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.

Latest Documentation

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=24828

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

For more about this release, see the R77.30 home page

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>05 December 2016</td>
<td>Updated Enabling Virtual Routers (on page 158) and How Failover Works (on page 154)</td>
</tr>
<tr>
<td>12 September 2016</td>
<td>Updated Configuring VLAN Interfaces - CLI (interface) (“Configuration Using the CLI” on page 42)</td>
</tr>
<tr>
<td>13 July 2016</td>
<td>Updated Configuring Bond Interfaces - WebUI (on page 44), general updates</td>
</tr>
<tr>
<td>09 May 2016</td>
<td>Updated Bond Interfaces (“Bond Interfaces (Link Aggregation)” on page 43) section. ARP is not supported after R75.40.</td>
</tr>
<tr>
<td>22 October 2015</td>
<td>Updated:</td>
</tr>
<tr>
<td></td>
<td>• Netflow Export (on page 78)</td>
</tr>
<tr>
<td></td>
<td>• Configuring ARP- WebUI (on page 59) and Configuring ARP - CLI (arp) (on page 60)</td>
</tr>
<tr>
<td></td>
<td>• Bond Interfaces (Link Aggregation) (on page 43)</td>
</tr>
<tr>
<td>16 September 2015</td>
<td>Updated:</td>
</tr>
<tr>
<td></td>
<td>• Bridge Interfaces (on page 48)</td>
</tr>
<tr>
<td></td>
<td>• High Availability VRRP section (“VRRP” on page 153)</td>
</tr>
<tr>
<td></td>
<td>• Managing User Accounts - CLI (user) (on page 125)</td>
</tr>
<tr>
<td></td>
<td>• Environment Commands (on page 26)</td>
</tr>
<tr>
<td></td>
<td>• Client Environment Output Format (on page 27)</td>
</tr>
<tr>
<td>16 July 2015</td>
<td>Updated CPUSE CLI command syntax in Downloading and Installing with CPUSE - clish (on page 199) and CLI Procedures - CPUSE (on page 205)</td>
</tr>
<tr>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 06 May 2015     | Updated for R77.30  
                    Added the list of Shared Features in Cloning Groups (on page 88)  
                    Added new Cloning Groups CLI commands in Configuring Cloning Groups - CLI (Cloning Groups) (on page 90) and Cloning Group Management mode in Configuring Cloning Groups - WebUI (on page 89)  
                    Corrected Host parameter description in Configuring RADIUS Servers - WebUI (on page 141) and in Configuring RADIUS Servers - CLI (aaa) (on page 142)  
                    Updated VRRP General Configuration Considerations (on page 169)                                                                                                                                                                                                 |
| 26 August 2014  | Made a correction in Understanding Monitored-Circuit VRRP (on page 155)                                                                                                                                                                                                      |
| 19 June 2014    | Cover changed to be relevant for all R77 versions  
                    Updated for R77.10  
                    • Added Monitoring RAID Synchronization (on page 186), Showing RAID Information - WebUI (on page 186), and Showing RAID Information - CLI (on page 186)  
                    Updated for R77.20  
                    • Added information on TACACS+ server configuration on Cisco ACS servers and the reference to the best practices sk, in Configuring TACACS+ Servers for Non-Local Gaia Users (on page 149).  
                    • Added the note on uninterrupted processes and policy enforcement during the snapshot creation in Snapshot Image Management (on page 180).  
                    • Software Updates renamed Upgrades (CPUSE) ("CPUSE" on page 196).                                                                                                                                                                                   |
<p>| 11 February 2014| • Updated expert mode command (&quot;Expert Mode&quot; on page 28).                                                                                                                                                                                                               |</p>
<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 January 2014</td>
<td>• Link to snapshot limitations added (&quot;Snapshot Image Management&quot; on page 180).</td>
</tr>
<tr>
<td></td>
<td>• Added procedures steps to the IPv4 Static Route (&quot;Configuring IPv4 Static Routes - WebUI&quot; on page 71) configuration procedure. Explained Local Scope.</td>
</tr>
<tr>
<td></td>
<td>• Corrected: Definition of the Host Access &gt; Allowed clients (&quot;Host Access&quot; on page 120) setting.</td>
</tr>
<tr>
<td></td>
<td>• Updated: Deny Access After Failed Login Attempts (on page 134)</td>
</tr>
<tr>
<td></td>
<td>• Fixed: Creating TACACS+ roles and the tacacs_enable command (&quot;Configuring Gaia as a TACACS+ Client&quot; on page 148)</td>
</tr>
<tr>
<td></td>
<td>• Updated: Restoring a factory default image (added) and Must not rename an exported image.</td>
</tr>
<tr>
<td></td>
<td>• Updated: Emergendisk: Can be used on all Check Point appliances and Open Servers (&quot;Emergendisk&quot; on page 192). Note (&quot;Booting from the Emergendisk Removable Device&quot; on page 193).</td>
</tr>
<tr>
<td></td>
<td>• Updated: Must not rename an exported image.</td>
</tr>
<tr>
<td>26 August 2013</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

**Feedback**

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

Please help us by sending your comments to mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Gaia R77 Versions Administration Guide.
Security Management Server and Firewall Commands ............................................ 209

cpca_client................................................................. 209
  cpca_client create_cert........................................... 209
  cpca_client revoke_cert.......................................... 210
  cpca_client lscert.................................................... 210
  cpca_client set_mgmt_tool...................................... 210

cp_conf............................................................... 211
  cp_conf sic.......................................................... 211
  cp_conf admin...................................................... 212
  cp_conf ca.......................................................... 212
  cp_conf finger...................................................... 213
  cp_conf lic.......................................................... 213
  cp_conf client....................................................... 213
  cp_conf ha.......................................................... 214
  cp_conf snmp....................................................... 214
  cp_conf auto....................................................... 214
  cp_conf sxl.......................................................... 215

cpconfig............................................................. 215

cpinfo............................................................... 215

cpstat............................................................... 216

cpstop............................................................... 218

fw ................................................................. 219
  fw -i ................................................................ 219
  fw ctl.............................................................. 220
  fw ctl debug..................................................... 221
  fw ctl affinity.................................................... 222
  fw ctl engine..................................................... 224
  fw ctl multik stat.............................................. 225
  fw ctl sdstat..................................................... 225
  fw fetch......................................................... 226
  fw fetchlogs..................................................... 227
  fw hastat........................................................ 228
  fw isp_link....................................................... 228
  fw kill.............................................................. 228
  fw lea_notify..................................................... 229
  fw lichosts....................................................... 229
  fw log.............................................................. 229
  fw logsswitch................................................... 232
  fw mergefiles..................................................... 233
  fw monitor......................................................... 234
  fw lslogs.......................................................... 237
  fw putkey........................................................ 238
  fw repairlog..................................................... 239
  fw sam............................................................ 239
  fw stat.............................................................. 243
  fw tab.............................................................. 244
  fw ver.............................................................. 245

fwm ............................................................... 246
  fwm dbimport.................................................... 246
  fwm expdate..................................................... 247
  fwm dbexport.................................................... 248
Gaia Overview

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

Gaia is a single, unified network security Operating System that combines the best of Check Point’s SecurePlatform operating system, 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 using the same syntactic rules. An enhanced help system and auto-completion further simplifies user operation.
- Role Based Administration - Enables Gaia administrators to create different roles. Administrators can allow users to access features by adding those functions to the user’s role definition. 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 ................................................................. 13
Logging in to the WebUI ...................................................... 14
Using the Interface Elements ............................................. 15

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 configuring Gaia platforms. Almost all system configuration tasks can be done 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 shows only basic configuration options. 2) Advanced mode 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

![WebUI Interface Screenshot]
### Introduction to the WebUI

#### Item Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Navigation tree</td>
</tr>
<tr>
<td>2</td>
<td>Toolbar</td>
</tr>
<tr>
<td>3</td>
<td>Search tool</td>
</tr>
<tr>
<td>4</td>
<td>Overview page with widgets that show system information</td>
</tr>
<tr>
<td>5</td>
<td>Status bar</td>
</tr>
</tbody>
</table>

**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 127).

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 **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:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Read/Write mode enabled.</td>
</tr>
<tr>
<td></td>
<td>Configuration locked (Read Only mode).</td>
</tr>
<tr>
<td></td>
<td>Opens the <strong>Console</strong> accessory for CLI commands. Available in the Read/Write mode only.</td>
</tr>
<tr>
<td></td>
<td>Opens the <strong>Scratch Pad</strong> accessory for writing notes or for quick copy/paste operations. Available in the Read/Write mode only.</td>
</tr>
</tbody>
</table>

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 ........................................................ 17
Showing System Overview Information - CLI .............................................................. 18
Changing System Edition ............................................................................................. 19

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.

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

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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) |
### Widget Description

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blades</td>
<td>Installed Software Blades. Those that are enabled in SmartDashboard are colored. Those that are not enabled are grayed out.</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>Interfaces, their status and IP addresses</td>
</tr>
<tr>
<td>Memory Monitor</td>
<td>Graphical display of memory usage</td>
</tr>
<tr>
<td>CPU Monitor</td>
<td>Graphical display of CPU usage</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Shows all system information.</td>
</tr>
<tr>
<td>os build</td>
<td>The Gaia build number.</td>
</tr>
<tr>
<td>os edition</td>
<td>The Gaia edition [32-bit or 64-bit].</td>
</tr>
<tr>
<td>os kernel</td>
<td>The Gaia kernel build number.</td>
</tr>
<tr>
<td>product</td>
<td>The Gaia version.</td>
</tr>
</tbody>
</table>
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
- Commands and Features
- Command Completion
- Command History
- Command Line Movement and Editing
- Obtaining a Configuration Lock
- 32 and 64-bit Gaia Editions
- Environment Commands
- Expert Mode
- User Defined (Extended) Commands

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 a command-line connection (SSH or a console) over a TCP/IP network.
2. Log on 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

<table>
<thead>
<tr>
<th>Main operations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Adds a new value to the system.</td>
</tr>
<tr>
<td>set</td>
<td>Sets a value in the system.</td>
</tr>
</tbody>
</table>
### Main operations

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Shows a value or values from the system.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a value from the system.</td>
</tr>
</tbody>
</table>

### Other operations

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>save</td>
<td>Saves the configuration changes made since the last save operation.</td>
</tr>
<tr>
<td>reboot</td>
<td>Restart the system.</td>
</tr>
<tr>
<td>halt</td>
<td>Turns the computer off.</td>
</tr>
<tr>
<td>quit</td>
<td>Exits from the CLI.</td>
</tr>
<tr>
<td>exit</td>
<td>Exits from the shell.</td>
</tr>
<tr>
<td>Start</td>
<td>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.</td>
</tr>
<tr>
<td>commit</td>
<td>Ends transaction by committing changes.</td>
</tr>
<tr>
<td>rollback</td>
<td>Ends transaction by discarding changes.</td>
</tr>
<tr>
<td>expert</td>
<td>Enter the expert shell. Allows low-level access to the system, including the file system.</td>
</tr>
<tr>
<td>ver</td>
<td>Shows the version of the active Gaia image.</td>
</tr>
<tr>
<td>revert</td>
<td>Revert the database.</td>
</tr>
<tr>
<td>help</td>
<td>Get help on navigating the CLI and some useful commands.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Press ...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TAB&gt;</td>
<td>Complete or fetch the keyword. For example</td>
</tr>
<tr>
<td></td>
<td>Gaia&gt; set in&lt;TAB&gt;</td>
</tr>
<tr>
<td></td>
<td>inactivity-timeout - Set inactivity timeout interface - Displays the interface related parameters</td>
</tr>
<tr>
<td></td>
<td>Gaia&gt; set in</td>
</tr>
<tr>
<td>&lt;SPACE&gt;</td>
<td>Show the arguments that the command for that feature accepts. For example:</td>
</tr>
<tr>
<td>&lt;TAB&gt;</td>
<td>Gaia&gt; set interface &lt;SPACE&gt; &lt;TAB&gt;</td>
</tr>
<tr>
<td></td>
<td>eth0 eth1 lo</td>
</tr>
<tr>
<td></td>
<td>Gaia&gt; set interface</td>
</tr>
<tr>
<td>&lt;ESC&gt;</td>
<td>See possible command completions. For example</td>
</tr>
<tr>
<td>&lt;ESC&gt;</td>
<td>Gaia&gt; set inter&lt;ESC&gt;&lt;ESC&gt;</td>
</tr>
<tr>
<td></td>
<td>set interface VALUE ipv4-address VALUE mask-length VALUE</td>
</tr>
<tr>
<td></td>
<td>set interface VALUE ipv4-address VALUE subnet-mask VALUE</td>
</tr>
<tr>
<td></td>
<td>set interface VALUE ipv6-address VALUE mask-length VALUE</td>
</tr>
<tr>
<td></td>
<td>set interface VALUE { comments VALUE mac-addr VALUE mtu VALUE state</td>
</tr>
<tr>
<td></td>
<td>speed VALUE duplex VALUE auto-negotiation VALUE }</td>
</tr>
<tr>
<td></td>
<td>set interface VALUE { ipv6-autoconfig VALUE }</td>
</tr>
<tr>
<td></td>
<td>Gaia&gt; set inter</td>
</tr>
<tr>
<td>?</td>
<td>Get help on a feature or keyword. For example</td>
</tr>
<tr>
<td></td>
<td>Gaia&gt; set interface &lt;&lt;&lt;</td>
</tr>
<tr>
<td></td>
<td>interface: {show/add/delete} interface &quot;interface-name&quot;</td>
</tr>
<tr>
<td></td>
<td>Gaia&gt; set interface</td>
</tr>
<tr>
<td>UP/DOWN</td>
<td>Browse the command history.</td>
</tr>
<tr>
<td>arrow</td>
<td>LEFT/RIGHT</td>
</tr>
<tr>
<td>arrow</td>
<td>Enter</td>
</tr>
</tbody>
</table>

Command History

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>↓</td>
<td>Recall previous command.</td>
</tr>
<tr>
<td>↑</td>
<td>Recall next command.</td>
</tr>
</tbody>
</table>
### Command Line Interface

#### 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.

<table>
<thead>
<tr>
<th>Word Designator</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The operation word.</td>
</tr>
<tr>
<td>n</td>
<td>The nth word.</td>
</tr>
<tr>
<td>^</td>
<td>The first argument; that is, word 1.</td>
</tr>
<tr>
<td>$</td>
<td>The last argument.</td>
</tr>
<tr>
<td>%</td>
<td>The word matched by the most recent <code>!?str!?</code> search.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>p</td>
<td>Print the new command but do not execute</td>
</tr>
<tr>
<td>s/str1/str2</td>
<td>Substitute <code>new</code> for the first occurrence of <code>old</code> in the word being referred to.</td>
</tr>
<tr>
<td>g</td>
<td>Apply changes over the entire command. Use this modified in conjunction with <code>s</code>, as in <code>gs/str1/str2</code>.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Keystroke combination</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alt-D</td>
<td>Delete next word.</td>
</tr>
<tr>
<td>Alt-F</td>
<td>Go to the next word.</td>
</tr>
<tr>
<td>Ctrl-Alt-H</td>
<td>Delete the previous word.</td>
</tr>
<tr>
<td>Ctrl-shift_</td>
<td>Repeat the previous word.</td>
</tr>
<tr>
<td>Ctrl-A</td>
<td>Move to the beginning of the line.</td>
</tr>
<tr>
<td>Ctrl-B</td>
<td>Move to the previous character.</td>
</tr>
<tr>
<td>Ctrl-E</td>
<td>Move to the end of the line.</td>
</tr>
<tr>
<td>Ctrl-F</td>
<td>Move to the next character.</td>
</tr>
<tr>
<td>Ctrl-H</td>
<td>Delete the previous character.</td>
</tr>
<tr>
<td>Ctrl-L</td>
<td>Clear the screen and show the current line at the top of the screen.</td>
</tr>
<tr>
<td>Ctrl-N</td>
<td>Next history item.</td>
</tr>
<tr>
<td>Ctrl-P</td>
<td>Previous history item.</td>
</tr>
<tr>
<td>Ctrl-R</td>
<td>Redisplay the current line.</td>
</tr>
<tr>
<td>Ctrl-U</td>
<td>Delete the current line.</td>
</tr>
</tbody>
</table>

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 127).

