluster

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

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

Configuring Network Switches

Best Practice - If you use the Spanning Tree protocol on Cisco switches connected to Check Point VRRP clusters, we recommend that you enable PortFast. PortFast sets interfaces to the Spanning Tree forwarding state, which prevents them from waiting for the standard forward-time interval.

If you use switches from a different vendor, we recommend that you use the equivalent feature for that vendor. If you use the Spanning Tree protocol without PortFast, or its equivalent, you may see delays during VRRP failover.

Enabling Virtual Routers

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

To enable VRRP clustering:

1. Install Gaia using the instructions in the *R80.10 Installation and Upgrade Guide*
<http://downloads.checkpoint.com/dc/download.htm?ID=54829>.
2. On the First Time Wizard **Products** page, select Security Gateway.
Do not select Security Management. The standalone environment (Security Gateway and Security Management Server) is not supported for VRRP.
3. Select **Unit is part of a cluster**.
4. Select **VRRP Cluster** from the list.
5. Continue with the next steps in the wizard.
6. When prompted to reboot the Security Gateway, click **Cancel**.
Do not reboot.

7. Do one of these steps:

- Run `cpconfig` on the Security Gateway. Select **Enable cluster membership for this gateway** to enable Firewall synchronization.

Note - This is the most common use and does not support active/active mode. You must configure VRRP so that the same cluster member is the VRRP master on all interfaces. Dynamic routing configuration must match on each cluster member.

OR:

- Do not enable ClusterXL.

Note - This is useful when each cluster member is required to be the VRRP master at the same time. You can configure two VRRP Virtual Routers on the same interface. Each cluster member can be the VRRP master for a different VRID on the same interface while it backs up the other. This configuration can also help run VRRP in a High-Availability pair with a device from another vendor. Disable the VRRP monitoring of the Firewall when you use this configuration. It is enabled by default but not supported with this configuration. Also, only Static Routes are supported with this configuration.

8. Enter `y` when prompted.

9. Reboot the Security Gateway.

Do this procedure for each Virtual Router member.

When you complete this procedure for each VRRP member, do these steps in the WebUI:

1. Select **VRRP** from the navigation tree.
2. Make sure that the **Disable All Virtual Routers** option is not selected.

When you complete these procedures, define your Virtual Routers using the WebUI or the CLI.

Configuring Global Settings for VRRP

This section includes shows you how to configure the global settings. Global settings apply to all Virtual Routers.

Configure these global settings:

Cold Start Delay - Delay period in seconds before a Security Gateway joins a Virtual Router. Default = 0.

Interface Delay - Configure this when the Preempt Mode of VRRP has been turned off. This is useful when the VRRP node with a higher priority is rebooted but must not preempt the existing VRRP master that is handling the traffic but is configured with a lower priority. Sometimes interfaces that come up take longer than the VRRP timeout to process incoming VRRP Hello packets. The *Interface Delay* extends the time that VRRP waits to receive Hello packets from the existing master.

Disable All Virtual Routers - Select this option to disable all Virtual Routers defined on this Gaia system. Clear this option to enable all Virtual Routers. By default, all Virtual Routers are enabled.

Monitor Firewall State - Select this option to let VRRP monitor the Security Gateway and automatically take appropriate action. This is enabled by default, which is the recommended setting when using VRRP with ClusterXL enabled. This must be disabled when using VRRP with ClusterXL disabled.

Important - If you disable **Monitor Firewall State**, VRRP can assign 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 master status.

Configuration Notes

Gaia starts to monitor the firewall after the cold start delay completes. This can cause some problems:

- If all the Security Gateway (member) interfaces in a Virtual Router fail, all Security Gateways become backups. None of the Security Gateways can become the master and no traffic is allowed.
- If you change the time on any of the Security Gateways (member), a failover occurs automatically.
- In certain situations, installing a firewall policy causes a failover. This can happen if it takes a long time to install the policy.

Configuring Monitored Circuit/Simplified VRRP

This section includes the procedure for configuring Monitored Circuit/Simplified VRRP.

Configuring Monitored Circuit/Simplified VRRP - CLI (mcvr)

Description

Use the `mcvr` command to configure Simplified/Monitored Circuit VRRP on a single gateway.

Syntax

Add and Delete commands

```
add mcvr vrid VALUE priority VALUE priority-delta VALUE
    [hello-interval VALUE authtype VALUE password VALUE]
add mcvr vrid VALUE backup-address VALUE vmac-mode VALUE [static-mac VALUE]
delete mcvr vrid VALUE
```

Important - The order that you run the `add mcvr` commands is important. Make sure that you run `add mcvr vrid VALUE priority VALUE priority-delta VALUE` first.

Set Commands

```
set mcvr vrid VALUE authtype VALUE [password VALUE]
set mcvr vrid VALUE backup-address VALUE vmac-mode VALUE [static-mac VALUE]
set mcvr vrid VALUE hello-interval VALUE
set mcvr vrid VALUE priority VALUE
```

Show commands

```
show mcvr vrid VALUE all
show mcvr vrid VALUE authtype
show mcvr vrid VALUE backup-addresses
show mcvr vrid VALUE hello-interval
show mcvr vrid VALUE password
show mcvr vrid VALUE priority
show mcvr vrid VALUE priority-delta
show mcvr vrids
```

Parameters

Parameter	Description
vrid	Enter a unique ID number for this virtual router. The range of valid values is 1 to 255.
authtype	none - No authentication necessary simple - A password is required for authentication You must use the same authentication method for all Security Gateways in a Virtual Router.
backup-addresses	This is the virtual IP address (VIP) for this Virtual Router. You can define more than one address for a Virtual Router. This IP address must be on the same subnet as an interface on the physical Security Gateway. The IP address must not match the IP address for another device on the subnet. You must configure the same backup address on each physical Security Gateway in the Virtual Router.
vmac-mode	VRRP - Sets the VMAC to the format outlined in the VRRP protocol specification RFC 3768. It is automatically set to the same value on all Security Gateways in a Virtual Router. This is the default. Interface - Sets the VMAC to the local interface MAC address. If you define this mode for the master and the backup, the VMAC is different for each. VRRP IP addresses are related to different VMACs because they are dependent on the physical interface MAC address of the current master. Static - Manually set the VMAC address. Enter the VMAC address after the <code>static-mac</code> keyword. Note - If you configure different VMACs on the master and backup, you must make sure that you select the correct proxy ARP setting for NAT. Extended - Gaia dynamically calculates and adds three bytes to the interface MAC address to generate more random address. If you select this mode, Gaia constructs the same MAC address for master and backups in the Virtual Router. Note - If you set the VMAC mode to Interface or Static, syslog error messages show when you restart the computer or during failover. This is caused by duplicate IP addresses for the master and backup. This is expected behavior because the master and backups temporarily use the same virtual IP address until they get master and backup status.
static-mac	If the vmac-mode parameter is set to static, you enter the static VMAC address.

Parameter	Description
hello-interval	(optional) Select the number of seconds, after which the master sends its VRRP advertisements. The valid range is between 1 (default) and 255 seconds. You must configure all VRRP routers on a Security Gateways with the same hello interval. Otherwise, more than one Security Gateway can be in the master state. The hello interval also defines the failover interval (the time a backup router waits to hear from the existing master before it takes on the master role). The value of the failover interval is three times the value of the hello interval (default - 3 seconds).
password	Enter an authentication password. This parameter is only relevant if the <code>authtype</code> value is set to simple .
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 master. The range of valid values 1 to 254.
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 backup, the value of the priority delta is subtracted from its priority. This gives a higher effective priority to a different Security Gateway member. If the effective priority of the current master is less than that of the backup, the backup becomes the master for this Virtual Router. If the effective priority for the current master and backup are the same, the gateway with the highest IP address becomes the master.
vrids	Shows all Virtual Routers.

Configuring Monitored Circuit/Simplified VRRP - WebUI

This section includes the basic procedure for configuring a Virtual Router using the Gaia WebUI.

To add a new Virtual Router:

1. In the navigation tree, select **VRRP**.
2. In the **Virtual Routers** section, click **Add**.
3. In the **Add Virtual Router** window, configure these parameters:
 - **Virtual Router ID** - Enter a unique ID number for this virtual router. The range of valid values is 1 to 255.
 - **Priority** - Enter the priority value, which selects the Security Gateway that takes over in the event of a failure. The Security Gateway with the highest available priority becomes the new master. The range of valid values 1 to 254. The default setting is 100.

- **Hello Interval** - (optional) Select the number of seconds, after which the 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 master state.

The hello interval also defines the failover interval (the time a backup router waits to hear from the existing master before it takes on the master role). The value of the failover interval is three times the value of the hello interval (default - 3 seconds).

- **Authentication:**
none - No authentication necessary
simple - A password is required for authentication

You must use the same authentication method for all Security Gateways in a Virtual Router. If you select **simple**, enter a password in the applicable field.

- **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 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 master is less than that of the backup, the backup becomes the master for this Virtual Router. If the effective priority for the current master and backup are the same, the gateway with the highest IP address becomes the master.

4. In the **Backup Addresses** section, click **Add**. Configure these parameters in the **Add Backup Address** window:

- **IPv4 address** - Enter the interface IPv4 address.
- **VMAC Mode** - Select one of these Virtual MAC modes:
 - **VRRP** - Sets the VMAC to use the standard VRRP protocol. It is automatically set to the same value on all Security Gateways in the Virtual Router. This is the default setting.
 - **Interface** - Sets the VMAC to the local interface MAC address. If you define this mode for the master and the 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 master.
Note - If you configure different VMACs on the master and 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 more random address. If you select this mode, Gaia constructs the same MAC address for master and backups in the Virtual Router.
Note - If you set the VMAC mode to Interface or Static, syslog error messages show when you restart the computer or during failover. This is caused by duplicate IP addresses for the master and backup. This is expected behavior because the master and backups temporarily use the same virtual IP address until they get master and backup status.

Click **Save**. The new VMAC mode shows in the in the **Backup Address** table.

5. To remove a backup address, select an address and click **Delete**. The address is removed from the **Backup Address** table.

- Click **Save**.

Configuring the VRRP Security Gateway Cluster in SmartConsole

- From the **Networks Objects** tree, select **Check Point > Security Cluster > Check Point appliance/ Open Server**.

The **Security Gateway Cluster Creation** window opens

- Choose **Wizard Mode**.
- Define the:
 - Cluster Name**
 - Cluster IPv4 Address**
 - For an IPv6 cluster: **Cluster IPv6 Address**
- Choose the Cluster's Solution: Gaia VRRP**.
- Click **Finish**.

Configuring VRRP Rules for the Security Gateway

- Define this rule above the Stealth Rule in the Rule Base:

Source	Destination	VPN	Services & Applications	Action
Firewalls (Group) fwcluster-object	mcast-224.0.0.1	Any	vrrp igmp	Accept

Where:

- Firewalls** -Simple Group object containing the firewall objects.
 - fwcluster-object** - the VRRP cluster object.
 - mcast-224.0.0.18** - Node Host object with the IP address 224.0.0.18.
- If your Security Gateways use dynamic routing protocols (such as OSPF or RIP), create new rules for each multicast destination IP address.

Alternatively, you can create a Network object to show all multicast network IP destinations with these values:

- Name: **MCAST.NET**
- IP: **224.0.0.0**
- Net mask: **240.0.0.0**

You can use one rule for all multicast protocols you agree to accept, as shown in this example:

Source	Destination	VPN	Services & Applications	Action
cluster_all_IPs	fwcluster-object MCAST.NET	Any	vrrp igmp ospf rip	Accept

Configuring Advanced VRRP

Advanced VRRP lets you configure Virtual Routers at the interface level. This section contains only those procedures that are directly related to Advanced VRRP configuration. The general procedures for configuring VRRP clusters are included in the VRRP sections.

With Advanced VRRP, you must configure every Virtual Router to monitor every VRRP interface.

To change from Advanced VRRP to Simplified/Monitored Circuit VRRP:

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 master. Do these steps to delete and add new interfaces with the necessary IP addresses:

1. Cause a failover to the backup.
2. Reduce the priority or disconnect an interface.
3. Delete the Virtual Router on the interface.
4. Create new Virtual Router using the new IP address.
5. Configure the Virtual Router as before.

Configuring Advanced VRRP - WebUI

To add a virtual router:

1. In the **Virtual Routers** section, click **Add**. The **Add New Virtual Router** window opens.
2. In **Virtual Router ID**, select the ID number of the virtual router.
3. In **Interface**, select the interface for the virtual router.
4. In **Priority**, 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 master. The range of values for priority is 1 to 254. The default setting is 100.
5. In **Hello Interval**, select the number of seconds at which the master sends VRRP advertisements. The range is 1-255 seconds (1 is default).

All nodes of a given Virtual Router must have the same hello Interval. If not, VRRP discards the packet and both platforms go to master state.

The hello interval also determines the failover interval; that is, how long it takes a backup router to take over from a failed master. If the master misses three hello advertisements, it is considered to be down because the minimum hello interval is 1 second, therefore the minimum failover time is 3 seconds (3 * Hello_interval).

6. In **Preempt Mode**, if you keep it selected (the default), when the original master fails, a backup system becomes the acting master. When the original master returns to service, it becomes master again.

If you clear it, when the original master fails, a backup system becomes the acting master, and the original does not become master again when it returns to service.

7. In **Auto-deactivation**, if you keep it clear (the default), a virtual router with the lowest priority available (1) can become master if no other Security Gateways exist on the network.

If you select it, the effective priority can become 0. With this priority, the virtual router does not become the master even if there are no other Security Gateways on the network. If you enable Auto-deactivation, 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.

8. For each Virtual Router, a virtual MAC (VMAC) address is assigned to the VIP. The VMAC address is included in all VRRP packet transmissions as the source MAC address. The physical MAC address is not used.

In **VMAC Mode**, select the mode:

- **VRRP**—the default mode. Gaia sets the VMAC to the format outlined in the VRRP protocol specification RFC 3768. It is automatically set to the same value on all nodes of a Virtual Router.
- **Interface**—Gaia sets the VMAC to the MAC address of the local interface. If you select **Interface** mode for both master and backup, the VMAC is different for each. The VRRP IP addresses are associated with different VMACs because they depend on the MAC address of the physical interfaces of the platform that is master at the time.

Note - If you configure different VMACs on the master and backup, you must choose the correct proxy ARP setting for Network Address Translation.

- **Static**—select this mode if you want to set the VMAC address manually. Then enter the 48-bit VMAC address in the Static VMAC text field.
- **Extended**—similar to VRRP mode, except the system dynamically calculates three additional bytes of the interface hardware MAC address to generate a more random address. If you select this mode, Gaia constructs the same MAC address for master and backup platforms within the Virtual Router.

Note - If you set the VMAC mode to interface or static, syslog error messages are displayed when you reboot or at failover, indicating duplicate IP addresses for the master and backup. This is expected behavior since both the master and backup routers temporarily use the same virtual IP address until they resolve into master and backup.

9. In **Authentication**, select **None** or **Simple** password.

You must select the same authentication method for all nodes in the Virtual Router.

10. To add Backup Addresses:

- a) In the **Backup Addresses** section, click **Add** to add a backup address.
The **Add Backup Address** window opens.
- b) In **IPv4 address**, enter the IPv4 address.
- c) Click **Save**. The address shows in the **Backup Address** table.
- d) To remove a backup address, select an address and click **Delete**.
The address is removed from the **Backup Address** table.

11. To configure Monitored interfaces:

- a) In the **Monitored Interfaces** section, click **Add**, to add a backup address.
A warning that this action locks the interface for this virtual route opens.
- b) Click **OK**. The **Add Monitored Interface** window opens.
 - (i) In **Interface**, from the drop-down list, select the interface.
 - (ii) In **Priority delta**, enter the number to subtract from the priority.
This creates an effective priority when an interface related to the backup fails. The range is 1-254.
 - (iii) Click **Save**. The interface and its priority delta show in the **Monitored Interfaces** table.
- c) To edit a monitored interface, select an interface and click **Edit**. The **Edit Monitored Interface** window opens.
 - (i) Enter or select the new priority delta.

(ii) Click **Save**.

- d) To remove a Monitored Interface, select an interface, and click **Delete**.
The interface is removed from the **Monitored Interfaces** table.

12. Click **Save**.

Configuring Advanced VRRP - CLI (vrrp)

Description

Use the `vrrp` command to configure Global and Advanced VRRP settings.

Syntax

Set Commands

```
set vrrp
  coldstart-delay VALUE
  disable-all-virtual-routers on|off
  monitor-firewall on|off
  interface-delay VALUE

set vrrp interface VALUE
  authtype none
  authtype simple VALUE
  monitored-circuit vrid VALUE auto-deactivation VALUE
  monitored-circuit vrid VALUE backup-address VALUE on|off
  monitored-circuit vrid VALUE hello-interval VALUE
  monitored-circuit vrid VALUE monitored-off
  monitored-circuit vrid VALUE monitored-on
  monitored-circuit vrid VALUE monitored-priority-delta VALUE
  monitored-circuit vrid VALUE off
  monitored-circuit vrid VALUE on
  monitored-circuit vrid VALUE preempt-mode VALUE
  monitored-circuit vrid VALUE priority VALUE
  monitored-circuit vrid VALUE vmac-mode default-vmac
  monitored-circuit vrid VALUE vmac-mode extended-vmac
  monitored-circuit vrid VALUE vmac-mode interface-vmac
  monitored-circuit vrid VALUE vmac-mode static-vmac VALUE off
  virtual-router vrid VALUE hello-interval VALUE
  virtual-router vrid VALUE off
  virtual-router vrid VALUE on
  virtual-router vrid VALUE vmac-mode default-vmac
  virtual-router vrid VALUE vmac-mode extended-vmac
  virtual-router vrid VALUE vmac-mode interface-vmac
  virtual-router vrid VALUE vmac-mode static-vmac VALUE
```

Show Commands

```
show vrrp
show vrrp interface VALUE
show vrrp interfaces
show vrrp stats
show vrrp summary
```

Parameters

Parameter	Description
<code>coldstart-delay</code>	Delay period in seconds before a Security Gateway joins a Virtual Router.