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
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>off</td>
<td>on</td>
</tr>
<tr>
<td>timeout</td>
<td>Enables config-lock for the specified interval in seconds (5-900).</td>
</tr>
</tbody>
</table>

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 R77 Release notes http://supportcontent.checkpoint.com/solutions?id=sk104859.

Open servers always install a 32-bit kernel, but you can switch to the 64-bit kernel using the Edition feature.

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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-lock {on</td>
<td>off}</td>
</tr>
<tr>
<td>debug {0-6}</td>
<td>Debug level. Predefined levels are:</td>
</tr>
<tr>
<td></td>
<td>• 0 - [Default] Do not debug, display error messages only</td>
</tr>
<tr>
<td></td>
<td>• 5 - Show confd requests and responses</td>
</tr>
<tr>
<td></td>
<td>• 6 - Show handler invocation parameters and results</td>
</tr>
<tr>
<td>echo-cmd {on</td>
<td>off}</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| on-failure {continue | stop} | Action performed on failure:  
* continue - Show error messages, but continue running commands from a file or a script  
* stop  - (Default) Stop running commands from a file or a script |
| output {pretty | structured | xml} | Command line output format (“Client Environment Output Format” on page 27). The default is pretty. |
| prompt <prompt_string> | Command prompt string. A valid prompt string can consist of any printable characters and a combination of these variables:  
* %H - Replaced with the Command number  
* %I - Replaced with the User ID  
* %M - Replaced with the Hostname  
* %P - Replaced with the Product I.  
* %U - Replaced with the Username  
To set the prompt back to the default, use the keyword default. |
| rows <row_number> | Number of rows to show in your terminal window. If the window size is changed, the number of rows will also change, unless the value is set to 0 (zero). |
| syntax-check {on | off} | Put the shell into syntax-check mode. Commands you enter are checked syntactically and are not executed, but values are validated. The default is off. |

### Client Environment Output Format

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>
  ```
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 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`

Expert- Password

A password protects that expert shell against authorized 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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hash</td>
<td>The password as an MD5 salted hash instead of plain text. Use this option when upgrading or restoring using backup scripts.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>command</td>
<td>Name of the extended command</td>
</tr>
<tr>
<td>path</td>
<td>Path of the extended command</td>
</tr>
<tr>
<td>description</td>
<td>Description of the extended command</td>
</tr>
</tbody>
</table>

### Example

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

1. To add the `free` command, run
   ```bash
   add command free path /usr/bin/free description "Display amount of free and used memory in the system"
   ```
2. Save the configuration. Run
   ```bash
   save config
   ```
3. Log out of Gaia and log in again.
4. To add the `free` command to the `systemDiagnosis` role, run
   ```bash
   add rba role systemDiagnosis domain-type System readwrite-features ext_free
   ```
5. To assign user john with the `systemDiagnosis` role, run
   ```bash
   add rba user john roles systemDiagnosis
   ```
Configuring Gaia for the First Time

In This Section:
- Running the First Time Configuration Wizard in WebUI ............................................ 31
- Running the First Time Configuration Wizard in CLI .................................................. 31

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


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_management=false"

For more information on valid parameters and values, see config_system (on page 32).

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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Valid values</th>
</tr>
</thead>
<tbody>
<tr>
<td>install_security_gw</td>
<td>Installs Security Gateway, if set to true.</td>
<td>• true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• false</td>
</tr>
<tr>
<td>install_ppak</td>
<td>Installs Performance Pack, if set to true. Must be set to true, if <code>install_security_gw</code> is set to true.</td>
<td>• true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• false</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Valid values</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>gateway_daip</td>
<td>Enables or disables dynamic IP gateway.</td>
<td>• true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• false</td>
</tr>
<tr>
<td></td>
<td>Note - must be set to false if ClusterXL or Security Management Server is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>enabled.</td>
<td></td>
</tr>
<tr>
<td>gateway_cluster_member</td>
<td>Enables or disables ClusterXL.</td>
<td>• true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• false</td>
</tr>
<tr>
<td>install_security_management</td>
<td>Installs Security Management Server, if set to true.</td>
<td>• true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• false</td>
</tr>
<tr>
<td>install_mgmt_primary</td>
<td>Makes the installed Security Management Server the primary one. The</td>
<td>• true</td>
</tr>
<tr>
<td></td>
<td>install_security_management must be set to true.</td>
<td>• false</td>
</tr>
<tr>
<td></td>
<td>Note - can only be set to true, if the install_mgmt_secondary is set to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>false.</td>
<td></td>
</tr>
<tr>
<td>install_mgmt_secondary</td>
<td>Makes the installed Security Management Server a secondary one. The</td>
<td>• true</td>
</tr>
<tr>
<td></td>
<td>install_security_management must be set to true.</td>
<td>• false</td>
</tr>
<tr>
<td></td>
<td>Note - can only be set to true, if the install_mgmt_primary is set to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>false.</td>
<td></td>
</tr>
<tr>
<td>install_mds_primary</td>
<td>Makes the installed Security Management Server the primary Multi-Domain</td>
<td>• true</td>
</tr>
<tr>
<td></td>
<td>Server.</td>
<td>• false</td>
</tr>
<tr>
<td></td>
<td>Note - can only be set to true, if the install_mds_secondary is set to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>false.</td>
<td></td>
</tr>
<tr>
<td>install_mds_secondary</td>
<td>Makes the installed Security Management Server a secondary Multi-Domain</td>
<td>• true</td>
</tr>
<tr>
<td></td>
<td>Server.</td>
<td>• false</td>
</tr>
<tr>
<td></td>
<td>Note - can only be set to true, if the install_mds_primary is set to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>false.</td>
<td></td>
</tr>
<tr>
<td>install_mlm</td>
<td>Installs Multi-Domain Log Server, if set to true.</td>
<td>• true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• false</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Valid values</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>install_mds_interface</td>
<td>Specifies Multi-Domain Server management interface.</td>
<td>Name of the interface exactly as it appears in the device configuration.</td>
</tr>
<tr>
<td></td>
<td>Examples: eth0, eth1</td>
<td></td>
</tr>
<tr>
<td>mgmt_admin_name</td>
<td>Sets management administrator’s username. Must be provided if install_security_management is set to true.</td>
<td>A string of alphanumeric characters.</td>
</tr>
<tr>
<td>mgmt_admin_passwd</td>
<td>Sets management administrator’s password. Must be provided if install_security_management is set to true.</td>
<td>A string of alphanumeric characters.</td>
</tr>
<tr>
<td>mgmt_gui_clients_radio</td>
<td>Specifies management WebUI clients that can connect to the Security Management Server.</td>
<td>• IPv4 address of a host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• range</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• network</td>
</tr>
<tr>
<td>mgmt_gui_clients_first_ip_field</td>
<td>Specifies the first address of the range, if mgmt_gui_clients_radio is set to range.</td>
<td>IPv4 address of a host.</td>
</tr>
<tr>
<td>mgmt_gui_clients_last_ip_field</td>
<td>Specifies the last address of the range, if mgmt_gui_clients_radio is set to range.</td>
<td>IPv4 address of a host.</td>
</tr>
<tr>
<td>mgmt_gui_clients_ip_field</td>
<td>Specifies the network address, if mgmt_gui_clients_radio is set to network.</td>
<td>IPv4 address of a network.</td>
</tr>
<tr>
<td>mgmt_gui_clients_subnet_field</td>
<td>Specifies the netmask, if mgmt_gui_clients_radio is set to network.</td>
<td>A number from 0 to 32.</td>
</tr>
<tr>
<td>ftw_sic_key</td>
<td>Sets a secure Internal Community key, if install_security_management is set to false.</td>
<td>A string of alphanumeric characters.</td>
</tr>
<tr>
<td>admin_hash</td>
<td>Sets administrator’s password.</td>
<td>A string of alphanumeric characters, enclosed between single quotation marks.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Valid values</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>iface</td>
<td>Interface name (optional).</td>
<td>Name of the interface exactly as it appears in the device configuration.</td>
</tr>
<tr>
<td></td>
<td>Examples: eth0, eth1</td>
<td>Examples: eth0, eth1</td>
</tr>
<tr>
<td>ipstat_v4</td>
<td>Turns static IPv4 configuration on, when set to manually.</td>
<td>• manually</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• off</td>
</tr>
<tr>
<td>ipaddr_v4</td>
<td>Sets IPv4 address of the management interface.</td>
<td>IPv4 address.</td>
</tr>
<tr>
<td>masklen_v4</td>
<td>Sets IPv4 mask length for the management interface.</td>
<td>A number from 0 to 32.</td>
</tr>
<tr>
<td>default_gw_v4</td>
<td>Specifies IPv4 address of the default gateway.</td>
<td>IPv4 address.</td>
</tr>
<tr>
<td>ipstat_v6</td>
<td>Turns static IPv6 configuration on, when set to manually.</td>
<td>• manually</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• off</td>
</tr>
<tr>
<td>ipaddr_v6</td>
<td>Sets IPv6 address of the management interface.</td>
<td>IPv6 address.</td>
</tr>
<tr>
<td>masklen_v6</td>
<td>Sets IPv6 mask length for the management interface.</td>
<td>A number from 0 to 128.</td>
</tr>
<tr>
<td>default_gw_v6</td>
<td>Specifies IPv6 address of the default gateway.</td>
<td>IPv6 address.</td>
</tr>
<tr>
<td>hostname</td>
<td>Sets the name of the local host (optional).</td>
<td>A string of alphanumeric characters.</td>
</tr>
<tr>
<td>domainname</td>
<td>Sets the domain name (optional).</td>
<td>Fully qualified domain name.</td>
</tr>
<tr>
<td></td>
<td>Example: somedomain.com</td>
<td>Example: somedomain.com</td>
</tr>
<tr>
<td>timezone</td>
<td>Sets the area/region (optional).</td>
<td>The value must be enclosed between single quotation marks.</td>
</tr>
<tr>
<td></td>
<td>Examples: 'America/New_York',</td>
<td>Examples: 'America/New_York',</td>
</tr>
<tr>
<td></td>
<td>'Asia/Jerusalem'</td>
<td>'Asia/Jerusalem'</td>
</tr>
<tr>
<td>ntp_primary</td>
<td>Sets the IP address of the primary NTP server (optional).</td>
<td>IPv4 address.</td>
</tr>
<tr>
<td>ntp_secondary</td>
<td>Sets the IP address of the secondary NTP server (optional).</td>
<td>IPv4 address.</td>
</tr>
<tr>
<td>primary</td>
<td>Sets the IP address of the primary DNS server (optional)</td>
<td>IPv4 address.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Valid values</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>secondary</td>
<td>Sets the IP address of the secondary DNS server (optional)</td>
<td>IPv4 address.</td>
</tr>
<tr>
<td>tertiary</td>
<td>Sets the IP address of the tertiary DNS server (optional)</td>
<td>IPv4 address.</td>
</tr>
<tr>
<td>download_info</td>
<td>Downloads Check Point Software Blade contracts and other important information, if set to true (optional, but highly recommended). For more information, see sk94508 <a href="http://supportcontent.checkpoint.com/solutions?id=sk94508">http://supportcontent.checkpoint.com/solutions?id=sk94508</a>.</td>
<td>• true • false</td>
</tr>
<tr>
<td>upload_info</td>
<td>Uploads data that helps Check Point provide you with optimal services, if set to true (optional, but highly recommended). For more information, see sk94509 <a href="http://supportcontent.checkpoint.com/solutions?id=sk94509">http://supportcontent.checkpoint.com/solutions?id=sk94509</a>.</td>
<td>• true • false</td>
</tr>
</tbody>
</table>
Network Management

In This Section:

- Network Interfaces ....................................................................................................... 37
- ARP ................................................................................................................................ 59
- DHCP Server ................................................................................................................. 62
- Hosts and DNS .............................................................................................................. 66
- IPv4 Static Routes ......................................................................................................... 70
- IPv6 Static Routes ......................................................................................................... 75
- Netflow Export .............................................................................................................. 78
- Performance Optimization ........................................................................................... 81

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 SmartDashboard, 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 by using 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.

<table>
<thead>
<tr>
<th>Link Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grey (Down)</td>
<td>The physical interface is disabled (Down).</td>
</tr>
<tr>
<td>Red (no Link)</td>
<td>The physical interface is enabled (up), but Gaia cannot find a network connection.</td>
</tr>
</tbody>
</table>
**Link Status**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green (Up) ![Green Icon]</td>
</tr>
<tr>
<td>The physical interface is enabled (up) and connected to the network.</td>
</tr>
</tbody>
</table>

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>
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Configures a physical or virtual interface</td>
</tr>
<tr>
<td>ipv4-address</td>
<td>Assigns the IPv4 or IPv6 address</td>
</tr>
<tr>
<td>ipv6-address</td>
<td>Assigns the IPv4 or IPv6 address</td>
</tr>
<tr>
<td>ipv6-autoconfig</td>
<td>If on, automatically gets the IPv6 address from the DHCP</td>
</tr>
<tr>
<td>mask-length</td>
<td>Configures IPv4 or IPv6 subnet mask length using CIDR (/xx) notation</td>
</tr>
<tr>
<td>subnet-mask</td>
<td>Configures IPv4 subnet mask using dotted decimal notation</td>
</tr>
<tr>
<td>comments</td>
<td>Adds free text comments to an interface definition</td>
</tr>
<tr>
<td>mac-addr</td>
<td>Configures the interface hardware MAC address</td>
</tr>
<tr>
<td>mtu</td>
<td>Configure the Maximum Transmission Unit size for an interface</td>
</tr>
<tr>
<td>state</td>
<td>Sets interfaces status to on [enabled] or off [disabled].</td>
</tr>
<tr>
<td>link-speed</td>
<td>Configures the interface link speed and duplex status</td>
</tr>
<tr>
<td>auto-negotiation</td>
<td>Configures automatic negotiation of interface link speed and duplex settings - on [enabled] or off [disabled]</td>
</tr>
</tbody>
</table>
Description: Configure physical interfaces

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP&gt;</td>
<td>IPv4 or IPv6 address</td>
</tr>
<tr>
<td>&lt;IF&gt;</td>
<td>Interface name</td>
</tr>
<tr>
<td>&lt;Mask&gt;</td>
<td>Interface net mask in dotted decimal or CIDR ((/xx) notation as applicable</td>
</tr>
<tr>
<td>&lt;MAC&gt;</td>
<td>Manually enter the applicable hardware address</td>
</tr>
<tr>
<td>&lt;MTU Setting&gt;</td>
<td>Integer greater or equal to 68 (Default = 1500)</td>
</tr>
<tr>
<td>&lt;Speed_Duplex&gt;</td>
<td>Enter the link speed in Mbps and duplex status using one of these values:</td>
</tr>
<tr>
<td></td>
<td>10M/half</td>
</tr>
<tr>
<td></td>
<td>10M/full</td>
</tr>
<tr>
<td></td>
<td>100M/half</td>
</tr>
<tr>
<td></td>
<td>100M/full</td>
</tr>
<tr>
<td></td>
<td>1000M/full</td>
</tr>
<tr>
<td></td>
<td>10000M/full</td>
</tr>
</tbody>
</table>

Examples:
- 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 eth1:0. The second alias added is eth1:1, 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>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP&gt;</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>&lt;IF&gt;</td>
<td>Interface name</td>
</tr>
<tr>
<td>&lt;Mask&gt;</td>
<td>IPv4 subnet mask length using CIDR (/xx) notation</td>
</tr>
<tr>
<td>&lt;Alias IF&gt;</td>
<td>Interface alias name in the format &lt;IF&gt;:XX, where XX is the automatically assigned sequence number.</td>
</tr>
</tbody>
</table>

**Examples**
- 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 eth1:0. The second alias added is eth1:1, 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**

- **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

**Values**

- `<IF>` Physical interface related to this VLAN
- `<VLAN ID>` VLAN identifier (integer range 2-4094)
- `<IP>` IP address (IPv4 or IPv6)
- `<Length>` Mask length (integer value)

**Example**

- `add interface eth1 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 eth1.99 vlan eth1`

**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 gives fault tolerance and increases throughput by sharing the load among many interfaces. Check Point devices support the IEEE 802.3ad Link Aggregation Control Protocol (LCAP) for dynamic link aggregation.

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 bond interfaces using one of these functional strategies:

- **High Availability (Active/Backup):** Gives redundancy when there is an interface or link failure. This strategy also supports switch redundancy. High Availability works in **Active/Backup** mode - Interface Active/Standby mode. When and 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 using one of these modes:
  - **Round Robin** - Selects the active slave interface sequentially.
  - **802.3ad** - Dynamically uses active slaves to share the traffic load using the LACP protocol. This protocol enables full interface monitoring between the gateway and a switch.
  - **XOR** - Selects the algorithm for slave selection according to 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** (uses 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 46).
2. Define the slave interfaces ("Defining Interfaces" on page 46) and set them to the UP State.
3. Set the bond operating mode ("Defining the Bond Operating Mode" on page 47).
4. Define other bond parameters: primary interface ("Defining the Primary Slave Interface" on page 46), media monitoring ("Defining the Media Monitoring Interval" on page 47), delay rate ("Defining the UP and Down Delay Times" on page 48).

**Link Aggregation - CLI (bonding)**

This section is a quick reference for Link Aggregation commands. The next sections include procedures for different tasks, including explanations of the configuration options.

Use these commands to configure link aggregation.

**Syntax:**

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

set bonding [group <bondID>] [primary <IFName>] [mii-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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bondID</td>
<td>ID of bond, an integer between 1 and 1024</td>
</tr>
<tr>
<td>IFName</td>
<td>Name of interface to add to the bond</td>
</tr>
<tr>
<td>primary</td>
<td>Name of primary interface in the bond</td>
</tr>
<tr>
<td>mii-interval</td>
<td>Frequency that the system polls the Media Independent Interface (MII) to get status</td>
</tr>
<tr>
<td>up-delay</td>
<td>Waiting time to confirm the interface status before taking the specified action (0-5000 ms, default = 200 ms)</td>
</tr>
<tr>
<td>down-delay</td>
<td></td>
</tr>
<tr>
<td>mode</td>
<td>Bond operating mode (&quot;Defining the Bond Operating Mode&quot; on page 47)</td>
</tr>
<tr>
<td>lacp-rate</td>
<td>Link Aggregation Control Protocol packet transmission rate:</td>
</tr>
<tr>
<td></td>
<td>• slow - LACPDU packet sent every 30 seconds</td>
</tr>
<tr>
<td></td>
<td>• fast - LACPDU packet sent every second</td>
</tr>
<tr>
<td>xmit-hash-policy</td>
<td>Algorithm for interface selected by TCP/IP layer</td>
</tr>
</tbody>
</table>

**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 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 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 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
```