Parameter	Description
<code>disable-all-virtual-routers [on off]</code>	on or off. Enable or disable all Virtual Routers on this Security Gateway.
<code>monitor-firewall on off</code>	Monitor Security Gateway status.
<code>interface-delay VALUE</code>	The Interface Delay controls how long to wait 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. Range: 0 - 3600 (seconds) Default: 0 seconds (no delay)
<code>vrrp interface VALUE</code>	The name of the specified Virtual Router interface
<code>authtype simple VALUE</code>	Enter a password to authenticate the Virtual Router.
<code>monitored-circuit vrid</code>	Enter the VRID.
<code>auto-deactivation</code>	on or off. On would create an effective priority 0. A virtual router with 0 priority cannot become a master.
<code>backup-address</code>	The IPv4 address of the backup Security Gateway.
<code>hello-interval</code>	The number of seconds at which the master sends VRRP advertisements. The range is 1-255 seconds (1 is default).
<code>monitored-priority-delta</code>	If an interface associated with a backup address fails, the value of the priority delta is subtracted from the priority to yield an effective priority for the physical router. When the effective priority on the master is less than the priority of another router in the Virtual Router, a new master is selected. The range is 1-254
<code>preempt-mode</code>	on or off. If on, after a failover, the original master becomes master again when returns to service. If off, the backup system that becomes master, remains master. There is no default value.
<code>priority</code>	The router with the higher priority becomes the new master when a failure occurs. The range is 1-254. The default setting is 100.
<code>virtual-router vrid</code>	The virtual router ID number

Configuring VRRP Clusters in SmartConsole

This section includes the procedure for configuring a VRRP cluster object in SmartConsole. Only those procedures that are related to VRRP are shown here.

1. In SmartConsole, create a new cluster object using the **Classic** mode.
2. Enter the VIP as the IP address.
3. On the **Cluster Members** page, add the physical Security Gateways included in the Virtual Router.
4. On the **ClusterXL and VRRP** page, select **High Availability** and then select **VRRP** from the list.
5. Select all of the options in the **Advanced** settings section, including **Use State Synchronization**.
6. On the **Topology** page, configure the cluster and member Security Gateway interfaces as required.
Make sure that you configure the synchronization interfaces.
7. Configure other cluster parameters as necessary.

Troubleshooting VRRP

This section shows known issues with VRRP configurations and fixes. Read this section before contacting Check Point Technical Support (<https://supportcenter.checkpoint.com>).

You can log information about errors and events for troubleshooting VRRP. Enable traces for VRRP.

To enable traces for VRRP:

1. In the WebUI tree, select **Routing > Routing Options**.
2. In the **Trace Options** section, in the **Filter Visible Tables Below** drop down list, select **VRRP**.
3. In the **VRRP** table, select an option, and click **Activate**.

The system restarts the routing subsystem and signals it to reread its configuration. The option you selected, its name and On/Off radio buttons show on the page.

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 nodes of the Virtual Router. You can also manually change the time and time zone on each node to match the other nodes. It must be no more than seconds apart.
- All routers of a Virtual Router must have the same Hello Interval.
- The Priority Delta must be sufficiently large for the Effective Priority to be lower than the master router. Otherwise, when you pull an interface for a Monitored-Circuit VRRP test, other interfaces do not release IP addresses.
- You can use different encryption accelerator cards in two appliances of one Virtual Router or IP cluster (such as the Check Point Encrypt Card in one appliance, and the older Check Point Encryption Accelerator Card in a different appliance). When you do, select encryption/authentication algorithms supported on the two cards. If the encryption/authentication algorithm is supported on the master only, and you use NAT, tunnels

failover incorrectly. If the encryption/authentication algorithm is supported on the master only, without NAT, tunnels are not accelerated after failover.

- Each unique Virtual Router ID must be configured with the same backup address on each gateway.
- The VRRP monitor in the WebUI 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.
- SNMP Get on Interfaces might list the incorrect IP addresses. This results in incorrect Policy. An SNMP Get (for the Firewall object Interfaces in the GUI Security Policy editor) fetches the lowest IP address for each interface. If interfaces are created when the node 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 firewall policies to accept VRRP packets on the Gaia platform. The multicast destination assigned by the IANA for VRRP is 224.0.0.18. If the policy does not accept packets to 224.0.0.18, firewall platforms in one Virtual Router take on Master state.

Monitored-Circuit VRRP in Switched Environments

With Monitored-Circuit VRRP, some Ethernet switches might not recognize the VRRP MAC address after a master to backup change. This is because many switches cache the MAC address related to the Ethernet device attached to a port. When failover to a backup router occurs, the Virtual Router MAC address changes to a different port. Switches that cache the MAC address might not change to the correct 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 that the security platforms are connected to.

It might be not possible to disable the MAC address caching. If so, set the address aging value sufficiently low that the addresses age out each second or two. This causes more overhead on the switch. Therefore, find out if this is a viable option for the model of switch you run.

The Spanning Tree protocol prevents Layer 2 loops across multiple bridges. Spanning-Tree can be enabled on the ports connected to the two sides of a VRRP pair. It can also see multicast Hello Packets come for the same MAC address from two different ports. When the two occur, it can suggest a loop, and the switch blocks traffic from one port. If a port is blocked, no security platforms in the VRRP pair can get Hello Packets from other. In which instance, the two of them enter the master router state.

If possible, turn off Spanning-Tree on the switch to resolve this issue. But, this can have deleterious 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 pair. PortFast causes a port to enter the Spanning-Tree forwarding state immediately, by passing the listening and learning states. The command to enable PortFast is `set spantree portfast 3/1-2 enable`, where 3/1-2 refers to slot 3, ports 1 and 2.

Maintenance

In This Section:

Licenses	177
License Activation	186
Snapshot Image Management	187
Download SmartConsole	191
Hardware Health Monitoring	191
Showing Hardware Information - CLI (show asset)	192
Monitoring RAID Synchronization	194
Shutdown	194
System Configuration Backup	195
Emergendisk	201

This chapter includes procedures and reference information for maintaining your Gaia computer.

Licenses

Licenses can be added or deleted using the:

- **Maintenance > Licenses** page of the WebUI
- Command line by running: `cplic_db_add` ("`cplic db_add`" on page 179) or `cplic del` (on page 180).



Note - While all the SecurePlatform `cplic` commands are available in Gaia, they are not grouped into a Gaia feature. To see a list of available commands and their parameters type `cplic` and press Enter.

Configuring Licenses - WebUI

If you need to obtain a license, visit the User Center (<https://usercenter.checkpoint.com>).

Adding a license:

1. In the tree view, click **Maintenance > Licenses**.
2. Click **New**.
The **Add License** window opens.
3. Enter the license data manually, or click **Paste License** to enter the data automatically.
The **Paste License** button only shows in Internet Explorer. For other browsers, paste the license strings into the empty text field.
4. Click **OK**.

Deleting a license:

1. In the tree view, click **Maintenance > Licenses**.
2. Select a license in the table
3. Click **Delete**.

Configuring Licenses - CLI (cplic)

The `cplic` command and all its derivatives relate to Check Point license management.

Best Practice - Manage licenses in SmartUpdate GUI.

All `cplic` commands are located in `$CPDIR/bin`. License Management is divided into three types of commands:

- *Local licensing commands* are executed on local machines.
- *Remote licensing commands* are commands which affect remote machines are executed on the Security Management Server.
- *License repository commands* are executed on the Security Management Server.

Syntax

Local Licensing:

```
cplic put ...
cplic del [-F <output file>] <signature>
cplic print [-h help] [-n noheader]
           [-x print signatures] [-t type]
           [-F <output file>] [-i <input file>]
           [-p preatures]
           [-D print only Domain licenses]
cplic check ...
cplic contract ...
```

Remote Licensing:

```
cplic put <object name> ...
cplic del <object name> [-F <output file>] <signature>
cplic get <object name | -all>
cplic upgrade -l input file
```

License Database Operations:

```
cplic db_add ...
cplic db_rm <signature>
cplic db_print <object name | -all> ...
```

For help on any command add the `-h` option

cplic check

Description

Confirms that the license includes the feature on the local gateway or Security Management Server.

Syntax

```
gw> cplic check [-p <product>] [-v <version>] [-c|-count] [-t <date>]
[-r|-routers] [-S|-SRusers] <feature>
```

Parameter	Description
<code>-p <product></code>	Product for which license information is requested. For example, <code>fw1</code> , <code>netso</code>
<code>-v <version></code>	Product version for which license information is requested.

Parameter	Description
-c -count	Outputs the number of licenses connected to this feature.
-t <date>	Checks license status on future date. Use the format ddmmmyyyy . A feature can be valid on a given date on one license, but invalid on another.
-r -routers	Checks how many routers are allowed. The <code>feature</code> option is not needed.
-S -SRusers	Checks how many SecuRemote users are allowed.
<feature>	<feature> for which license information is requested.

cplic db_add

Description

Adds one or more licenses to the license repository on the Security Management Server.

When local licenses are added to the license repository, they are automatically attached to the intended Check Point gateway. Central licenses have to undergo the attachment process. This command is a license repository command and can only be executed on the Security Management Server.

Syntax

```
> cplic db_add -l <license-file> [<host>] [<expiration-date>] [<signature>]
[<SKU/features>]
```

Parameter	Description
-l <license-file>	Name of the file that contains the license.
<host>	Security Management Server hostname or IP address.
<expiration-date>	The license expiration date.
<signature>	The license signature string. For example: aa6uwknDc-CE6CRtjhv-zipOVWSnm-z98N7Ck3m The string is case sensitive and the hyphens are optional.
<SKU/features>	The SKU of the license summarizes the features included in the license. For example, CPSUITE-EVAL-3DES-VNG

Example

If the file `192.0.2.11.lic` contains one or more licenses, the command: `cplic db_add -l 192.0.2.11.lic` produces output similar to:

```
Adding license to database ...
```

```
Operation Done
```

cplic db_print

Description

Displays the details of Check Point licenses stored in the license repository on the Security Management Server.