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

Check Point security devices support bridge interfaces that implement native, Layer-2 bridging. Configuring an interface as a bridge lets network administrators deploy security devices in an existing topology without reconfiguring the existing IP routing scheme. This is an important advantage for large-scale, complex environments. Gaia does not support Spanning Tree Protocol (STP) bridges.

You configure Ethernet interfaces (including aggregated interfaces) on your Check Point security device to work like ports on a physical bridge.

Note - An interface that is configured as a bond slave, cannot be configured as a bridge interface.

The bridge interfaces send traffic using 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.

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

- `add bridging group <Group ID> [interface <interface>]`
- `delete bridging group <Group ID> interface <interface>`
- `show bridging group <Group ID>`

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Group ID&gt;</td>
<td>ID of bridging group</td>
</tr>
<tr>
<td>&lt;interface&gt;</td>
<td>Interface name</td>
</tr>
</tbody>
</table>

**Example** - `add bridging group 56 interface eth1`

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

Configuring Bridge Mode with the CLI

Bridge interfaces are known as **Bridging Groups** in Gaia cli.sh 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 by adding a sequence number to the string 'loop'. For example, the name of first loopback interface is loop00. She 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>

<table>
<thead>
<tr>
<th>Parameters and Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loopback</td>
<td>Configures a loopback interface.</td>
</tr>
<tr>
<td>lo</td>
<td>You must use the lo (local interface) keyword to define a loopback interface.</td>
</tr>
<tr>
<td>&lt;IP&gt;</td>
<td>IPv4 or IPv6 address.</td>
</tr>
<tr>
<td>&lt;Mask&gt;</td>
<td>IPv4 subnet mask or IPv6 mask length using CIDR (/xx) notation.</td>
</tr>
<tr>
<td>&lt;IF&gt;</td>
<td>Loopback interface name [loopXX]</td>
</tr>
</tbody>
</table>

**Examples**
- 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 R77 VPN Administration Guide [link](http://supportcontent.checkpoint.com/solutions?id=sk104859).

The procedure for configuring a VTI includes these steps:
1. Make sure that the VPN Software Blade is enabled and licensed 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 52) that includes the two peer Security Gateways.
4. Make Route Based VPN the default option ("Making Route Based VPN the Default Option" on page 52). Do this procedure one time for each Security Management Server.
5. Define the VTI ("Configuring VPN Tunnel Interfaces" on page 52) using the WebUI or CLI.
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 *R77 VPN Administration Guide*

To define a VPN Community for Site to Site VPN:

1. In SmartDashboard, 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 SmartDashboard 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 SmartDashboard, 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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type numbered</td>
<td>Defines a <strong>numbered</strong> VTI that uses a specified, static IPv4 addresses for local and remote connections</td>
</tr>
<tr>
<td>type unnumbered</td>
<td>Defines an <strong>unnumbered</strong> VTI that uses the interface and the remote peer name to get addresses</td>
</tr>
<tr>
<td>local</td>
<td>Defines the local peer IPv4 address (numbered VTI only)</td>
</tr>
<tr>
<td>remote</td>
<td>Defines the remote peer IPv4 address (numbered VTI only)</td>
</tr>
<tr>
<td>peer</td>
<td>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.</td>
</tr>
<tr>
<td>dev</td>
<td>Defines the interface (unnumbered VTI only)</td>
</tr>
<tr>
<td>Parameter</td>
<td>Values</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
</tr>
<tr>
<td>&lt;Tunnel ID&gt;</td>
<td>Unique tunnel name (integer from 1 to 99) Gaia automatically adds the prefix 'vpnt' to the tunnel name Example: vnpt10</td>
</tr>
<tr>
<td>&lt;Local IP&gt;</td>
<td>Local peer IPv4 address (numbered VTI only) in dotted decimal format</td>
</tr>
<tr>
<td>&lt;remote IP&gt;</td>
<td>Remote peer IPv4 address (numbered VTI only) in dotted decimal format</td>
</tr>
<tr>
<td>&lt;Peer ID&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;IF&gt;</td>
<td>Local peer interface name (unnumbered VTI only)</td>
</tr>
</tbody>
</table>

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).

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Tunnel</td>
<td>Any</td>
<td>Any</td>
<td>MyIntranet</td>
<td>Any</td>
<td>accept</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Tunnel</td>
<td>Any</td>
<td>Any</td>
<td>MyIntranet &gt; MyIntranet MyIntranet &gt; Internal_Clear Internal_Clear &gt; MyIntranet</td>
<td>Any</td>
<td>accept</td>
</tr>
</tbody>
</table>

**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 SmartDashboard, go to Policy > Global Properties > VPN > Advanced.
2. Select the Enable VPN Directional Match in VPN Column option.
3. In SmartDashboard, 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 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 SmartDashboard, add a rule that allows traffic to the VPN community (or all communities) using the OSPF service.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow OSPF</td>
<td>Any</td>
<td>Any</td>
<td>MyIntranet</td>
<td>ospf</td>
<td>accept</td>
</tr>
</tbody>
</table>

**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>
```
<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>interface</strong></td>
<td>Configures a physical or virtual interface</td>
</tr>
<tr>
<td><strong>6in4</strong></td>
<td>Configures a 6in4 tunnel for IPv6 traffic over an IPv4 network</td>
</tr>
<tr>
<td><strong>6to4</strong></td>
<td>Configures a 6to4 tunnel for IPv6 traffic over an IPv4 network</td>
</tr>
<tr>
<td><strong>remote</strong></td>
<td>Sets the remote IP address for a 6in4 or 6to4 tunnel</td>
</tr>
<tr>
<td><strong>ttl</strong></td>
<td>Sets the time-to-live value for a 6in4 or 6to4 tunnel</td>
</tr>
<tr>
<td><strong>alias</strong></td>
<td>Assigns more than one IP addresses to a physical interface (IPv4 only)</td>
</tr>
<tr>
<td><strong>loopback</strong></td>
<td>Assigns an IP address to a logical loopback interface. This can be useful as a proxy for an unnumbered interface.</td>
</tr>
<tr>
<td><strong>vlan</strong></td>
<td>Assigns a VLAN tag to an existing physical interface to create a logical subnet.</td>
</tr>
<tr>
<td><strong>ipv4-address</strong></td>
<td>Assigns the IPv4 or IPv6 address</td>
</tr>
<tr>
<td><strong>ipv6-address</strong></td>
<td>Assigns the IPv4 or IPv6 address</td>
</tr>
<tr>
<td><strong>ipv6-autoconfig</strong></td>
<td>If on, automatically gets the IPv6 address from the DHCP</td>
</tr>
<tr>
<td><strong>mask-length</strong></td>
<td>Configures IPv4 or IPv6 subnet mask length using CIDR (/xx) notation</td>
</tr>
<tr>
<td><strong>subnet-mask</strong></td>
<td>Configures IPv4 subnet mask using dotted decimal notation</td>
</tr>
<tr>
<td><strong>comments</strong></td>
<td>Adds free text comments to an interface definition</td>
</tr>
<tr>
<td><strong>mac-addr</strong></td>
<td>Configures the interface hardware MAC address</td>
</tr>
<tr>
<td><strong>mtu</strong></td>
<td>Configure the Maximum Transmission Unit size for an interface</td>
</tr>
<tr>
<td><strong>state</strong></td>
<td>Sets interfaces status to on (enabled) or off (disabled).</td>
</tr>
<tr>
<td><strong>link-speed</strong></td>
<td>Configures the interface link speed and duplex status</td>
</tr>
<tr>
<td><strong>auto-negotiation</strong></td>
<td>Configures automatic negotiation of interface link speed and duplex settings - on (enabled) or off (disabled)</td>
</tr>
</tbody>
</table>
### Parameter Values

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Tunnel ID&gt;</td>
<td>Unique tunnel identifier (Integer in the range 2-4094)</td>
</tr>
<tr>
<td>&lt;IP&gt;</td>
<td>IPv4 or IPv6 address</td>
</tr>
<tr>
<td>&lt;IF&gt;</td>
<td>Interface name</td>
</tr>
<tr>
<td>&lt;Time&gt;</td>
<td>TTL time in seconds in the range 0-255 (default = 0)</td>
</tr>
<tr>
<td>&lt;VLAN ID&gt;</td>
<td>Integer in the range 2-4094</td>
</tr>
<tr>
<td>&lt;Mask&gt;</td>
<td>Interface net mask in dotted decimal or CIDR (/xx) notation as applicable</td>
</tr>
<tr>
<td>&lt;MAC&gt;</td>
<td>Manually enter the applicable hardware address</td>
</tr>
<tr>
<td>&lt;MTU Setting&gt;</td>
<td>Integer greater or equal to 68 (Default = 1500)</td>
</tr>
<tr>
<td>&lt;Speed&gt;</td>
<td>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</td>
</tr>
</tbody>
</table>

### Examples
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: 1024, 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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>static</td>
<td>Configured static arp entries</td>
</tr>
<tr>
<td>dynamic</td>
<td>Configured dynamic arp entries</td>
</tr>
<tr>
<td>ipv4-address</td>
<td>IP Address of a static ARP entry. Range: Dotted-quad ([0-255].[0-255].[0-255].[0-255]). Default: No Default</td>
</tr>
<tr>
<td>macaddress</td>
<td>The hardware address used when forwarding packets to the given IP address. Range: Six hexadecimal octets separated by colon. Default: No Default</td>
</tr>
<tr>
<td>table validity-timeout</td>
<td>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)</td>
</tr>
<tr>
<td>table cache-size</td>
<td>This is the maximum number of entries in the ARP cache. Default: 1024, Range: 1024-16384</td>
</tr>
</tbody>
</table>

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 allocates 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 will assign to hosts.
7. Optional: Define a Default Lease in seconds, for host IPv4 addresses. This is applied 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)

**Description**  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
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>subnet VALUE</td>
<td>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</td>
</tr>
<tr>
<td>netmask VALUE</td>
<td>The IPv4 subnet mask in CIDR notation. For example, 24</td>
</tr>
<tr>
<td>start VALUE</td>
<td>The IPv4 address that starts the allocated IP Pool range. For example 192.0.2.20</td>
</tr>
<tr>
<td>end VALUE</td>
<td>The IPv4 address that ends the allocated IP Pool range. For example 192.0.2.90</td>
</tr>
<tr>
<td>include-ip-pool VALUE</td>
<td>The range of IPv4 addresses to include in the IP pool. For example 192.0.2.20–192.0.2.90</td>
</tr>
<tr>
<td>exclude-ip-pool VALUE</td>
<td>The range of IPv4 addresses to exclude from the IP pool. For example: 192.0.2.155–192.0.2.254</td>
</tr>
<tr>
<td>enable</td>
<td>Enable the DHCP Server subnet, or the DHCP Server process (depending on the context).</td>
</tr>
<tr>
<td>disable</td>
<td>Disable the DHCP Server subnet, or the DHCP Server process (depending on the context).</td>
</tr>
<tr>
<td>default-lease VALUE</td>
<td>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.</td>
</tr>
<tr>
<td>max-lease VALUE</td>
<td>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.</td>
</tr>
<tr>
<td>default-gateway VALUE</td>
<td>The IPv4 address of the default gateway for the network hosts</td>
</tr>
<tr>
<td>domain VALUE</td>
<td>The domain name of the network hosts. For example, example.com.</td>
</tr>
<tr>
<td>dns VALUE</td>
<td>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</td>
</tr>
<tr>
<td>all</td>
<td>All DHCP server configuration settings.</td>
</tr>
<tr>
<td>subnets</td>
<td>DHCP Server subnet configuration settings.</td>
</tr>
<tr>
<td>subnet VALUE ip-pools</td>
<td>The IP pools in the DHCP Server subnet, and their status: Enabled or Disabled.</td>
</tr>
<tr>
<td>status</td>
<td>The status of the DHCP Server process: Enabled or disabled.</td>
</tr>
</tbody>
</table>

**Example**

gw-9403be> show dhcp server all
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.
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name VALUE</td>
<td>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 may not end in a dash or a period. There is no default value.</td>
</tr>
<tr>
<td>ipv4-address VALUE</td>
<td>The IPv4 address of the host</td>
</tr>
<tr>
<td>ipv6-address VALUE</td>
<td>The IPv6 address of the host</td>
</tr>
</tbody>
</table>

Domain Name Service (DNS)

Gaia uses the Domain Name Service (DNS) to translate host names into IP addresses. To enable DNS lookups, you must specify the primary DNS server for your system. You can also specify secondary and tertiary DNS servers. When resolving host names, the system 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:
   a) DNS Suffix. The name that is put at the end of all DNS searches if they fail. By default, it should 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 may 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 allowed.

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

b) IPv4 address or IPv6 of the **Primary DNS Server**. The server to use when resolving hostnames. This should be a host running a DNS server.

c) (Optional) IPv4 or IPv6 address of the **Secondary DNS Server**. The server to use when resolving hostnames if the primary server does not respond. This should be a host running a DNS server.

d) (Optional) IPv4 or IPv6 address of the **Tertiary DNS Server**. The server to use when resolving hostnames if the primary and secondary servers do not respond. This should be a host running 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>primary</strong></td>
<td>The server to use when resolving hostnames. This should be a host running a DNS server. An IPv4 or IPv6 address.</td>
</tr>
<tr>
<td><strong>secondary</strong></td>
<td>The server to use when resolving hostnames if the primary server does not respond. This should be a host running a DNS server. An IPv4 or IPv6 address.</td>
</tr>
<tr>
<td><strong>tertiary</strong></td>
<td>The server to use when resolving hostnames if the primary and secondary servers do not respond. This should be a host running a DNS server. An IPv4 or IPv6 address.</td>
</tr>
<tr>
<td><strong>suffix</strong></td>
<td>The name that is put at the end of all DNS searches if they fail. By default, it should 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 may consist only of alphanumeric characters and hyphens. The domain name syntax is described in RFC 1035 [modified slightly in RFC 1123]. <strong>Note:</strong> Domain names that are also valid numeric IP addresses, for example 10.19.76.100, though syntactically correct, are not allowed. For example, if you set the DNS Suffix to example.com and try to ping some host foo (by running ping foo), and foo cannot be resolved, then the resolving computer will try to resolve foo.example.com.</td>
</tr>
</tbody>
</table>

### 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 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 selecting 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>
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nexthop</td>
<td>Defines the next hop path, which can be a gateway, blackhole or reject.</td>
</tr>
<tr>
<td>gateway</td>
<td>Accepts and sends packets to the specified destination.</td>
</tr>
<tr>
<td>blackhole</td>
<td>Drops packets, but does not send an error message.</td>
</tr>
<tr>
<td>reject</td>
<td>Drops packets and sends an error message to the traffic source.</td>
</tr>
<tr>
<td>address</td>
<td>Identifies the next hop gateway by its IP address.</td>
</tr>
<tr>
<td>logical</td>
<td>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.</td>
</tr>
<tr>
<td>priority</td>
<td>Assigns a path priority when there are many different paths. The available path with the lowest priority value is selected.</td>
</tr>
<tr>
<td>on</td>
<td>Adds the specified route or next hop.</td>
</tr>
<tr>
<td>off</td>
<td>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.</td>
</tr>
<tr>
<td>rank</td>
<td>Selects a route when 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.</td>
</tr>
<tr>
<td>scopelocal</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Destination&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;GW IP&gt;</td>
<td>Gateway IP address in dotted decimal notation in dotted decimal format without a net mask.</td>
</tr>
<tr>
<td>&lt;GW IF&gt;</td>
<td>Name of the interface that connects to the next hop gateway.</td>
</tr>
<tr>
<td>&lt;P Value&gt;</td>
<td>Priority. An integer between 1 and 8 (default=1).</td>
</tr>
<tr>
<td>&lt;Rank Value&gt;</td>
<td>Rank. An integer between 0 and 255 (default=0).</td>
</tr>
</tbody>
</table>
Examples

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 192.0.2.100 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:

type: 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 ID - 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 (ipv6 static-route)

This section includes a complete command reference for the `ipv6 static-route` command. You can only use the `set` operation with this command, even when adding or deleting a static route.

**Description**
Add, change or delete an IPv4 static route.

**Syntax**
```
set ipv6 static-route <Destination>
   nexthop gateway <GW IP>
   [priority <P Value>] on|off
   interface <GW IF> [priority <P Value>] on|off
   nexthop blackhole
   nexthop reject
   off
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nexthop</td>
<td>Defines the next hop path.</td>
</tr>
<tr>
<td>on</td>
<td>Enables the specified route or next hop.</td>
</tr>
<tr>
<td>off</td>
<td>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.</td>
</tr>
<tr>
<td>gateway</td>
<td>Accepts and sends packets to the specified destination.</td>
</tr>
<tr>
<td>blackhole</td>
<td>Drops packets, but does not send an error message.</td>
</tr>
<tr>
<td>reject</td>
<td>Drops packets and sends an error message to the traffic source.</td>
</tr>
<tr>
<td>interface</td>
<td>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.</td>
</tr>
<tr>
<td>priority</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Value**

- `<Destination>`: Destination IP address.
- `<Route Type>`: gateway - Accepts and sends packets to the specified destination.
  reject - Drops packets and sends an error message to the traffic source.
  blackhole - Drops packets, but does not send an error message.
- `<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.
- `<P Value>`: Integer value between 1 and 8 (default=1).
**Examples**

set ipv6 static-route 3100:192::0/64 nexthop 3900:172::1 priority 2 on

set ipv6 static-route 3100:192::0/64 nexthop 3900:172::1 interface eth3 priority 2 on

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

set ipv6 static-route 3300:123::0/64 nexthop blackhole

**Comments**

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

---

**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
```

<table>
<thead>
<tr>
<th>Codes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Connected, S - Static, B - BGP, Rg - RIPng, A - Aggregate, O - OSPFv3 IntraArea (IA - InterArea, E - External), K - Kernel Remnant, H - Hidden, P - Suppressed</td>
</tr>
</tbody>
</table>

| 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
```

**Destination** - Destination IPv6 address.

**GW IP** - Next hop gateway IPv6 address.

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

**Destination** - Destination IPv6 address.

**GW IP** - Next hop gateway interface name.

**Example:**

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>The IPv4 address to which NetFlow packets are sent. This is mandatory.</td>
</tr>
<tr>
<td>UDP port Number</td>
<td>The UDP port number on which the collector is listening. This is mandatory.</td>
</tr>
<tr>
<td>Export format</td>
<td>The NetFlow protocol version to send: 5 or 9. Each has a different packet format. The default is 9.</td>
</tr>
<tr>
<td>Source IP address</td>
<td><strong>Optional:</strong> 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.</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip VALUE</td>
<td>The IPv4 address to which NetFlow packets are sent. This is mandatory.</td>
</tr>
<tr>
<td>port VALUE</td>
<td>The UDP port number on which the collector is listening. This is mandatory. There is no default or standard port number for NetFlow.</td>
</tr>
<tr>
<td>srcaddr VALUE</td>
<td><strong>Optional:</strong> 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.</td>
</tr>
<tr>
<td>export-format VALUE</td>
<td>The NetFlow protocol version to send: 5 or 9. Each has a different packet format. The default is 9.</td>
</tr>
<tr>
<td>for-ip VALUE</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 [R77 Performance Optimization Guide](http://supportcontent.checkpoint.com/documentation_download?ID=24808).
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`.

System Management

In This Section:

Time ............................................................................................................................... 84  
Cloning Groups ............................................................................................................. 88  
SNMP ............................................................................................................................. 95  
Job Scheduler ............................................................................................................. 107  
Mail Notification .......................................................................................................... 109  
Messages .................................................................................................................... 110  
Session ........................................................................................................................ 112  
Core Dumps ................................................................................................................ 112  
System Configuration ................................................................................................. 114  
System Logging .......................................................................................................... 115  
Network Access .......................................................................................................... 117  
Configuring the WebUI Web server ........................................................................... 118  
Host Access ................................................................................................................ 120

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. We recommend that you 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

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

#### Example

```
show ntp servers
```

#### Output

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool.ntp.org</td>
<td>Primary</td>
<td>4</td>
</tr>
</tbody>
</table>

#### 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. 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock</td>
<td>The current system day, date, and time. The current system time is in HH:MM:SS format.</td>
</tr>
</tbody>
</table>

#### 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;date&gt;</td>
<td>The date in the YYYY-MM-DD format.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;time of day&gt;</td>
<td>The current system time in HH:MM:SS format</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Area&gt;</td>
<td>Continent or geographic area. Valid values: Africa, America, Antarctica, Asia, Atlantic, Australia, Europe, Indian, Pacific</td>
</tr>
<tr>
<td>&lt;Region&gt;</td>
<td>Region within the specified area.</td>
</tr>
</tbody>
</table>

**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
- ARP
- 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
- BGP
- IGMP
- PIM
- Static Multicast Routes
- RIP
- OSPF
- IPv6 OSPF
- Route Aggregation
- Inbound Route Filters
- Route Redistribution
- Route Map
- Routing Options
- Policy Based Routing
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 SmartDashboard, 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 SmartDashboard, 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 clish 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.