Syntax

```
> cplic db_print <object name | -all> [-n noheader] [-x print signatures] [-t type] [-a attached]
```

Parameter	Description
Object name	Prints only the licenses attached to Object name. Object name is the name of the Check Point Security Gateway object as defined in SmartConsole.
-all	Prints all the licenses in the license repository
-n OR -noheader	Prints licenses with no header.
-x	Prints licenses with their signature.
-t OR -type	Prints licenses with their type: Central or Local.
-a OR -attached	Show which object the license is attached to. Useful if the -all option is specified.

Note - This command is a license repository command and can only run on the Security Management Server.

cplic db_rm

Description

Removes a license from the license repository on the Security Management Server. It can be executed ONLY after the license was detached using the `cplic del` command. Once the license has been removed from the repository, it can no longer be used.

Syntax

```
> cplic db_rm <signature>
```

Parameter	Description
Signature	The signature string within the license.

Example

```
cplic db_rm 2f540abb-d3bcb001-7e54513e-kfyigpwn
```

Note - This command is a license repository command and can only run on the Security Management Server.

cplic del

Description

Deletes a single Check Point license on a host, including unwanted evaluation, expired, and other licenses. Used for both local and remote machines

Syntax

```
> cplic del [-F <output file>] <signature> <object name>
```

Parameter	Description
-F <output file>	Sends the output to <output file> instead of the screen.
<signature>	The signature string within the license.

cplic del <object name>

Description

Detaches a Central license from a Check Point Security Gateway. When this command is executed, the license repository is automatically updated. The Central license remains in the repository as an unattached license. This command can only run on a Security Management Server.

Syntax

```
> cplic del <object name> [-F <outputfile>] [-ip <dynamic ip>] <signature>
```

Parameter	Description
<object name>	The name of the Check Point Security Gateway object as defined in SmartConsole.
-F <outputfile>	Diverts the output to <code>outputfile</code> rather than to the screen.
-ip <dynamic ip>	Deletes the license on the Check Point Security Gateway with the specified IP address. Use this parameter to delete a license on a DAIP Check Point Security Gateway. Note - If this parameter is used, then object name must be a DAIP gateway.
<signature>	The signature string within the license.

Note - This is a Remote Licensing command which affects remote machines that is executed on the Security Management Server.

cplic get

Description

Retrieves all licenses from Security Gateways into the license repository on the Security Management Server. This command helps to synchronize the repository with the Check Point Security Gateways. When the command is run, all local changes are updated.

Syntax

```
> cplic get {<ipaddr>|<hostname>|-all} [-v41]
```

Parameter	Description
<i><ipaddr></i>	The IP address of the Check Point Security Gateway from which licenses are to be retrieved.
<i><hostname></i>	The name of the Check Point Security Gateway object as defined in SmartConsole from which licenses are to be retrieved.
-all	Retrieves licenses from all Check Point gateways in the managed network.
-v41	Retrieves version 4.1 licenses from the NF Check Point gateway. Used to upgrade version 4.1 licenses.

Example

If the Check Point Security Gateway with the object name `caruso` contains four Local licenses, and the license repository contains two other Local licenses, the command `cplic get caruso` produces output similar to the following:

```
Get retrieved 4 licenses.
Get removed 2 licenses.
```

Note - This is a Remote Licensing Command which affects remote machines that is executed on the Security Management Server.

cplic put

Description

Installs one or more local licenses on a local machine.

Syntax

```
> cplic put [-o|-overwrite] [-c|-check-only] [-s|-select] [-F <output file>]
[-P|-Pre-boot] [-k|-kernel-only] -l <license-file> [<host>] [<expiration date>]
[<signature>] [<SKU/feature>]
```

Parameter	Description
-o -overwrite	On a Security Management Server this erases all existing licenses and replaces them with the new licenses. On a Check Point Security Gateway this erases only the local licenses but not central licenses that are installed remotely.
-c -check-only	Verifies the license. Checks if the IP of the license matches the machine and if the signature is valid.
-s -select	Selects only the local license whose IP address matches the IP address of the machine.
-F <outputfile>	Outputs the result of the command to the designated file rather than to the screen.
-P -Pre-boot	Use this option after you have upgraded and before you reboot the machine. Use of this option will prevent certain error messages.

Parameter	Description
-K -kernel-only	Pushes the current valid licenses to the kernel. For support use only.
-l <license-file>	Name of the file that contains the license.
<host>	Security Management Server hostname or IP address.
<expiration-date>	The license expiration date
<signature>	The license signature string. For example: aa6uwknDc-CE6CRtjhv-zipOVWSnm-z98N7Ck3m (The string is case sensitive and the hyphens are optional).
<SKU/features>	The SKU of the license summarizes the features included in the license. For example: CPMSUITE-EVAL-3DES-vNG

Note - Copy and paste the following parameters from the license received from the User Center.

- **host** - One of the following:
 - **All platforms** - The IP address of the external interface (in dot notation). The last part cannot be 0 or 255.
 - **Solaris2** - The response to the `hostid` command (beginning with 0x).
- **expiration date** - The license expiration date. It can be `never`
- **signature** - The license signature string.
For example: aa6uwknDc-CE6CRtjhv-zipOVWSnm-z98N7Ck3m (Case sensitive. The hyphens are optional.)
- **SKU/features** - A string listing the SKU and the Certificate Key of the license. The SKU of the license summarizes the features included in the license. For example:
CPMP-EVAL-1-3DES-NG CK0123456789ab

Example

`cplic put -l 215.153.142.130.lic` produces output similar to the following:

```
Host      Expiration SKU
215.153.142.130 26Dec2001 CPMP-EVAL-1-3DES-NG CK0123456789ab
```

cplic put <object name> ...

Description

Attaches one or more central or local licenses remotely. When this command is executed, the license repository is also updated.

Syntax

```
> cplic put <object name> [-ip dynamic ip] [-F <output file>]
-l <license-file> [<host>] [<expiration date>] [<signature>] [<SKU/feature>]
```

Parameter	Description
<code>object name</code>	The name of the Check Point Security Gateway object, as defined in SmartConsole.
<code>-ip dynamic ip</code>	Installs the license on the Check Point Security Gateway with the specified IP address. This parameter is used for installing a license on a DAIP Check Point gateway. Note - If this parameter is used, then the object name must be a DAIP Check Point gateway.
<code>-F <outputfile></code>	Diverts the output to <code><outputfile></code> rather than to the screen.
<code>-l <license-file></code>	Installs the licenses from <code><license-file></code> .
<code>-l <license-file></code>	Name of the file that contains the license.
<code><host></code>	Security Management Server hostname or IP address.
<code><expiration-date></code>	The license expiration date.
<code><signature></code>	The license signature string. For example: <code>aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m</code> The string is case sensitive and the hyphens are optional.
<code><SKU/features></code>	The SKU of the license summarizes the features included in the license. For example: <code>CPSUITE-EVAL-3DES-vNG</code>

Note - This is a remote licensing command which affects remote machines. It is executed on the Security Management Server.

Copy and paste the following parameters from the license received from the User Center. More than one license can be attached.

- `host` - The target hostname or IP address.
- `expiration date` - The license expiration date. It can be `never`
- `signature` - The license signature string. For example:
`aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m` (Case sensitive. The hyphens are optional)
- `SKU/features` - A string listing the SKU and the certificate key of the license. The SKU of the license summarizes the features included in the license. For example:
`CPMP-EVAL-1-3DES-NG CK0123456789ab`

cplic print

Description

The `cplic print` command, located in `$CPDIR/bin`, prints details of Check Point licenses on the local machine.

Syntax

```
> cplic print [-n|-noheader][-x prints signatures][-t type][-F <outputfile>]
[-p preatures]
```

Parameter	Description
-n -noheader	Prints licenses with no header.
-x	Prints licenses with their signature.
-t -type	Prints licenses showing their type: Central or Local.
-F <outputfile>	Diverts the output to <code>outputfile</code>
-p -preatures	Prints licenses resolved to primitive features.

Note - On a Check Point gateway, this command prints all licenses that are installed on the local machine, both local and central licenses.

cplic upgrade

Description

Upgrades licenses in the license repository with licenses in a license file from the user center.

Syntax

```
> cplic upgrade -l <inputfile>
```

Parameter	Description
-l <inputfile>	Upgrades the licenses in the license repository and Check Point gateways to match the licenses in <inputfile>.

Example

This example explains the procedure to upgrade the licenses in the license repository. There are two Software Blade licenses in the file. One does not match any license on a remote gateway, the other matches a version NGX license on a gateway that has to be upgraded.

- Upgrade the Security Management Server to the latest version.
Ensure that there is connectivity between the Security Management Server and the Security Gateways with the previous product versions.
- Import all licenses into the license repository. This can also be done after upgrading the products on the remote gateways.
- Run the command: `cplic get -all`
For example:
Getting licenses from all modules ...
count:root(su) [~] # cplic get -all
golda:
Retrieved 1 licenses.
Detached 0 licenses.
Removed 0 licenses.

```
count:
Retrieved 1 licenses.
Detached 0 licenses.
Removed 0 licenses.
```

- To see all the licenses in the repository, run the command `cplic db_print -all -a`

```
count:root(su) [~] # cplic db_print -all -a
Retrieving license information from database ...
The following licenses appear in the database:
=====
Host          Expiration Features
192.0.2.11    Never      CPFW-FIG-25-53      CK-49C3A3CC7121 golda
192.0.2.11    26Nov2012 CPSUITE-EVAL-3DES-NGX CK-1234567890 count
```
- In the User Center <http://usercenter.checkpoint.com>, view the licenses for the products that were upgraded from version NGX to a Software Blades license. You can also create new upgraded licenses.
- Download a file containing the upgraded licenses. Only download licenses for the products that were upgraded from version NGX to Software Blades.
- If you did not import the version NGX licenses into the repository, import the version NGX licenses now. Use the command `cplic get -all`
- Run the license upgrade command: `cplic upgrade -l <inputfile>`
 - The licenses in the downloaded license file and in the license repository are compared.
 - If the certificate keys and features match, the old licenses in the repository and in the remote Security Gateways are updated with the new licenses.
 - A report of the results of the license upgrade is printed.