To join a Cloning Group:
1. Open the Gaia gateway WebUI.
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.
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>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local-ip &lt;IPv4 address&gt;</td>
<td>The IPv4 address used to synchronize shared features between members of the Cloning Group.</td>
</tr>
<tr>
<td>mode &lt;manual</td>
<td>cluster-xl&gt;</td>
</tr>
<tr>
<td>name &lt;Cloning Group_name&gt;</td>
<td>Name of the Cloning Group.</td>
</tr>
<tr>
<td>password</td>
<td>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.</td>
</tr>
<tr>
<td>state on</td>
<td>off</td>
</tr>
</tbody>
</table>

To add Shared Features
Run this command: `add cloning-group shared-feature <feature>`
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>feature</td>
<td>The name of the feature to be synchronized between the members of the Cloning Group:</td>
</tr>
<tr>
<td></td>
<td>• aggregate</td>
</tr>
<tr>
<td></td>
<td>• bgp</td>
</tr>
<tr>
<td></td>
<td>• bootp</td>
</tr>
<tr>
<td></td>
<td>• cron</td>
</tr>
<tr>
<td></td>
<td>• dns</td>
</tr>
<tr>
<td></td>
<td>• hosts</td>
</tr>
<tr>
<td></td>
<td>• igmp</td>
</tr>
<tr>
<td></td>
<td>• inboundfilters</td>
</tr>
<tr>
<td></td>
<td>• time</td>
</tr>
<tr>
<td></td>
<td>• ntp</td>
</tr>
<tr>
<td></td>
<td>• message</td>
</tr>
<tr>
<td></td>
<td>• ospf</td>
</tr>
<tr>
<td></td>
<td>• ospf3</td>
</tr>
<tr>
<td></td>
<td>• password-controls</td>
</tr>
<tr>
<td></td>
<td>• mailrelay</td>
</tr>
<tr>
<td></td>
<td>• display-format</td>
</tr>
<tr>
<td></td>
<td>• http</td>
</tr>
<tr>
<td></td>
<td>• net-access</td>
</tr>
<tr>
<td></td>
<td>• users-and-roles</td>
</tr>
<tr>
<td></td>
<td>• arp</td>
</tr>
<tr>
<td></td>
<td>• syslog</td>
</tr>
<tr>
<td></td>
<td>• proxy</td>
</tr>
<tr>
<td></td>
<td>• host-access</td>
</tr>
<tr>
<td></td>
<td>• pbr</td>
</tr>
<tr>
<td></td>
<td>• pim</td>
</tr>
<tr>
<td></td>
<td>• redistribution</td>
</tr>
<tr>
<td></td>
<td>• rip</td>
</tr>
<tr>
<td></td>
<td>• routemap</td>
</tr>
<tr>
<td></td>
<td>• routingoptions</td>
</tr>
<tr>
<td></td>
<td>• static</td>
</tr>
<tr>
<td></td>
<td>• static-mroute</td>
</tr>
<tr>
<td></td>
<td>• snmp</td>
</tr>
</tbody>
</table>
To delete Shared Features

Run this command: `delete cloning-group shared feature <feature>`
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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  
  • arp  
  • 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>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4_address</td>
<td>The IPv4 address of a member of the Cloning Group.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This option is not available if you are logged into the cadmin account.</td>
</tr>
</tbody>
</table>

To remove a member from a Cloning Group:

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

To view Cloning Group Attributes:

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

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

To re-synchronize a Cloning Group:

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

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:

<table>
<thead>
<tr>
<th>MIB</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard MIBs</td>
<td>/usr/share/snmp/mibs</td>
</tr>
<tr>
<td>Check Point MIBs</td>
<td>$CPDIR/lib/snmp</td>
</tr>
<tr>
<td>Check Point Gaia trap MIBs</td>
<td>/etc/snmp</td>
</tr>
</tbody>
</table>

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](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). It is recommended to 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:

<table>
<thead>
<tr>
<th>Type of Trap</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>coldStart</td>
<td>Notifies when the SNMPv2 agent is re-initialized.</td>
</tr>
<tr>
<td>linkUpLinkDown</td>
<td>Notifies when one of the links changes state to up or down.</td>
</tr>
<tr>
<td>authorizationError</td>
<td>Notifies when an SNMP operation is not properly authenticated.</td>
</tr>
<tr>
<td>configurationChange</td>
<td>Notifies when a change to the system configuration is applied.</td>
</tr>
<tr>
<td>configurationSave</td>
<td>Notifies when a permanent change to the system configuration occurs.</td>
</tr>
<tr>
<td>Type of Trap</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>lowDiskSpace</td>
<td>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.</td>
</tr>
<tr>
<td>powerSupplyFailure</td>
<td>Notifies when a power supply for the system fails. This trap is supported only on platforms with two power supplies installed and running.</td>
</tr>
<tr>
<td>fanFailure</td>
<td>Notifies when a CPU or chassis fan fails.</td>
</tr>
<tr>
<td>overTemperature</td>
<td>Notifies when the temperature rises above the threshold.</td>
</tr>
<tr>
<td>highVoltage</td>
<td>Notify if one of the voltage sensors exceeds its maximum value.</td>
</tr>
<tr>
<td>lowVoltage</td>
<td>Notify if one of the voltage sensors falls below its minimum value.</td>
</tr>
<tr>
<td>raidVolumeState</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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.
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 Pass Phrase, enter a password for the user that is between 8 and 128 characters in length.
7. 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.
8. 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> (for version R77.10 and higher)
- add snmp address <IP_address> (for version R77 and earlier)

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 for you to enter a password.
ss-phrase VALUE

Important - We do not recommend the following command because the passwords are stored as plain text in the command history:
add snmp usm user VALUE security-level authPriv
auth-pass-phrase VALUE privacy-pass-phrase VALUE

To export an authNoPriv snmp user to another Gaia system use:
add snmp usm user VALUE security-level authNoPriv
auth-pass-phrase-hashed VALUE

Get the hashed password by running:
show configuration snmp

add snmp usm user VALUE security-level authPriv

This opens an interactive dialog for you to enter passwords.

To export an authPriv snmp user to another Gaia system use:
add snmp usm user VALUE security-level authPriv
auth-pass-phrase-hashed VALUE privacy-pass-phrase-hashed VALUE

Get the hashed password by running:
show configuration snmp

Set Commands:
set snmp usm user VALUE security-level authNoPriv
auth-pass-phrase VALUE

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp agent</td>
<td>on or off to enable or disable.</td>
</tr>
<tr>
<td>snmp agent-version</td>
<td>any or v3-Only</td>
</tr>
<tr>
<td>location</td>
<td>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</td>
</tr>
<tr>
<td>contact</td>
<td>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</td>
</tr>
<tr>
<td>snmp address</td>
<td>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.</td>
</tr>
<tr>
<td>snmp interface</td>
<td>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.</td>
</tr>
<tr>
<td>community &lt;c_name&gt; read-only</td>
<td>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 <strong>public</strong>. We recommend that you assign community names based on industry-standard password conventions.</td>
</tr>
<tr>
<td>community &lt;c_name&gt; read-write</td>
<td>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 <strong>public</strong>. We recommend that you assign community names based on industry-standard password conventions.</td>
</tr>
<tr>
<td>usm user</td>
<td>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.</td>
</tr>
<tr>
<td>authNoPriv</td>
<td>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 <code>set snmp usm user &lt;name&gt; &lt;usm-read-only / usm-read-write&gt;</code></td>
</tr>
<tr>
<td>authPriv</td>
<td>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 &lt;name&gt; &lt;usm-read-only / usm-read-write&gt;</code></td>
</tr>
<tr>
<td>auth-pass-phrase</td>
<td>A password for the user that is between 8 and 128 characters in length.</td>
</tr>
<tr>
<td>auth-pass-phrase-hashed</td>
<td>A hashed password which is the output of the command <code>show configuration snmp</code></td>
</tr>
<tr>
<td>privacy-pass-phrase</td>
<td>A pass phrase that is between 8 and 128 characters in length. Used for protection against disclosure of SNMP message payloads.</td>
</tr>
<tr>
<td>privacy-pass-phrase-hashed</td>
<td>A hashed password which is the output of the command <code>show configuration snmp</code></td>
</tr>
<tr>
<td>usm users</td>
<td>All USM users</td>
</tr>
<tr>
<td>traps receiver</td>
<td>IP address selected to receive traps sent by the agent.</td>
</tr>
<tr>
<td>community</td>
<td>Set a string</td>
</tr>
<tr>
<td>traps trap</td>
<td>The trap name</td>
</tr>
<tr>
<td>polling-frequency</td>
<td>The polling frequency in seconds. Default is 20 seconds.</td>
</tr>
<tr>
<td>trap-user</td>
<td>The user which generates the traps.</td>
</tr>
</tbody>
</table>
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 98).

- In `auth-pass-phrase` and `privacy-pass-phrase`, notice the different options for regular and hashed pass phrase:
  `auth-pass-phrase` and `auth-pass-phrasehashed`
  `privacy-pass-phrase` and `privacy-pass-phrasehashed`

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.

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

⚠️ 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.

<table>
<thead>
<tr>
<th>Variable-bindings element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Value that is associated with each object instance; specified in a PDU request.</td>
</tr>
<tr>
<td>unSpecified</td>
<td>A NULL value is used in retrieval requests.</td>
</tr>
<tr>
<td>noSuchObject</td>
<td>Indicates that the agent does not implement the object referred to by this object identifier.</td>
</tr>
<tr>
<td>noSuchInstance</td>
<td>Indicates that this object does not exist for this operation.</td>
</tr>
<tr>
<td>endOfMIBView</td>
<td>Indicates an attempt to reference an object identifier that is beyond the end of the MIB at the agent.</td>
</tr>
</tbody>
</table>

**GetRequest**

The following table lists possible value field sets in the response PDU or error-status messages when performing a GetRequest.

<table>
<thead>
<tr>
<th>Value Field Set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>noSuchObject</td>
<td>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>.</td>
</tr>
<tr>
<td>noSuchInstance</td>
<td>If the variable’s name does not exactly match the name of a variable, its value field is set to <code>noSuchInstance</code>.</td>
</tr>
<tr>
<td>genErr</td>
<td>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.</td>
</tr>
<tr>
<td>tooBig</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 110).

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**
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 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>job</td>
<td>The name of the job.</td>
</tr>
<tr>
<td>command</td>
<td>The name of the command.</td>
</tr>
<tr>
<td>recurrence daily time</td>
<td>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.</td>
</tr>
</tbody>
</table>
To specify a job for once a month, enter \texttt{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.

To specify a job for once a week, enter \texttt{recurrence\ weekly\ days}, and the day by number, when 0 is Sunday and 6 is Saturday.

Specify a job that will run at every system startup.

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.

To specify the time, enter the time in the twenty four hour clock format. For example: 14:00.

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 110).

\textbf{Comments} Only Show commands provide an output.

\section*{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
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>The IP address or hostname of the mail server to receive mail notifications. For example: mail.company.com</td>
</tr>
<tr>
<td>username</td>
<td>The username on the mail server that receives the admin or monitor mail notifications. For example: <a href="mailto:user@mail.company.com">user@mail.company.com</a></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th></th>
<th>Banner Message</th>
<th>Message of the Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Message</td>
<td>“This system is for authorized use only”</td>
<td>“You have logged into the system”</td>
</tr>
<tr>
<td>When shown in WebUI</td>
<td>Browser login page, before logging in</td>
<td>After logging in to the system</td>
</tr>
<tr>
<td>When shown in clish</td>
<td>When logging in, before entering the password</td>
<td>After logging in to the system</td>
</tr>
<tr>
<td>Default state</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
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)

<table>
<thead>
<tr>
<th>Description</th>
<th>Manage inactivity timeout (in minutes) for the command line shell.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>set inactivity-timeout VALUE</td>
</tr>
<tr>
<td></td>
<td>show inactivity-timeout</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>inactivity-timeout</td>
<td>The inactivity timeout (in minutes) for the command line.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total space limit</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range</strong>: 0-99999 MB</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: 1000 MB</td>
</tr>
<tr>
<td>Dumps per process</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range</strong>: 0 - 99999</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: 2</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total VALUE</td>
<td>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.</td>
</tr>
<tr>
<td>• Range: 0-99999 MB</td>
<td>• Default: 1000 MB</td>
</tr>
<tr>
<td>per_process VALUE</td>
<td>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 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.</td>
</tr>
<tr>
<td>• Range: 0 - 99999</td>
<td>• Default: 2</td>
</tr>
</tbody>
</table>

### 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.
3. Create IPv6 objects in SmartDashboard.

### 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.

<table>
<thead>
<tr>
<th>Description</th>
<th>Use this command to enable or disable IPv6 support.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>set ipv6-state off</td>
</tr>
<tr>
<td></td>
<td>set ipv6-state on</td>
</tr>
<tr>
<td></td>
<td>show ipv6-state</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>off</td>
</tr>
</tbody>
</table>
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
<table>
<thead>
<tr>
<th>syslog</th>
<th>Configures the system logging.</th>
</tr>
</thead>
<tbody>
<tr>
<td>log-remote-address</td>
<td>Configures remote IP address for system logging.</td>
</tr>
<tr>
<td>level</td>
<td>Filters a severity level for the system logging.</td>
</tr>
<tr>
<td>filename</td>
<td>Configures or shows the file name of the system log.</td>
</tr>
<tr>
<td>&lt;remote ip&gt;</td>
<td>IP address of remote computer.</td>
</tr>
<tr>
<td>&lt;severity&gt;</td>
<td>syslog severity level. These are the legal values:</td>
</tr>
<tr>
<td></td>
<td>• emerg</td>
</tr>
<tr>
<td></td>
<td>• alert</td>
</tr>
<tr>
<td></td>
<td>• crit</td>
</tr>
<tr>
<td></td>
<td>• err</td>
</tr>
<tr>
<td></td>
<td>• warning</td>
</tr>
<tr>
<td></td>
<td>• notice</td>
</tr>
<tr>
<td></td>
<td>• info</td>
</tr>
<tr>
<td></td>
<td>• debug</td>
</tr>
<tr>
<td></td>
<td>• all</td>
</tr>
<tr>
<td>&lt;file&gt;</td>
<td>System log file name.</td>
</tr>
</tbody>
</table>

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.

### 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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>daemon-enable</td>
<td>on or off</td>
</tr>
</tbody>
</table>

**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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session-timeout</td>
<td>VALUE</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssl-port VALUE</td>
<td>Integers between 1 and 65535 inclusive. Default: &quot;443&quot;.</td>
</tr>
</tbody>
</table>

**Comments**
Use this command for initial configuration only. Changing the port number on the command line may cause inconsistency with the setting defined in SmartDashboard. Use SmartDashboard 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**
```
show web daemon-enable
```

**Output**
```
gw-gaia> show web daemon-enable
WebDaemonEnable on
```

Showing the web session-timeout

**Description**
Use this command to show the state of the web session time-out

**Syntax**
```
show web session-timeout
```

**Output**
```
gw-gaia> show web session-timeout
WebSessionTimeout 99
```

Showing the web SSL-port

**Description**
Use this command to show the web SSL-port

**Syntax**
```
show web ssl-port
```

**Output**
```
gw-gaia> show web ssl-port
web-ssl-port 443
```
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4-address</td>
<td>The IPv4 address of the allowed host</td>
</tr>
<tr>
<td>mask-length</td>
<td>The mask-length of the allowed network</td>
</tr>
</tbody>
</table>

**Example**

```
gw-gaia> add allowed-client host any-host
```

**Output**

```
gw-gaia> show allowed-client all

Type       Address          Mask Length
Host        Any
```

```
gw-gaia>
```
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, using PIM (Sparse Mode (SM), Dense Mode (DM) and Source-Specific Multicast (SSM)) and IGMP.

User Management

In This Section:

- Change My Password ................................................................................................. 122
- Users ........................................................................................................................... 123
- Roles ............................................................................................................................ 127
- Password Policy .......................................................................................................... 131
- Authentication Servers ............................................................................................... 140
- System Groups ............................................................................................................ 149
- GUI Clients .................................................................................................................. 151

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 his or her own 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 127).

**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`
User Management

• 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**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Name</td>
<td>Name used to identify the user. The valid characters are alphanumeric characters, dash (-), and underscore (_).</td>
</tr>
<tr>
<td></td>
<td><strong>Range:</strong> 1-32 characters</td>
</tr>
<tr>
<td>Real Name</td>
<td>User’s real name or other informative label.</td>
</tr>
<tr>
<td>Home directory</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Shell            | • /etc/cli.sh - User is allowed to use the full Gaia CLI (clish). This is the default option. By default, some basic networking commands (such as ping) are also available. The *Extended Commands mechanism* makes it possible to add Linux commands that can be used. User can run shell to enter the bash shell.  
|                  | • /bin/bash, /bin/csh, /bin/sh, /bin/tcsh - Standard Linux shells. User can run clish to enter the clish shell.  
|                  | • /usr/bin/scponly - User is allowed to log in only using SCP, and to transfer files to and from the system. No other commands are allowed.  
<p>|                  | • /sbin/nologin - User is not allowed to log in.                            |
| Password         | Use this field to enter a new password if you are changing it.              |
|                  | <strong>Range:</strong> 6-128 characters. All printable characters are allowed.          |
|                  | <strong>Note</strong> - If you use an asterisk (*) in a password, users with that password are unable to log in. |
| Reset Password   | Change the user password.                                                  |
|                  | <strong>Important</strong> - After resetting the password, tell the user to immediately change their password in User Management &gt; Change My Password. |
| Confirm Password | Re-enter the new password if you are changing it.                           |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User must change password at next logon</td>
<td><strong>Important</strong> - After selecting this option, tell the user to immediately change their password in <em>User Management &gt; Change My Password</em>.</td>
</tr>
<tr>
<td>Access Mechanisms</td>
<td>Choose whether the user is able to access Gaia from the command line, from the WebUI, both, or neither.</td>
</tr>
<tr>
<td>Roles</td>
<td>Assign a role to the user. Define the roles in <em>User Management &gt; Roles</em>.</td>
</tr>
</tbody>
</table>

**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:

```bash
add user <username> uid <user_ID> homedir <dir>
```

To modify a user account:

```bash
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:

```bash
delete user <user_ID>
```

To view summary information about all users:

```bash
show users
```

To view information about a user

```bash
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>]
```

**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.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user <code>&lt;username&gt;</code></td>
<td>Unique login username - an alphanumeric string, 1 to 32 characters long, that can contain dashes (-) and underscores (_), but not spaces.</td>
</tr>
<tr>
<td>force-password-change</td>
<td>If set to yes, forces the user to change their password on the next login.</td>
</tr>
<tr>
<td>gid <code>&lt;group_ID&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td>homedir <code>&lt;dir&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td>lock-out off</td>
<td>Unlock the user, if the user was locked-out. The password expiration date is adjusted, if necessary.</td>
</tr>
<tr>
<td>newpass <code>&lt;passwd&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td>password</td>
<td>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.</td>
</tr>
<tr>
<td>password-hash <code>&lt;hash&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td>realname <code>&lt;name&gt;</code></td>
<td>User description, most commonly user’s real name - an alphanumeric string that can contain spaces. The default is the username with capitalized first letter.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>shell &lt;login_sh&gt;</td>
<td>User’s command interpreter [shell], which is invoked when the user logs in. The default shell is /etc/cli.sh 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. /bin/bash, /bin/csh, /bin/sh, /bin/tcsh - Standard Linux shells. To switch to the clish shell, the user has to run the command clish. /usr/bin/scponly - User is allowed to log in only using SCP, and to transfer files to and from the system. No other commands are allowed. /sbin/nologin - User is not allowed to log in.</td>
</tr>
<tr>
<td>uid &lt;user_ID&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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 a 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**

```plaintext
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 <List>

delete rba user <User Name> access-mechanisms [Web-UI | CLI]
delete rba user <User Name> roles <List>
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role &lt;Name&gt;</td>
<td>Role name as a character string that contains letters, numbers or the underscore (_) character. The role name must with a letter.</td>
</tr>
<tr>
<td>Domain-type System</td>
<td>Reserved for future use.</td>
</tr>
<tr>
<td>readonly-features</td>
<td>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.</td>
</tr>
<tr>
<td>readwrite-features</td>
<td>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.</td>
</tr>
<tr>
<td>user &lt;User name&gt;</td>
<td>User to which access mechanism permissions and roles are assigned.</td>
</tr>
<tr>
<td>roles &lt;List&gt;</td>
<td>Comma separated list of role names that are assigned to or removed from the specified user.</td>
</tr>
<tr>
<td>access-mechanisms</td>
<td>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.</td>
</tr>
</tbody>
</table>
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:

```bash
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 network 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 122).

## Password Strength

Strong, unique passwords that use a variety of character types and require password changes, are key factors in your overall network 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 132)
   - **Password History** (on page 133)
   - **Mandatory Password change** (on page 133)
   - **Deny Access to Unused Accounts** (on page 134)
   - **Deny Access After Failed Login Attempts** (on page 134)
3. Click **Apply**.

**Password Strength**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimum Password Length</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 6-128</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 6</td>
</tr>
</tbody>
</table>
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" effectively disables this check. Changes to this setting do not affect existing passwords.

- **Range**: 1-4
- **Default**: 2

**Password History**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check for Password Reuse</td>
<td>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 <strong>History length</strong>. Does not apply to SNMP passwords. Enables or disables password history checking and password history recording, for all users.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: Selected.</td>
</tr>
<tr>
<td>History Length</td>
<td>The number of former passwords to keep and check against for each user.</td>
</tr>
<tr>
<td></td>
<td><strong>Range</strong>: 1-1000.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 10.</td>
</tr>
</tbody>
</table>

**Mandatory Password Change**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Expiration</td>
<td>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 <strong>never</strong>, passwords do not expire. Does not apply to SNMP users.</td>
</tr>
<tr>
<td></td>
<td><strong>Range</strong>: 1-1827 or Password never expire.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: Password never expire.</td>
</tr>
<tr>
<td>Warn users before password expiration</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Range</strong>: 1-366.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 7.</td>
</tr>
</tbody>
</table>
**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 `set user <username> password` or from the WebUI User Management > Users page.

- **Default**: Not selected

---

### Deny Access to Unused Accounts

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny access to unused accounts</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: Not selected</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Days of non-use before lock-out</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Range</strong>: 30-1827</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 365</td>
</tr>
</tbody>
</table>

---

### 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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny access after failed login attempts</td>
<td>If the configured limit is reached, the user is locked out [unable to log in] for a configurable period of time.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Allow access again after time</th>
<th>Description</th>
</tr>
</thead>
</table>

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**

```bash
set password-controls
  min-password-length <6-128>
  palindrome-check <on |off>
  complexity <1-4>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>min-password-length &lt;6-128&gt;</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Range:</strong> 6-128</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 6</td>
</tr>
</tbody>
</table>
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 Management

#### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password-expiration &lt;never, 1-1827&gt;</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range:</strong> 1-1827 or never.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default:</strong> never.</td>
</tr>
<tr>
<td>expiration-warning-days &lt;1-366&gt;</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range:</strong> 1-366.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default:</strong> 7.</td>
</tr>
<tr>
<td>expiration-lockout-days &lt;never, 1-1827&gt;</td>
<td>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 set user &lt;username&gt; lock-out.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range:</strong> 1-1827, or never</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default:</strong> never</td>
</tr>
<tr>
<td>force-change-when &lt;no</td>
<td>password&gt;</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range:</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>no</strong> - Disables this functionality.</td>
</tr>
<tr>
<td></td>
<td>• <strong>password</strong> - Forces users to change their password after their password was changed using the command set user &lt;username&gt; password or from the WebUI User Management &gt; Users page.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default:</strong> no</td>
</tr>
</tbody>
</table>

#### Deny Access to Unused Accounts

**set password-controls**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny-on-nonuse enable &lt;off</td>
<td>on&gt;</td>
</tr>
<tr>
<td>deny-on-nonuse allowed-days &lt;30-1827&gt;</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range:</strong> on/off</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default:</strong> off</td>
</tr>
</tbody>
</table>
**Deny Access After Failed Login Attempts**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny-on-fail enable &lt;off</td>
<td>on&gt;</td>
</tr>
<tr>
<td>deny-on-fail failures-allowed &lt;2-1000&gt;</td>
<td>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,</td>
</tr>
</tbody>
</table>

**Note** - These configurations do not apply to the admin user. The admin user is not blocked irrespective of failed login attempts.

- **Range**: on/off
- **Default**: off
- **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

```bash
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
```
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 uses a remote server to authenticate users for Gaia. All information sent to the TACACS+ server is encrypted.

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

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 guide administration Guide.
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>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.</td>
</tr>
<tr>
<td>Host</td>
<td>RADIUS server host name or IP address (IPv4 or IPv6).</td>
</tr>
<tr>
<td>UDP Port</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Warning</strong> - 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.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>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.</td>
</tr>
<tr>
<td>Timeout in Seconds</td>
<td><strong>Optional</strong>: 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.</td>
</tr>
<tr>
<td>Network Access Server (NAS)</td>
<td><strong>Optional</strong>: 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 <a href="http://freeradius.org/rfc/rfc2865.html#NAS-IP-Address">http://freeradius.org/rfc/rfc2865.html#NAS-IP-Address</a>. If no NAS IP Address is chosen, the IPv4 address of the Gaia host is used.</td>
</tr>
<tr>
<td>Super User ID</td>
<td><strong>Optional</strong>: The UID for the RADIUS super user. Select 0 or 96. If the UID is 0 there is no need to run the <strong>sudo</strong> command to get super user permissions (&quot;Configuring RADIUS Servers for Non-Local Gaia Users&quot; on page 144).</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>priority</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>new-priority</strong></td>
<td>The priority of the new RADIUS server</td>
</tr>
<tr>
<td><strong>host</strong></td>
<td>Host name or the IP address (IPv4 or IPv6) of the RADIUS server</td>
</tr>
<tr>
<td><strong>port</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>prompt secret</strong></td>
<td>Shared secret [password] text string. The system prompts you to enter the value.</td>
</tr>
<tr>
<td><strong>timeout</strong></td>
<td>The number of seconds to wait for the server to respond. The default value 3 seconds.</td>
</tr>
<tr>
<td><strong>secret</strong></td>
<td>The shared secret used to authenticate the RADIUS server and the local client. You must define this value on your RADIUS server.</td>
</tr>
<tr>
<td><strong>super-user-uid</strong></td>
<td>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 144).</td>
</tr>
<tr>
<td><strong>NAS-IP</strong></td>
<td>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 <a href="http://freeradius.org/rfc/rfc2865.html#NAS-IP-Address">http://freeradius.org/rfc/rfc2865.html#NAS-IP-Address</a>. If no NAS IP Address is chosen, the IPv4 address of the Gaia host is used.</td>
</tr>
</tbody>
</table>

**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 127).

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Priority</strong></td>
<td>The priority of the TACACS+ server. Must be unique for this operating system. The priority is used to:</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- Identify the server in commands. A command with priority 1 applies to the server with priority 1.</td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>The TACACS+ server IPv4 address.</td>
</tr>
<tr>
<td><strong>Shared Key</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Timeout in Seconds</strong></td>
<td>The maximum number of seconds to wait for the server to respond.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
### 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 127).
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.

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout VALUE</td>
<td>The maximum number of seconds to wait for the server to respond.</td>
</tr>
<tr>
<td>• Range: 1-60.</td>
<td></td>
</tr>
<tr>
<td>• Default: 5</td>
<td></td>
</tr>
<tr>
<td>new-priority VALUE</td>
<td>The new priority.</td>
</tr>
<tr>
<td>state VALUE</td>
<td>Range:</td>
</tr>
<tr>
<td>• On - Enable TACACS+ authentication for all servers.</td>
<td></td>
</tr>
<tr>
<td>• Off - Disable TACACS+ authentication for all servers.</td>
<td></td>
</tr>
<tr>
<td>list</td>
<td>The list of TACACS+ servers that this system is configured to use.</td>
</tr>
</tbody>
</table>

**Example**

`set aaa tacacs-servers priority 2 server 10.10.10.99 key MySharedSecretKey timeout 10`
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 **Cntl+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:


**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 127).

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group VALUE</td>
<td>Name of group. 1-8 alphanumeric characters. Must be unique on your system.</td>
</tr>
<tr>
<td>gid VALUE</td>
<td>Numeric Group ID. Must be unique on your system.</td>
</tr>
<tr>
<td>member VALUE</td>
<td>Name of an existing user. For example, admin or monitor.</td>
</tr>
</tbody>
</table>

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.

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 ............................................................................................................................ 153
- Advanced VRRP ........................................................................................................... 164
- Troubleshooting VRRP ............................................................................................... 168

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:

- **Advanced VRRP** - Every VRRP interface must be explicitly configured to monitor every other VRRP interface
- **Simplified/Monitored Circuit VRRP** - All the VRRP interfaces automatically monitor other VRRP interfaces

⚠️ **Important** - You cannot have a standalone deployment (Security Gateway and Security Management Server on the same computer) in a Gaia VRRP cluster.

Understanding VRRP

Each VRRP cluster, known as a Virtual Router, has a unique identifier, known as the VRID (Virtual Router Identifier). A Virtual Router can have one or more virtual IP addresses (VIP) to which other network nodes connect as a final destination or the next hop in a route.

By assigning a virtual IP address (VIP), you can define alternate paths for nodes configured with static default routes. Only the master is assigned a VIP. The backup is assigned a VIP upon failover when it becomes the master. Nodes can have alternate paths with static default routes in the event of a failure. Static default routes minimize configuration and processing overhead on host computers.

**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.

<table>
<thead>
<tr>
<th>VRRP Term</th>
<th>ClusterXL Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRRP Cluster</td>
<td>Cluster</td>
<td>A group of Security Gateways that provides redundancy.</td>
</tr>
<tr>
<td>VRRP Router</td>
<td>Member</td>
<td>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.</td>
</tr>
<tr>
<td>VRRP Term</td>
<td>ClusterXL Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Master</td>
<td>Primary (active)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>member</td>
<td></td>
</tr>
<tr>
<td>Backup</td>
<td>Backup (standby)</td>
<td>A redundant Security Gateway (Security Gateway) that is available to take over for the master in the event of a failure.</td>
</tr>
<tr>
<td></td>
<td>member</td>
<td></td>
</tr>
<tr>
<td>VRID</td>
<td>Cluster name</td>
<td>Unique Virtual Router identifier The VRID is the also last byte of the MAC address.</td>
</tr>
<tr>
<td>VIP</td>
<td>Cluster IP address</td>
<td>Virtual IP address assigned to a Virtual Router. VIPs are routable from internal and/or external network resources. The VIP is called <em>Backup Address</em> in the WebUI.</td>
</tr>
<tr>
<td>VMAC</td>
<td></td>
<td>Virtual MAC address assigned to a Virtual Router.</td>
</tr>
<tr>
<td>VRRP Transition</td>
<td>Failover</td>
<td>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.</td>
</tr>
</tbody>
</table>

**VRRP Types**

You can configure VRRP using one of these types:

- **Simplified/Monitored Circuit VRRP**
  The simplified Monitored Circuit VRRP configuration contains all of the basic parameters and is applicable for most environments. When using the simple method, you configure each Virtual Router as one unit.