Note - This is a remote licensing command which affects remote Security Gateways. It is executed on the Security Management Server.

For more about managing licenses, see the R80.10 *Installation and Upgrade Guide* <http://downloads.checkpoint.com/dc/download.htm?ID=54829>.

License Activation

A license can be activated online or offline. Appliances with Internet connectivity and access to the Check Point User Center automatically fetch the license.

- A license check takes place immediately on a newly installed Security Management Server and continues until a license is attached.
- On a Security Gateway, a license check takes place before establishing SIC with the management server. If the gateway has Internet connectivity, a license is fetched. If no connectivity exists, automatic activation attempts continue after SIC is established until the gateway is activated.

To manually activate a license Online:

1. Open the **Gaia WebUI**.
2. If necessary, configure a proxy on the **System Management > Proxy** page.
3. Open **Maintenance > License Status**.
4. Click **Activate Now**.

Gaia fetches the license, the status changes to *Activated*. Available blades populate the table. If the appliance does not have access to the Internet or User Center, you can manually activate the license if you have the license string.

To manually activate a license offline:

1. Open the **Gaia WebUI**.
2. Open **Maintenance > License Status**.
3. Click **Offline Activation**.
4. Click **New**.
5. Paste the license string into the **Add License** window.

The above activation procedures are relevant for these Gaia appliances:

- 2200
- 3000
- 4000
- 5000
- 12000
- 13000
- 15000
- 21000
- 23000
- TE Appliances
- Smart-1

To delete a license:

1. Open the **Gaia WebUI**.
2. Open **Maintenance > License Status**.
3. Click **Offline Activation**.
4. Select the license.
5. Click **Delete**.

Snapshot Image Management

A snapshot is a backup of the system settings and products. It includes:

- File system, with customized files
- System configuration (interfaces, routing, hostname, and similar)
- Software Blades
- Management database (on a Security Management Server or a Multi-Domain Server)

A snapshot is very large. A snapshot includes the entire root partition and some of the `/var/log` partition and other important files. For this reason, snapshots cannot be scheduled the same way that Backups can. Backup and Restore is the preferred method of recovery.

Note -

- When Gaia creates a snapshot, all system processes and services continue to run. Policy enforcement is not interrupted.
- You can import a snapshot created on a different release or on this release. You must import it to the same appliance or open server hardware model.
- After importing the snapshot, you must activate the device license from the WebUI or the User Center.

Snapshot options:

- **Revert** to a user created image.
- **Revert** to a factory default image, which is automatically created on Check Point appliances by the installation or upgrade procedure.
- **Delete** an image from the local system.
- **Export** an existing image. This creates a compressed version of the image. You can download the exported image to a different computer and delete the exported image from the Gaia computer. This saves disk space. You must not rename the exported image. If you rename a snapshot image, it is not possible to revert to it.
- **Import** an exported image.
- **View** a list of images that are stored locally.

IMPORTANT: Before using Snapshot image management, see the known limitations <http://supportcontent.checkpoint.com/solutions?id=sk98068>.

Best Practice -**Create Snapshots:**

- Immediately after Gaia installation and first-time configuration.
- Before making a major system change, such as installing a Jumbo Hotfix or route changes.

It is not recommended to use snapshots as a way of regularly backing up your system. System Backup is the preferred method ("[Backing up the System](#)" on page 37). Schedule system backups on a regular basis, daily or weekly, to preserve the Gaia OS configuration and firewall database.

Snapshot Prerequisites

Before you create a snapshot image, consider these prerequisites:

- To create the snapshot image requires free space on the disk. The required free disk space is the size of the system root partition multiplied by 1.15.

Note - A snapshot is created in unallocated space on the disk. Not all of the unallocated space on a disk can be used for snapshots. To find out if you have enough free space for snapshots:

- a) Open a command line on the gateway or Security Management Server.
- b) In clish, run: `show snapshots`.

The output shows the amount of space on the disk available for snapshots. The value does not represent all of the unallocated space on the disk.

- The free space required in the export file storage location is the size of the snapshot multiplied by two.

- The minimum size of a snapshot is 2.5G. Therefore, the minimum available space necessary in the export file storage location is 5G.

Working with Snapshot Management - WebUI

Before you create a snapshot image, make sure the appliance or storage destination meets the prerequisites.

To create a snapshot:

1. In the tree view, click **Maintenance > Snapshot Management**.
2. Click **New**. The **New Image** window opens.
3. In the **Name** field, enter a name for the image.
4. Optional: In the **Description** field, enter a description for the image.
5. Click **OK**.

To restore a snapshot:

1. In the tree view, click **Maintenance > Image Management**.
2. Select an image.
3. Click **Revert**. The **Revert** window opens.
Note - Pay close attention to the warnings about overwriting settings, the credentials, and the reboot and the image details.
4. Click **OK**.

To delete a snapshot:

1. In the tree view, click **Maintenance > Snapshot Management**.
2. Select an image.
3. Click **Delete**. The **Delete Image** window opens.
4. Click **Ok**.

To export a snapshot:

1. Make sure that there is enough disk space in: `/var/log`
2. In the tree view, click **Maintenance > Snapshot Management**.
3. Select an image.
4. Click **Export**. The **Export Image (name)** window.
5. Click **Start Export**.

To import an image:

1. In the tree view, click **Maintenance > Snapshot Management**.
2. Select an image.
3. Click **Import**. The **Import Image** window opens.
4. Click **Browse** to select the import file for upload.
5. Click **Upload**.
6. Click **OK**.



Note - You must not rename the exported image. If you rename a snapshot image, it is not possible to revert to it.

Working with Snapshot Management - CLI (snapshot)

Before you create a snapshot image, make sure the appliance or storage destination meets the prerequisites.

Description Manage system images (snapshots)

Syntax

To make a new image:
add snapshot VALUE desc VALUE

To delete an image
delete snapshot VALUE

To export or import an image, or to revert to an image:
set snapshot export VALUE path VALUE name VALUE
set snapshot import VALUE path VALUE name VALUE
set snapshot revert VALUE

To show image information
show snapshot VALUE all
show snapshot VALUE date
show snapshot VALUE desc
show snapshot VALUE size
show snapshots

Parameters

Parameter	Description
snapshot VALUE	Name of the image.
desc VALUE	Description of the image.
snapshot export VALUE	Name of the image to export.
snapshot import VALUE	Name of the image to import.
name VALUE	The storage location for the exported image on the local file system. For example: /var/log/
all	All image details

Examples:

```
add snapshot snap1 desc first_image_after_installation
set snapshot export snap1 path /home/admin/ name first_image_after_installation
```

Comments

You must not rename the exported image. If you rename a snapshot image, it is not possible to revert to it.

Factory default images are created automatically when you install or upgrade an appliance to another release. You can restore your Check Point appliance to the factory default image for a specified release.

Note - This procedure overwrites all current configuration settings. We recommend that you create a backup image before you restore a factory default image.

To restore a factory default image:

1. From your appliance command line, run:
`set fcd revert <default_image_name>`
2. Follow the instructions on the screen.
3. Restart the appliance.

Download SmartConsole

You can download the SmartConsole application package from a Gaia Security Management Server to your WebUI client computer. After downloading the package you can install it and use it to connect to the Security Management Server.

Download SmartConsole - WebUI

To download the Check Point SmartConsole applications installation package:

1. In the tree view, select one of:
 - **Overview**. At the top of the page, click **Download Now!**
 - **Maintenance > Download SmartConsole**.
2. Click **Download**.

Hardware Health Monitoring

You can monitor these hardware elements:

- Fan sensors—Shows the fan number, status, and value.
- System Temperature sensor
- Voltage sensors
- Power Supply (on machines that support it)

Showing Hardware Health Monitoring Information - WebUI

In the navigation tree, click **Maintenance > Hardware Health**.

You can see the status of the machine fans, system temperature, the voltages, and (for supported hardware only) the power supply.



Note - The **Hardware Health Monitoring** page only appears for supported hardware.

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 Monitoring Information - CLI (sysenv)

Description

These commands display the status for various system components. Components for which the status can be displayed include temperature, voltage, power supplies, and fans. The command returns status only for installed components.

Syntax

To display all system status information:

```
show sysenv all
```

To display all system component information:

```
show sysenv fans
show sysenv ps
show sysenv temp
show sysenv volt
```

Parameters

Parameter	Description
ps	Power Supply (for supported hardware only)

Example

```
show sysenv all
```

Output

```
gw-3002f0> 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

Showing Hardware Information - CLI (show asset)

Description

Shows information about the hardware on which Gaia is installed. The information shown depends

on the type of hardware. Common types of information shown are:

- Serial number
- Amount of physical RAM
- CPU frequency
- Number of disks in the system
- Disk capacity

Syntax

```
show asset all
show asset TAB
show asset <category name>
```

Parameters

Parameter	Description
all	Show all available hardware information. The information shown depends on the type of hardware.
TAB	Show a list of asset categories, such as <code>system</code> and <code>disk</code> . The available categories depend on the type of hardware.
<category name>	Show available information for a specific category

Example 1

```
clish> show asset TAB
```

Output 1

```
system all
```

Example 2

```
clish> show asset all
```

Output 2

```
Platform: Check Point 4400
Serial Number: abcdefghijklmn
CPU Frequency: 2600Mhz
Disk Size: 250GB
```

Monitoring RAID Synchronization

In R80.10, you can monitor the RAID status of the disks to see when the hard disks are synchronized. If you reboot the appliance before the hard disks are synchronized, the synchronization starts again at the next boot.

Showing RAID Information - WebUI

To monitor the RAID status of the disks - WebUI:

In the navigation tree, click **Maintenance > RAID Monitoring**.

RAID Volumes and **RAID Volume Disks** information shows.

Showing RAID Information - CLI

To monitor the RAID status of the disks - CLI:

Run one of these commands:

- `raid_diagnostic`

This shows data about the RAID and hard disks, with the percent synchronization done.

This is an example output for Smart-1 225. DiskID 0 is the left hard disk. DiskID 1 is the right hard disk.