- **Advanced VRRP**
  Use this procedure if you are working with:
  - A system on which VRRP has already been configured using this method
  - An environment where you also want to monitor interfaces that are not running VRRP

You cannot use the Simple and Advanced types together on the same Security Gateway.

**How 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 also 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.

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 Delta value to calculate an Effective Priority value. The Virtual Router with the highest effective priority becomes the new master.

Monitored-circuit VRRP prevents connection issues caused by asymmetric routes when only one interface on a master fails (not the master itself). This problem occurs in environments where a gateway is a member of two or more Virtual Routers, typically one with internal interfaces and the other with external interfaces.

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.

When using the simplified method, Monitored-circuit VRRP monitors all VRRP interfaces on the Security Gateways. When using Advanced VRRP, you configure each interface in a Virtual Router separately. If one interface on a master fails, it releases priority for all VRRP interfaces on that master. This lets the master fail over on all Virtual Routers that include the failed master.

To release the priority, Gaia uses the priority delta value. This is a Check Point proprietary parameter that you define when configuring a Virtual Router. The priority algorithm subtracts the priority delta from the priority value to calculate an effective priority. 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.

See Configuring Monitored-Circuit VRRP using the Simplified Method and Configuring Advanced VRRP (“Advanced VRRP” on page 164) for configuration details.
**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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Master Security Gateway</td>
</tr>
<tr>
<td>2</td>
<td>Backup Security Gateway</td>
</tr>
<tr>
<td>3</td>
<td>Virtual Router VRID 5 - Virtual IP Address (Backup Address) is 192.168.2.5</td>
</tr>
<tr>
<td>4</td>
<td>Internal Network and hosts</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Virtual Router VRID 5. External Virtual IP Address (Backup Address) is 192.168.2.5</td>
</tr>
<tr>
<td>2</td>
<td>Master Security Gateway</td>
</tr>
<tr>
<td>3</td>
<td>Backup Security Gateway</td>
</tr>
<tr>
<td>4</td>
<td>Virtual Router VRID 5. Internal Virtual IP Address (Backup Address) is 192.168.3.5</td>
</tr>
<tr>
<td>5</td>
<td>Internal network and hosts</td>
</tr>
</tbody>
</table>
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. 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

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:


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.


7. Do one of these steps:
   - Run cpconfig on the Security Gateway. Select Enable cluster membership for this gateway to enable FW sync.
     
     **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 multiple 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 VRRP’s monitoring of the FW when you use this configuration. It is enabled by default but not supported with this configuration

8. Enter y when prompted.

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:

1. **Cold Start Delay** - Delay period in seconds before a Security Gateway joins a Virtual Router. Default = 0.

2. **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.

3. **Monitor Firewall State** - Select this option to let VRRP monitor the Security Gateway and automatically take appropriate action. This feature is enabled by default, which is the recommend setting for Security Gateways.

   **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.
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 is 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.

6. Click **Save**.

Configuring Simplified/Monitored Circuit 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 vridds
```
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrid</td>
<td>Enter a unique ID number for this virtual router. The range of valid values is 1 to 255.</td>
</tr>
</tbody>
</table>
| 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 static-mac 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hello-interval</td>
<td>(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).</td>
</tr>
<tr>
<td>password</td>
<td>Enter an authentication password. This parameter is only relevant if the <code>authype</code> value is set to <code>simple</code>.</td>
</tr>
<tr>
<td>priority</td>
<td>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.</td>
</tr>
<tr>
<td>priority delta</td>
<td>Enter the value to subtract from the <code>Priority</code> 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.</td>
</tr>
<tr>
<td>vrids</td>
<td>Shows all Virtual Routers.</td>
</tr>
</tbody>
</table>

## Configuring the VRRP Security Gateway Cluster in SmartDashboard

1. From the **Networks Objects** tree, select **Check Point > Security Cluster > Check Point appliance/ Open Server**.

   The **Security Gateway Cluster Creation** window opens

2. Choose **Wizard Mode**.

3. Define the:
   - **Cluster Name**
   - **Cluster IPv4 Address**
   - For an IPv6 cluster: **Cluster IPv6 Address**

4. Choose the **Cluster’s Solution**: Gaia VRRP.

5. Click **Finish**.
Configuring VRRP Rules for the Security Gateway

1. Define this rule above the Stealth Rule in the Rule Base:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls</td>
<td>mcast-224.0.0.1</td>
<td>Any Traffic</td>
<td>vrp</td>
<td>accept</td>
</tr>
<tr>
<td>fwcluster-object</td>
<td>mcast-224.0.0.1</td>
<td>Any Traffic</td>
<td>igmp</td>
<td></td>
</tr>
</tbody>
</table>

Where:
- **Firewalls** - Simple Group object containing the firewall objects.
- **fwcluster-object** - the VRRP cluster object.
- **mcast-224.0.0.18** - Node Host object with the IP address 224.0.0.18.

2. If your Security Gateways use dynamic routing protocols (such as OSPF or RIP), create new rules for each multicast destination IP address.

Alternatively, you can create a Network object to show all multicast network IP destinations with these values:
- **Name:** MCAST.NET
- **IP:** 224.0.0.0
- **Net mask:** 240.0.0.0

You can use one rule for all multicast protocols you agree to accept, as shown in this example:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster_all_Ps</td>
<td>MCAST.NET</td>
<td>Any Traffic</td>
<td>vrp</td>
<td>accept</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>igmp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ospf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>udp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>rip</td>
<td></td>
</tr>
</tbody>
</table>

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
set vrrp interface VALUE
authtype none
authtype simple
monitored-circuit vrid auto-deactivation
monitored-circuit vrid backup-address on|off
monitored-circuit vrid hello-interval
monitored-circuit vrid monitored-off
monitored-circuit vrid monitored-on
monitored-circuit vrid monitored-priority-delta
monitored-circuit vrid off
monitored-circuit vrid on
monitored-circuit vrid preempt-mode
monitored-circuit vrid priority
monitored-circuit vrid vmac-mode default-vmac
monitored-circuit vrid vmac-mode extended-vmac
monitored-circuit vrid vmac-mode interface-vmac
monitored-circuit vrid vmac-mode static-vmac
virtual-router vrid hello-interval
virtual-router vrid off
virtual-router vrid on
virtual-router vrid vmac-mode default-vmac
virtual-router vrid vmac-mode extended-vmac
virtual-router vrid vmac-mode interface-vmac
virtual-router vrid vmac-mode static-vmac

Show Commands
show vrrp
show vrrp interface
show vrrp interfaces
show vrrp stats
show vrrp summary

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>coldstart-delay</td>
<td>Delay period in seconds before a Security Gateway joins a Virtual Router.</td>
</tr>
<tr>
<td>disable-all-virtual-routers</td>
<td>on or off. Enable or disable all Virtual Routers on this Security Gateway.</td>
</tr>
<tr>
<td>monitor-firewall</td>
<td>Monitor Security Gateway status.</td>
</tr>
<tr>
<td>vrrp interface</td>
<td>The name of the specified Virtual Router interface</td>
</tr>
<tr>
<td>authtype simple</td>
<td>Enter a password to authenticate the Virtual Router.</td>
</tr>
<tr>
<td>monitored-circuit vrid</td>
<td>Enter the VRID.</td>
</tr>
<tr>
<td>auto-deactivation</td>
<td>on or off. On would create an effective priority 0. A virtual router with 0 priority cannot become a master.</td>
</tr>
<tr>
<td>backup-address</td>
<td>The IPv4 address of the backup Security Gateway.</td>
</tr>
<tr>
<td>hello-interval</td>
<td>The number of seconds at which the master sends VRRP advertisements. The range is 1-255 seconds (1 is default).</td>
</tr>
</tbody>
</table>
### Configuring VRRP Clusters in SmartDashboard

This section includes the procedure for configuring a VRRP cluster object in SmartDashboard. Only those procedures that are related to VRRP are shown here.

1. In SmartDashboard, 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](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**.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitored-priority-delta</td>
<td>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</td>
</tr>
<tr>
<td>preempt-mode</td>
<td><strong>on</strong> or <strong>off</strong>. 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.</td>
</tr>
<tr>
<td>priority</td>
<td>The router with the higher priority becomes the new master when a failure occurs. The range is 1-254. The default setting is 100.</td>
</tr>
<tr>
<td>virtual-router vrid</td>
<td>The virtual router ID number</td>
</tr>
</tbody>
</table>
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 ........................................................................................................................................ 171
- License Activation ........................................................................................................................... 180
- Snapshot Image Management ........................................................................................................ 180
- Download SmartConsole .................................................................................................................. 183
- Hardware Health Monitoring ............................................................................................................ 184
- Showing Hardware Information - CLI (show asset) ......................................................................... 185
- Monitoring RAID Synchronization .................................................................................................. 186
- Shutdown .......................................................................................................................................... 186
- System Configuration Backup ........................................................................................................ 187
- Emergendisk ..................................................................................................................................... 192

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 173) or cplic del (on page 174).

  **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.

**Note** - SmartUpdate GUI is the recommended way of managing licenses.

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**  Makes sure 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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-p &lt;product&gt;</code></td>
<td>Product for which license information is requested. For example fw1, netso</td>
</tr>
<tr>
<td><code>-v &lt;version&gt;</code></td>
<td>Product version for which license information is requested</td>
</tr>
<tr>
<td>`-c</td>
<td>-count`</td>
</tr>
</tbody>
</table>
-t <date>

Check license status on future date. Use the format `ddmmyyyy`. A feature may be valid on a given date on one license, but invalid in another.

-r|-routers

Check how many routers are allowed. The `feature` option is not needed.

-S|-SRusers

Check how many SecuRemote users are allowed.

<feature>

<feature> for which license information is requested

**cplic db_add**

**Description**

Used to add one or more licenses to the license repository on the Security Management server. When local license are added to the license repository, they are automatically attached to its intended Check Point gateway, central licenses need to undergo the attachment process.

This command is a license repository command, and can only be executed on the Security Management server.

**Syntax**

```bash
> cplic db_add -l <license-file> [host] [expiration-date] [signature] [SKU/features]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-l</td>
<td>Name of the file that contains the license</td>
</tr>
<tr>
<td>host</td>
<td>Security Management Server hostname or IP address</td>
</tr>
<tr>
<td>expiration-date</td>
<td>The license expiration date</td>
</tr>
<tr>
<td>signature</td>
<td>The License signature string. For example: aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m (The string is case sensitive and the hyphens are optional)</td>
</tr>
<tr>
<td>SKU/features</td>
<td>The SKU of the license summarizes the features included in the license. For example: CPSUITE-EVAL-3DES-vNG</td>
</tr>
</tbody>
</table>

**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` will produce output similar to the following:

```
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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>Print only the licenses attached to Object name. Object name is the name of the Check Point Security Gateway object, as defined in SmartDashboard.</td>
</tr>
<tr>
<td>-all</td>
<td>Print all the licenses in the license repository</td>
</tr>
<tr>
<td>-noheader</td>
<td>Print licenses with no header.</td>
</tr>
<tr>
<td>(or -n)</td>
<td></td>
</tr>
<tr>
<td>-x</td>
<td>Print licenses with their signature</td>
</tr>
<tr>
<td>-t</td>
<td>Print licenses with their type: Central or Local.</td>
</tr>
<tr>
<td>(or -type)</td>
<td></td>
</tr>
<tr>
<td>-a</td>
<td>Show which object the license is attached to. Useful if the -all option is specified.</td>
</tr>
<tr>
<td>(or -attached)</td>
<td></td>
</tr>
</tbody>
</table>

**Comments**

This command is a license repository command, and can only be executed on the Security Management server.

### `cplic db_rm`

**Description**
The `cplic db_rm` command 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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>The signature string within the license.</td>
</tr>
</tbody>
</table>

**Example**

```
cplic db_rm 2f540abb-d3bcb001-7e54513e-kfyigpwn
```

**Comments**

This command is a license repository command, and can only be executed on the Security Management server.

### `cplic del`

**Description**
Delete 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>
```
### cplic del <object name>

**Description**  Detach 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 be executed only on a Security Management server.

**Syntax**

```plaintext
> cplic del <object name> [-F <outputfile>] [-ip <dynamic ip>] <signature>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;object name&gt;</td>
<td>The name of the Check Point Security Gateway object, as defined in SmartDashboard.</td>
</tr>
<tr>
<td>-F &lt;outputfile&gt;</td>
<td>Divert the output to &lt;outputfile&gt; rather than to the screen.</td>
</tr>
<tr>
<td>-ip &lt;dynamic ip&gt;</td>
<td>Delete the license on the Check Point Security Gateway with the specified IP address. This parameter is used for deleting a license on a DAIP Check Point Security Gateway. <strong>Note</strong> - If this parameter is used, then object name must be a DAIP gateway.</td>
</tr>
<tr>
<td>&lt;signature&gt;</td>
<td>The signature string within the license.</td>
</tr>
</tbody>
</table>

**Comments**  This is a Remote Licensing command which affects remote machines that is executed on the Security Management server.

### cplic get

**Description**  The cplic get command retrieves all licenses from a Security Gateway (or from all Security Gateways) into the license repository on the Security Management Server. This command helps you to synchronize the repository with the Check Point Security Gateways. When the command is run, all local changes are updated.

**Syntax**

```plaintext
> cplic get {<ipaddr>|<hostname>|-all} [-v41]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ipaddr&gt;</td>
<td>The IP address of the Check Point Security Gateway from which licenses are to be retrieved.</td>
</tr>
<tr>
<td>&lt;hostname&gt;</td>
<td>The name of the Check Point Security Gateway object (as defined in SmartDashboard) from which licenses are to be retrieved.</td>
</tr>
</tbody>
</table>
### cplic get

**Description** Retrieve licenses from all Check Point gateways in the managed network.

- **-all**
  - Retrieve licenses from all Check Point gateways in the managed network.