```
Expert@cpmodule1#raid_diagnostic
Raid Status:
VolumeID:0 RaidLevel: RAID-1 NumberOfDisks:2 RaidSize:465GB State:DEGRADED Flags: ENABLED RESYNC _IN_PROGRESS
DiskID:0 DiskNumber:0 Vendor:ATA ProductID:<HDD Model> Size:465GB State:ONLINE Flags:NONE
DiskID:1 DiskNumber:1 Vendor:ATA ProductID:<HDD Model> Size:465GB State:INITIALIZING Flags:OUT_OF_SYNC SyncState: 12%
```

- `cpstat os -f raidInfo`

This shows almost the same information as the `raid_diagnostic` command, in tabular format.

Shutdown

There are two ways to shut down:

- **Reboot:** Shut down the system and then immediately restart it.
- **Halt:** Shut down the system.

Shutting Down - WebUI

To shut down the system and then immediately restart it:

1. In the tree view, click **Maintenance > Shut Down**.
2. Click **Reboot**.

To shut down the system:

1. In the tree view, click **Maintenance > Shut Down**.
2. Click **Halt**.

Shutting Down - CLI (halt, reboot)

To shut down the system and then immediately restart it:

Run the `reboot` command.

To shut down the system:

Run the `halt` command.

System Configuration Backup

- Back up the configuration of the Gaia operating system and of the Security Management Server database. You can restore a previously saved configuration. The configuration is saved to a .tgz file. You can store backups locally, or remotely to a TFTP, SCP or FTP server. You can run the backup manually or on a schedule.
- Save your Gaia system configuration settings as a ready-to-run CLI script. This lets you quickly restore your system configuration after a system failure or migration.



Notes -

- You can only do a migration using the same Gaia version on the source and target computers.
- When you do a backup for a Security Management Server, make sure to close all SmartConsole clients. Otherwise, the backup does not start.

Backing Up and Restoring the System - WebUI

To add a backup:

1. In the tree view, click **Maintenance > System Backup**
2. Click **Add Backup**.

The **New Backup** window opens.

3. Select the location of the backup file:
 - **This appliance**
 - **TFTP server**. Specify the IP address.
 - **SCP server**. Specify the IP address, user name and password.
 - **FTP server**. Specify the IP address, user name and password.

Note - Gaia does not support change of file names. You can change a file name in your file system. Make sure not to use special characters.

To restore from a backup:

1. In the tree view, click **Maintenance > System Backup**.
2. Select the backup file and click **Restore Backup**.

To delete a backup

1. In the tree view, click **Maintenance > System Backup**.

2. Select the backup file and click **Delete**.

Backing Up and Restoring the System - CLI (Backup)

Description

Create and save the system's configuration.

Syntax

```
add backup {local | tftp ip <ip>|{ftp | scp} ip <ip> username <name> password plain}
```

Parameters

Parameter	Description
local	Save the backup locally, to /var/CPbackup/backups/
ip	The IP address of the remote server.
username	User name required to log in to the remote FTP or SCP server.
password plain	At the prompt, enter the password for the remote FTP or SCP server.

Output

```
gw> add backup local
Creating backup package. Use the command 'show backups' to monitor creation progress.
```

```
gw> show backup status
Performing local backup
```

```
gw> show backups
backup_gw-8b0891_22_7_2012_14_29.tgz Sun, Jul 22, 2012 109.73 MB
```

Note - Gaia does not support change of file names. You can change a file name in your file system. Make sure not to use special characters.

Restoring a Configuration

Description Use these commands to restore the system's configuration from a backup file.

Syntax**To restore a backup from a locally held file:**

```
set backup restore local <TAB>
```

To restore a backup from a remote server using FTP:

```
set backup restore ftp ip VALUE file VALUE username VALUE password plain
```

To restore a backup from a remote server using TFTP:

```
set backup restore tftp ip VALUE file VALUE
```

To restore a backup from a remote server using SCP:

```
set backup restore scp ip VALUE file VALUE username VALUE password plain
```

Parameters

Parameter	Description
local <TAB>	The <TAB> does an auto-complete on the name and location of the backup file.
ip VALUE	The IP address of the remote server.
file VALUE	The location and name of the file on the remote server.
username VALUE	User name required to log in to the remote server.
password plain	At the prompt, enter the password for the remote server.

Comments To apply the new configuration, you must reboot.



Note - To quickly restore the Gaia OS configuration after a system failure or migration, use the configuration ("[Working with System Configuration - CLI \(configuration\)](#)" on page 200) feature.

To monitor the creation of a backup: `show backup status`

To see the status of the last backup: `show backups`

Configuring Scheduled Backups - WebUI

Note - When you do a backup for a Security Management Server, make sure to close all SmartConsole clients. Otherwise, scheduled backup does not start.

To add a scheduled backup:

1. In the tree view, click **Maintenance > System Backup**.
2. Click **Add Scheduled Backup**. The **New Scheduled Backup** window opens.
3. In **Backup Name**, enter the name of the job. Use alphanumeric characters only, and no spaces.
4. In **Backup Type**, enter the location of the backup file.
 - **This appliance**

- **TFTP server.** Specify the IP address.
 - **SCP server.** Specify the IP address, user name and password.
 - **FTP server.** Specify the IP address, user name and password.
5. In **Backup Schedule**, select the frequency (**Daily, Weekly, Monthly**) for this backup. Where relevant, enter the **Time** of day for the job, in the 24 hour clock format.
 6. Click **Add**. The scheduled backup shows in the **Scheduled Backups** table.

To delete a scheduled backup:

1. In the tree view, click **Maintenance > System Backup**.
2. In the **Scheduled Backups** table, select the backup to delete.
3. Click **Delete**.

Configuring Scheduled Backups - CLI (backup-scheduled)

Note - When you do a backup for a Security Management Server, make sure to close all SmartConsole clients. Otherwise, scheduled backup will not start.

Description Configure a scheduled backup of the system configuration

Syntax

To add a scheduled backup locally:

```
add backup-scheduled name VALUE local
```

To add a scheduled backup on a remote server using FTP:

```
add backup-scheduled name VALUE ftp ip VALUE username VALUE password plain
```

To add a scheduled backup on a remote server using SCP:

```
add backup-scheduled name VALUE scp ip VALUE username VALUE password plain
```

To add a scheduled backup on a remote server using TFTP:

```
add backup-scheduled name VALUE tftp ip VALUE
```

To configure a daily backup schedule:

```
set backup-scheduled name VALUE recurrence daily time VALUE
```

To configure a monthly backup schedule:

```
set backup-scheduled name VALUE recurrence monthly month VALUE days VALUE time VALUE
```

To configure a weekly backup schedule:

```
set backup-scheduled name VALUE recurrence weekly days VALUE time VALUE
```

To show the details of the scheduled backup:

```
show backup-scheduled VALUE
```

To delete a scheduled backup:

```
delete backup-scheduled VALUE
```

Parameters

Parameter	Description
name VALUE	The name of the scheduled backup
ip VALUE	The IP address of the FTP, TFTP, or SCP remote server
username VALUE	User name required to log in to the remote server
backup-scheduled VALUE	The name of a scheduled backup
password plain	At the prompt, enter the password for the remote server
recurrence daily time	To specify a job for once a day, enter recurrence daily time, and the time of day, in the 24 hour clock format. For example: 14:00.
recurrence monthly month	To specify a job for once a month, enter recurrence monthly month, and the specific months. Each month by number, and separate by commas. For example: for January through March, enter 1,2,3

recurrence weekly days	To specify a job for once a week, enter recurrence weekly, and the day by number, when 0 is Sunday and 6 is Saturday.
time	To specify the time, enter the time in the twenty four hour clock format. For example: 14:00.
days	When the recurrence is weekly: To specify the days, enter the day by number: 0 is Sunday and 6 is Saturday. When the recurrence is monthly: To specify the days, enter the day by number: 1 to 31. Separate several days with commas. For example: for Monday and Thursday enter 1,4

Working with System Configuration - CLI (configuration)

You can save your Gaia system configuration settings as a ready-to-run CLI script. This feature lets you quickly restore your system configuration after a system failure or migration.



Note - You can only do a migration using the same Gaia version on the source and target computers.

To save the system configuration to a CLI Script, run:

```
save configuration <script name>
```

To restore configuration settings, run:

```
load configuration <script name>
```

<script name> - Name of the script file.

To see the latest configuration settings, run:

```
show configuration
```

This example shows part of the configuration settings as last saved to a CLI script:

```
mem103> show configuration
#
# Configuration of mem103
# Language version: 10.0v1
#
# Exported by admin on Mon Mar 19 15:06:22 2012
#
set hostname mem103
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

```

Emergendisk

Emergendisk is a set of tools on a removable USB device for emergency password recovery and file system access. You can use an Emergendisk bootable USB device on all Check Point appliances and Open Servers.

You can create an Emergendisk removable device that contains these tools:

- **Password recovery** - If you forget your administrator password, you can restore the initial system administrator username and password (admin/admin).
- **System Recovery** - If the Gaia system does not boot up, use the `emergendisk` tool to boot Gaia from the removable device. You can also use `emergendisk` to see the file system as it was when Gaia was installed. You can then copy files to the damaged system.
- **Disk Erasure** - Use the DBAN open source tools to securely erase a hard disk. The dban.org site gives this description of the tools: "Darik's Boot and Nuke ("DBAN") is a self-contained boot floppy that securely wipes the hard disks of most computers. DBAN is appropriate for bulk or emergency data destruction."

This is the Emergendisk menu:

```

+-----+
|                                     |
|                               Rescue USB Drive                               |
|-----+-----+
| Boot EmergenDisk with console                                             |
| Reset Admin Password                                                       |
| Boot EmergenDisk with vga                                                 |
| Darik's Boot and Nuke (DBAN)                                             |
| Boot from local drive                                                     |
|-----+-----+
+-----+

```

Press [Tab] to edit options

Creating the Emergendisk Removable Device

Emergendisk is a set of tools on a removable USB device for emergency password recovery and file system access. An Emergendisk bootable USB device can be used on all Check Point appliances and Open Servers.

To create the Emergendisk:

1. At the CLI, type `expert` and then your `expert` password.
2. Insert a removable device into the USB port on the Gaia computer.
3. Run:
`emergendisk`
4. Select the removable device.

A warning message shows:

```
Warning! all data will be lost from device
Are you sure you want to continue [yes/no]?
```

5. Type yes

The device is formatted and files are copied. A progress bar shows.

After some minutes a success message appears:

```
Emergendisk created successfully
```

Booting from the Emergendisk Removable Device

If the Gaia system does not boot up, use the `emergendisk` tool to boot Gaia from the removable device. You can also use `emergendisk` to see the file system as it was when Gaia was installed. You can then copy files to the damaged system.

To boot from the Emergendisk removable device:

1. At the CLI, type `expert` and then your expert password.
2. Insert the Emergendisk removable device into the USB port on the Gaia computer.
3. Reboot. At the prompt, type
`reboot`

The Emergendisk menu shows.

4. Select one of these options:
`Boot emergendisk with VGA`
`Boot emergendisk with console`

After the reboot, you are in the USB file system. You can see the files system on the Gaia computer in the `/mnt/hdd` directory.

Note - When using an Emergendisk removable device that was created on a different Gaia computer, it may fail to mount the local file system.

Resetting the Administrator Password

If you forget your administrator password, you can restore the initial system administrator username and password (`admin/admin`).

To reset the administrator password:

1. At the CLI, type `expert` and then your expert password.
2. Insert the removable device into the USB port on the Gaia computer.
3. At the prompt, type:
`reboot`

After the reboot, the Emergendisk menu shows.

4. Select the option:
`Reset Admin Password`

Console messages show. After some minutes, this message shows:

```
Admin password successfully reset
Please remove disk or any other media and press enter to restart
```

5. Remove the removable device from the USB port.

6. Press Enter to reboot

The administrator username/password is admin/admin.

Irrecoverably Erasing Data using DBAN

Use the DBAN open source tools to securely erase a hard disk. The dban.org site gives this description of the tools: "Darik's Boot and Nuke ("DBAN") is a self-contained boot floppy that securely wipes the hard disks of most computers. DBAN is appropriate for bulk or emergency data destruction."

To Erase the Disk of the DBAN tools:

1. At the CLI, type `expert` and then your expert password.
2. Insert the removable device into the USB port on the Gaia computer with the disk to erase.
3. At the prompt, type `reboot`

After the reboot, the Emergendisk menu opens.

4. Select this option:
Darik's Boot and Nuke (DBAN)
5. The DBAN menu shows the different ways to erase the disk.

Press [Tab] to edit options

```
+-----+
|
|
+-----+
| autonuke
| dban
| dod
| dod3pass
| dodshort
| gutmann
| ops2
| paranoid
| prng
| quick
| zero
| nofloppy
|
+-----+
```

6. Select the required option.

CPUSE

In This Section:

Configuring a CPUSE Policy - WebUI	204
Configuring CPUSE Mail Notifications - WebUI	205
Configuring CPUSE - WebUI	206
Reviewing CPUSE – clish.....	207

Note - The *Software Updates* feature was renamed to *Check Point Upgrade Service Engine* [CPUSE] in R77.20.

With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself. The software update packages and full images are for major releases, minor releases and Hotfixes. All of the CPUSE processes are handled by the Deployment Agent daemon (DA).

Gaia automatically locates and shows the available software update packages and full images that are relevant to the Gaia operating system version installed on the computer, the computer's role (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, located on the Check Point Support Center, that is only available to limited audiences.

When you update Check Point software, make sure to:

- Define the CPUSE policy for downloads and installation.
Downloads can be:
 - Manual
 - Automatic
 - Scheduled (daily, weekly, monthly, or once only).Installations are:
 - Hotfixes are downloaded and installed automatically by default
 - Full installation and upgrade packages must be installed manually
- Define mail notifications for completed package actions and for the new package updates.
- Run the software download and installation.

Configuring a CPUSE Policy - WebUI

To define the CPUSE policy:

1. In the WebUI, go to the **Upgrades (CPUSE) > Software Updates Policy** page.
2. In the **Software Deployment Policy > Download Hotfixes** section, select the method to download Hotfixes:
 - **Manually** (default) - initiated through WebUI or in clish
 - **Scheduled** - at a certain time **Daily**, **Weekly** (select day of the week), **Monthly** (select day of the month), or **Once** (select a date)
 - **Automatic** - as they become available

CPUSE checks for updates every three hours while the computer is on, immediately after the computer boots up, and at the time of access of the Upgrades (CPUSE) page in WebUI.

Note - Full installation packages can only be downloaded manually.

3. To help Check Point collect download and installation statistics that are used only to improve the CPUSE service, select **Send download and installation data of Software Updates to Check Point**.
 4. Select **Self tests to perform** for sanity checks, after installing or upgrading with CPUSE:
 - **Start Check Point Processes** - To make sure that Check Point processes are running
 - **Install Policy** - To make sure that it is possible to install a policy
 - **Network Link Up** - To make sure that the network interfaces on the Gaia computer that were up before the upgrade, are up after it
 5. Select **Self Test - Auto-rollback upon failure** to run a fall-back procedure if the installed package fails one of the sanity tests. The fall-back procedure automatically restores the version that was active before the package was installed, and sends a notification that the installation failed
- Note** - If this option is not selected, only the notification is sent.
6. Select **Periodically update new Deployment Agent version**, to keep the Deployment Agent up to date.
 7. Click **Apply**.

Configuring CPUSE Mail Notifications - WebUI

You can be notified by email of these software update events:

- New packages in the Check Point Support Center that are available for download
- Packages that have been downloaded to the Gaia computer
- Package installation success or failure

To configure CPUSE notifications:

1. In the WebUI, go to the **Upgrades (CPUSE) > Software Updates Policy** page.
2. Click **Add**.

Note - You must have the **Mail Server** and the **User Name** of the sender of the CPUSE notifications configured in the **System Management > Mail Notification** page, before you can configure **Mail Notifications**. Otherwise, the **Add** action for **Mail Notifications** is disabled.
3. Enter a notification recipient's **Email address**, and select the types of notification they will receive:
 - **New Available Packages**
 - **Download Status**
 - **Install Status**
4. Click **OK**.

Configuring CPUSE - WebUI

If you configure the Upgrades (CPUSE) policy and mail notifications before you download and run an upgrade, you will receive these email notifications, depending on your configuration:

- **New Available Packages** - When a package becomes available for download from the Check Point Support Center
- **Download Status** - When an upgrade package or a full installation image is downloaded and available for installation
- **Install Status** - When an upgrade or a new installation is finished

If a package fails to download or install, an email notification is also sent.

To manually download an installation and upgrade package:

1. In the **Upgrades (CPUSE) > Status and Actions** page, select a package with the status **Available for Download**.
2. Click **Download**.

When the package is downloaded successfully, the package status changes to **Downloaded Successfully**. If the download fails, the status changes to **Download Failed**. An appropriate email notification is sent.

To manually download a Hotfix package:

1. In the **Upgrades (CPUSE) > Status and Actions** page, select a package with the status **Available for Download**.
2. Click **More** and select **Download**.

When the package is downloaded successfully, the status changes to **Downloaded Successfully**. If the download fails, the status changes to **Download Failed**. An appropriate email notification is sent.

To manually install a Hotfix or an installation and upgrade package:

1. In the **Upgrades (CPUSE) > Status and Actions** page, select a package with the status **Downloaded Successfully** or **Available to Download**.
2. **Optional:** To make sure that the package can be used to do an installation or upgrade, click **More > Verifier**.
This action checks for available disk space and makes sure that the upgrade is valid and that there is no conflict between the new Hotfix or installation/upgrade package and previously installed Hotfixes.
3. Install or upgrade:
 - To install a Hotfix package, select a Hotfix and click **Install Update**.
 - To do a clean installation of a full image on a new partition with no configuration migration, select a package and click **Clean Install**
 - To upgrade using a full image, select a package and click **Upgrade**.

When the package is installed on the Gaia computer, the package status changes to **Installed** and an email notification is sent.

To add a private package to the list of available package:

You can add a private package to the list of available packages. A private package is a Hotfix, located on the Check Point Support Center, that is only available to limited audiences.

1. In the **Upgrades (CPUSE) > Status and Actions** page, click **Add hotfixes from the cloud**.
2. In the window that opens, insert the search string that you received from Check Point Support and click search.
3. When the package is found, click the package name.
The package is added to the list of packages.

If on your local drive you have a CPUSE-compatible package that you copied from another gateway or from the Check Point Download Center, you can add it to the list of available packages.

Note - You can only import CPUSE-compatible packages.

To import a package from your local drive to the list of available packages:

1. In the **Upgrades (CPUSE) > Status and Actions** page, from the toolbar, select **Import Package**.
2. In the window that opens, browse to the package on your computer and click **Import**.
3. Click **OK**.
The package is added to the list of packages.

By default, all packages are shown in the **Package** list. You can filter the list of packages to only see those that are recommended or installed.

To filter the list of packages:

In the **Upgrades (CPUSE) > Status and Actions** page, click **Showing Recommended Packages** and select an option:

- **Recommended** (default)
- **Installed**
- **All**

Reviewing CPUSE – clish

Description

Show information about the Deployment Agent:

- The mail notifications configuration
- The CPUSE policy for downloads and installation
- The Deployment Agent status, Deployment Agent build number, the connection status, and the current update status
- The packages that are available for download, downloaded, imported, installed, and recommended by Check Point
- The details of a specific package - the display name, description, size, type, status, reboot requirement, Check Point recommendation, components contained, packages containing it, download date/time, import date/time, installation date/time, and installation log location

Syntax

```
show installer {mail-notifications {<num> | <email>} | package <num> |
packages {all | available-for-download | downloaded | imported | installed
| recommended} | policy {all | downloads | periodically-self-update |
self-test {all | auto-rollback | install-policy | network-link-up |
```

```
start-processes} | send-cpuse-data} | status {agent | all | build | connection  
| license | update-from-cloud}}
```

Parameters

Parameter	Description
mail-notifications {<num> <email>}	Show these email notifications configured for the user number <num> or for the email address <email>: • For changes in download status • For changes in installation status • For new available packages
package <num>	Show this information about the package number <num>, as shown in the list of packages: • Display name • Description • Size • Type - Version, Wrapper, or Hotfix • Status - Download or installation status and reason for failure if applicable • Requires reboot - Yes or No • Recommended - Is the package recommended by Check Point? • Contains - List of components (files, archives) inside the package • Contained-in - Name of archive containing the package • Downloaded on - The date of the download • Imported on - The date of the import • Installed on - The date of the installation • Installation log - The name of the installation log Note - To see the numbered list of packages, type <code>show installer package</code> and hit <i>Tab</i>. Make sure to enter a <i>space</i> after the word <i>package</i>.
packages {all available-for-download downloaded imported installed recommended}	Show the list of all installation and Hotfix packages that are: • Available for download • Downloaded • Imported • Installed • Recommended by Check Point • All - all of the above

<pre>policy {all downloads periodically-self -update self-test {all auto-rollback install-policy network-link-up start-processes} send-cpuse-data}</pre>	Show the CPUSE policy configuration details: • policy rule for Hotfix downloads (installation packages are downloaded manually only) • policy rule for periodic updates of the Deployment Version • Self tests configured for sanity checks after upgrading with CPUSE - • auto-rollback - if on, runs a fall-back procedure when the installed package fails one of the sanity tests (automatically restores the version that was active before the package was installed and sends a notification that the installation failed) • install-policy - if on, makes sure that it is possible to install a policy • network-link-up - if on, makes sure that all the network interfaces on the Gaia computer are up • start-processes - if on, makes sure that Check Point processes are running • policy rule for sending the CPUSE download and installation information to Check Point
<pre>status {agent all build connection license update-from-cloud }</pre>	Show this information about the Deployment Agent: • Status - enabled or disabled • Build number • Connection status - connected or disconnected (also shows the cause of any connection problem, if relevant) • License status - active with the expiration date or expired • Last update from the cloud

CLI Procedures - CPUSE

This is a general approach to configuring CPUSE through CLI:

1. Review the current CPUSE configuration and status.
2. Configure the software deployment policy (not mandatory, can be done at another time).
3. Configure the CPUSE email notifications (not mandatory, can be done at another time).
4. Download a package.
5. Make sure that the package you wish to install is compatible with the system.
6. Install the package.

To review current CPUSE configuration and status:

- Run this command to see the packages that are available for download:

```
show installer packages available-for-download
```
- Run this command to see the packages that are downloaded and available for installation:

```
show installer packages downloaded
```

- Run this command to see the installed packages:
`show installer packages installed`
- Run this command to see the recommended packages:
`show installer packages recommended`
- Run this command to see the imported packages:
`show installer packages imported`
- Run this command to see all packages and their status:
`show installer packages all`

To configure the Software Deployment Policy:

1. Configure the way to download Hotfixes:
 - Manually - `set installer policy downloads manual`
 - As they become available - `set installer policy downloads automatic`
 - According to specified schedule - `set installer policy downloads scheduled {daily <time> | monthly <day> at <time> | once <date> at <time> | weekly <day_of_the_week> at <time>}`
2. Turn on the self test sanity checks and auto-rollback:
 - To make sure that it is possible to install the policy - `set installer policy self-test install-policy on`
 - To make sure that all the network interfaces are up - `set installer policy self-test network-link-up on`
 - To make sure that Check Point processes are running - `set installer policy self-test start-processes on`
 - To run a fall-back procedure if the installed package fails one of the sanity tests - `set installer policy self-test auto-rollback on`
3. Turn self-updates on, to keep the Deployment Agent up to date: `set installer policy periodically-self-update on`
4. Configure the option to send the download and installation data, to help Check Point improve the CPUSE service -
`set installer policy send-cpuse-data on`

To configure the CPUSE email notifications:

Turn on these options:

- For changes in download status - `set installer mail-notifications {<num> | <email>} download-status on`
- For changes in installation status - `set installer mail-notifications {<num> | <email>} install-status on`
- For new available packages - `set installer mail-notifications {<num> | <email>} new-available-packages on`

To install a Check Point package, you must first download it, then install it. If you need to install a Hotfix, you can first download it and then install it, or download and install it with one command.

To download a package from the Check Point Download Center:

1. List the names and the sequence numbers of the packages available for download from the Check Point Download Center: type `installer download` and press the `TAB` key.

2. Download a package: `installer download {<num> | <package>} [not-interactive]`
You can run the command with either the sequence number or the name of the package, and either in interactive (default) or non-interactive mode.

You can pause a download, if necessary.

To pause a download:

1. List the names and the sequence numbers of the packages that are being downloaded: type `installer download` and press the *TAB* key.
2. Pause the download: `installer download {<num> | <package>} pause`
You can run the command with either the sequence number or the name of the package.

To resume a download:

1. List the names and the sequence numbers of the packages for which the downloads were paused: type `installer download` and press the *TAB* key.
2. Resume the download: `installer download {<num> | <package>} resume`
You can run the command with either the sequence number or the name of the package, and either in interactive (default) or non-interactive mode.

To import a package:

1. Check for new available packages in the Check Point Cloud: `installer check-for-updates [not-interactive]`
You can run the command in interactive (default) or non-interactive mode.
2. Import a package:
 - From the Check Point Cloud: `import cloud <package> [not-interactive]`
 - From an ftp server: `import ftp <ip_addr> path <path> username <username> [password <password>] [not-interactive]`
 - From a location on the local computer: `import local <path> [not-interactive]`
 You can run the command in interactive (default) or non-interactive mode.

To make sure that the package is compatible with the system:

1. List the names and the sequence numbers of the packages available for installation: type `installer verify` and press the *TAB* key.
2. Verify a package: `installer verify {<num> | <package>} [not-interactive]`
You can run the command with either the sequence number or the name of the package, and either in interactive (default) or non-interactive mode.

To install a package:

1. List the names and the sequence numbers of the downloaded and imported packages: type `installer install` and press the *TAB* key.
2. Install a package: `installer install {<num> | <package>} [not-interactive]`
You can run the command with either the sequence number or the name of the package, and either in interactive (default) or non-interactive mode.

To download and install a Hotfix with one command:

1. List the names and the sequence numbers of the Hotfixes available for download and installation: type `installer download-and-install` and press the *TAB* key.
2. Download and install a Hotfix: `installer download-and-install {<num> | <package>} [not-interactive]`

You can run the command with either the sequence number or the name of the package, and either in interactive (default) or non-interactive mode.

To upgrade to a later version:

1. List the names and the sequence numbers of the downloaded packages: type `installer upgrade` and press the *TAB* key.
2. Run the upgrade: `installer upgrade {<num> | <package>} [not-interactive]`

You can run the command with either the sequence number or the name of the package, and either in interactive (default) or non-interactive mode.

To uninstall a package:

1. List the names and the sequence numbers of the installed packages: type `installer uninstall` and press the *TAB* key.
2. Uninstall a package: `installer uninstall {<num> | <package>} [not-interactive]`

You can run the command with either the sequence number or the name of the package, and either in interactive (default) or non-interactive mode.

To clear some disk space, you can delete packages you do not need.

To delete a package from the disk:

1. List the names and the sequence numbers of the downloaded packages: type `installer delete` and press the *TAB* key.
2. Delete a package: `installer delete {<num> | <package>} [not-interactive]`

You can run the command with either the sequence number or the name of the package, and either in interactive (default) or non-interactive mode.