- **-v41**
  - Retrieve 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.

**Comments** This is a Remote Licensing Command which affects remote machines that is executed on the Security Management Server.

### cplic put

**Description** Install 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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-o</td>
<td>-overwrite</td>
</tr>
<tr>
<td>-c</td>
<td>-check-only</td>
</tr>
<tr>
<td>-s</td>
<td>-select</td>
</tr>
<tr>
<td>-F &lt;outputfile&gt;</td>
<td>Outputs the result of the command to the designated file rather than to the screen.</td>
</tr>
<tr>
<td>-P</td>
<td>-Pre-boot</td>
</tr>
<tr>
<td>-k</td>
<td>-kernel-only</td>
</tr>
<tr>
<td>-l &lt;license-file&gt;</td>
<td>Name of the file that contains the license</td>
</tr>
<tr>
<td>&lt;host&gt;</td>
<td>Security Management Server hostname or IP address</td>
</tr>
<tr>
<td>&lt;expiration-date&gt;</td>
<td>The license expiration date</td>
</tr>
</tbody>
</table>
### Table: License Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;signature&gt;</td>
<td>The License signature string. For example: <code>aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m</code> (The string is case sensitive and the hyphens are optional)</td>
</tr>
<tr>
<td>&lt;SKU/features&gt;</td>
<td>The SKU of the license summarizes the features included in the license. For example: <code>CPMP-EVAL-1-3DES-NG CK0123456789ab</code></td>
</tr>
</tbody>
</table>

### Comments

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); last part cannot be 0 or 255.
  - **Solaris2** - The response to the `hostid` command (beginning with 0x).

- **expiration date** - The license expiration date. 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:
```

<table>
<thead>
<tr>
<th>Host</th>
<th>Expiration</th>
<th>SKU</th>
</tr>
</thead>
<tbody>
<tr>
<td>215.153.142.130</td>
<td>26Dec2001</td>
<td>CPMP-EVAL-1-3DES-NG CK0123456789ab</td>
</tr>
</tbody>
</table>

### `cplic put <object name> ...`

**Description**  
Use the `cplic put` command to attach one or more central or local license 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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>object name</td>
<td>The name of the Check Point Security Gateway object, as defined in SmartDashboard.</td>
</tr>
<tr>
<td>-ip dynamic ip</td>
<td>Install 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.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: If this parameter is used, then object name must be a DAIP Check Point gateway.</td>
</tr>
<tr>
<td>-F &lt;outputfile&gt;</td>
<td>Divert the output to <code>&lt;outputfile&gt;</code> rather than to the screen.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>-l &lt;license-file&gt;</td>
<td>Installs the license(s) from &lt;license-file&gt;.</td>
</tr>
<tr>
<td>-l &lt;license-file&gt;</td>
<td>Name of the file that contains the license</td>
</tr>
<tr>
<td>&lt;host&gt;</td>
<td>Security Management Server hostname or IP address</td>
</tr>
<tr>
<td>&lt;expiration-date&gt;</td>
<td>The license expiration date</td>
</tr>
<tr>
<td>&lt;signature&gt;</td>
<td>The License signature string. For example:</td>
</tr>
<tr>
<td></td>
<td>aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m (The string is case sensitive and the hyphens are optional)</td>
</tr>
<tr>
<td>&lt;SKU/features&gt;</td>
<td>The SKU of the license summarizes the features included in the license. For example: CPSUITE-EVAL-3DES-vNG</td>
</tr>
</tbody>
</table>

**Comments**  This is a *Remote Licensing Command* which affects remote machines that 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. 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

**cplc print**

**Description**  The `cplc print` command (located in $CPDIR/bin) prints details of Check Point licenses on the local machine.

**Syntax**

```
> cplc print [-n|--noheader] [-x prints signatures] [-t type] [-F <outputfile>] [-p preatures]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-n</td>
<td>--noheader</td>
</tr>
<tr>
<td>-x</td>
<td>Print licenses with their signature</td>
</tr>
<tr>
<td>-t</td>
<td>--type</td>
</tr>
</tbody>
</table>
**Parameter** | **Description**
--- | ---
-F <outputfile> | Divert the output to `outputfile`.
-p|-preatures | Print licenses resolved to primitive features.

**Comments** On a Check Point gateway, this command will print all licenses that are installed on the local machine — both Local and Central licenses.

---

**cplic upgrade**

**Description** Use the `cplic upgrade` command to upgrade licenses in the license repository using licenses in a license file obtained from the User Center.

**Syntax**

```plaintext
> 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** The following example explains the procedure which needs to take place in order to upgrade the licenses in the license repository.

- 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 version products.
- 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:

  ```plaintext
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`

  ```plaintext
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 CFW-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 and 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 using 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.

• In the example, there are two Software Blades licenses in the file. One does not match any license on a remote Security Gateway, the other matches a version NGX license on a Security Gateway that should be upgraded:

**Comments** This is a Remote Licensing Command which affects remote Security Gateways, that is executed on the Security Management Server.

**Further Info.** For more about managing licenses, see the R77 Installation and Upgrade Guide http://supportcontent.checkpoint.com/documentation_download?ID=24831.

License Activation

On a Check Point 2012 Appliance, you can get a license automatically from the User Center and activate it.

**To Activate a License on a Check Point 2012 Appliance:**

1. Open the Maintenance > License Activation page.
2. If there is a proxy server between the appliance and the Internet:
   a) Click Use a Proxy Server.
   b) Enter the proxy server IP Address and Port.
3. On a Security Gateway-only appliance: Enter the Security Management Server IP address and follow the instructions.
4. Click Activate License.

Snapshot Image Management

A snapshot is a backup of the system settings and products:

• 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)
You can import a snapshot that was made on a different release or on this release. You must import it to the same appliance or open server hardware model.

**IMPORTANT:** 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].

**Note** - During the snapshot creation, all the system processes and services continue to run, and the security policy enforcement does not get interrupted.

### Configuring Snapshot Management - WebUI

Before you create a snapshot image, make sure the storage computer or appliance fulfills the prerequisites.

**To create a snapshot:**

1. In the tree view, click Maintenance > Image Management.
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 > Image 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 > Image 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 > Image 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.

---

**Configuring Snapshot Management - CLI (snapshot)**

**Description**
Manage system images (also known as 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snapshot VALUE</td>
<td>Name of the image</td>
</tr>
<tr>
<td>desc VALUE</td>
<td>Description of the image</td>
</tr>
<tr>
<td>snapshot export</td>
<td>The name of the image to export</td>
</tr>
<tr>
<td>snapshot import</td>
<td>The name of the image to import</td>
</tr>
<tr>
<td>path VALUE</td>
<td>The storage location for the exported image. For example: /var/log</td>
</tr>
<tr>
<td>name VALUE</td>
<td>The name of the exported image (not the original image).</td>
</tr>
<tr>
<td>all</td>
<td>All image details</td>
</tr>
</tbody>
</table>

Comments

- To create the snapshot image requires free space on the Backup partition. The required free disk space is the actual size of the root partition, multiplied by 1.15.

- The available 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.

- 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
```
### 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 <category name>
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Show all available hardware information. The information shown depends on the type of hardware.</td>
</tr>
<tr>
<td>&lt;category name&gt;</td>
<td>Show available information for a specific category</td>
</tr>
</tbody>
</table>

**Example 1**

clish> show asset TAB

**Output 1**

```
system all
```

**Example 2**

clish> show asset all

---

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ps</td>
<td>Power Supply [for supported hardware only]</td>
</tr>
</tbody>
</table>

**Example**

```
show sysenv all
```

**Output**

```
gw-3002f0> show sysenv all

Hardware Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>unit</th>
<th>type</th>
<th>status</th>
<th>Maximum</th>
<th>Minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>+12V</td>
<td>29.44</td>
<td>Volt</td>
<td>Voltage</td>
<td>0</td>
<td>12.6</td>
<td>11.4</td>
</tr>
<tr>
<td>+5V</td>
<td>6.02</td>
<td>Volt</td>
<td>Voltage</td>
<td>0</td>
<td>5.3</td>
<td>4.75</td>
</tr>
<tr>
<td>VBat</td>
<td>3.23</td>
<td>Volt</td>
<td>Voltage</td>
<td>0</td>
<td>3.47</td>
<td>2.7</td>
</tr>
</tbody>
</table>
```
Monitoring RAID Synchronization

In R77, 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.
  ```
  raid_diagnostic
  Raid Status:
  RAID: 1 Number Of Disks: 2 RaidSize: 465GB State: DEGRADED Flags: ENABLED REDSYNC_IN_PROGRESS
  DiskID: 0 DiskNumber: 0 Vendor: AHA ProductID: R40M Model: 465GB State: ONLINE Flags: NONE
  ```
- `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

**Note** - This feature is available in a R75.40 Gaia Feature Release (Gaia+) clean installation. It is not available when upgrading to R75.40 Gaia.

- 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.

  **Note** - You can only do a migration using the same Gaia version on the source and target computers.

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.

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)

Backing Up a Configuration

**Description**
Use these commands to create and save the system’s configuration.

**Syntax**

To create and save a backup locally:
```
add backup local
```

To create and save a backup on a remote server using FTP:
```
add backup ftp ip VALUE username VALUE password plain
```

To create and save a backup on a remote server using TFTP:
```
add backup tftp ip VALUE
```

To save a backup on a remote server using SCP:
```
add backup scp ip VALUE username VALUE password plain
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip VALUE</td>
<td>The IP address of the remote server.</td>
</tr>
<tr>
<td>username VALUE</td>
<td>User name required to log in to the remote server.</td>
</tr>
<tr>
<td>password plain</td>
<td>At the prompt, enter the password for the remote server.</td>
</tr>
</tbody>
</table>

**Example**
```
add backup local
```

**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
```

**Comments**
Backup configurations are stored in: `/var/CPbackup/backups/`
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local &lt;TAB&gt;</td>
<td>The &lt;TAB&gt; does an auto-complete on the name and location of the backup file.</td>
</tr>
<tr>
<td>ip VALUE</td>
<td>The IP address of the remote server.</td>
</tr>
<tr>
<td>file VALUE</td>
<td>The location and name of the file on the remote server.</td>
</tr>
<tr>
<td>username VALUE</td>
<td>User name required to log in to the remote server.</td>
</tr>
<tr>
<td>password plain</td>
<td>At the prompt, enter the password for the remote server.</td>
</tr>
</tbody>
</table>

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 191) feature.

Monitoring Backup Status

To monitor the creation of a backup:
show backup status

To show the status of the last backup performed:
show backups

Configuring Scheduled Backups - WebUI

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)

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name VALUE</td>
<td>The name of the scheduled backup</td>
</tr>
<tr>
<td>ip VALUE</td>
<td>The IP address of the FTP, TFTP, or SCP remote server</td>
</tr>
<tr>
<td>username VALUE</td>
<td>User name required to log in to the remote server</td>
</tr>
<tr>
<td>backup-scheduled VALUE</td>
<td>The name of a scheduled backup</td>
</tr>
<tr>
<td>password plain</td>
<td>At the prompt, enter the password for the remote server</td>
</tr>
<tr>
<td>recurrence daily time</td>
<td>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.</td>
</tr>
<tr>
<td>recurrence monthly month</td>
<td>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</td>
</tr>
<tr>
<td>recurrence weekly days</td>
<td>To specify a job for once a week, enter recurrence weekly, and the day by number, when 0 is Sunday and 6 is Saturday.</td>
</tr>
<tr>
<td>time</td>
<td>To specify the time, enter the time in the twenty four hour clock format. For example: 14:00.</td>
</tr>
</tbody>
</table>
| 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. An Emergendisk bootable USB device can be used 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:

<table>
<thead>
<tr>
<th>Boot EmergenDisk with console</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset Admin Password</td>
</tr>
<tr>
<td>Boot EmergenDisk with vga</td>
</tr>
<tr>
<td>Darik's Boot and Nuke (DBAN)</td>
</tr>
<tr>
<td>Boot from local drive</td>
</tr>
</tbody>
</table>

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. Choose 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. Choose 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. Choose 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. Choose the option:
   Darik’s Boot and Nuke (DBAN)
5. The DBAN menu shows the different ways of erasing the disk.
Press [Tab] to edit options

- autonuke
- dban
- dod
- dod3pass
- dodshort
- gutmann
- ops2
- paranoid
- prng
- quick
- zero
- nofloppy

6. Choose the required option.
CPUSE

In This Section:

- Configuring CPUSE - WebUI ................................................................. 196
- Configuring a CPUSE Policy - WebUI .................................................... 198
- Configuring CPUSE Mail Notifications - WebUI .................................... 199
- Downloading and Installing with CPUSE - clish ................................... 199
- Reviewing CPUSE – clish ........................................................................ 201
- Configuring a CPUSE Policy - clish ........................................................ 204
- Configuring CPUSE Mail Notifications - clish ....................................... 205
- CLI Procedures - CPUSE ........................................................................... 205

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 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 package:

1. In the **Upgrades (CPUSE) > Status and Actions** page, click **More** and 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:

1. In the **Upgrades (CPUSE) > Status and Actions** page, click **Showing Recommended Packages** and select an option:
   - **Recommended** (default)
   - **Installed**
   - **All**

**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**.

### Downloading and Installing with CPUSE - clish

**Description**

Run these CPUSE procedures:

- Update, start, or stop the Deployment Agent (the daemon that handles all CPUSE processes)
- Check for available updates, verify compatibility of the installation package with the computer, download, install, delete, or import full installation packages and hotfixes
Syntax


Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| agent {start | stop | update [not-interactive]} | Run these operations on the installer agent:  
  • start - Start the Deployment Agent daemon  
  The Deployment Agent starts automatically on system start-up, as part of the cpstart process.  
  • stop - Stop the Deployment Agent daemon  
  • update [not-interactive] - Update the Deployment Agent  
  This command runs in interactive mode by default. To run it in non-interactive mode, run with the not-interactive option. |
| check-for-updates [not-interactive] | Check for new available packages in Check Point cloud. This command runs in interactive mode by default. To run it in non-interactive mode, run with the not-interactive option. |
| delete {<num> | <package>} [not-interactive] | Delete a package. Provide the package filename - <package>, or number <num>. To see all downloaded packages, type installer delete and press the TAB key. This command runs in interactive mode by default. To run it in non-interactive mode, run with the not-interactive option. |
| download {<num> | <package>} [pause | resume | not-interactive] | Download a package. Provide the package filename - <package>, or number <num>. To see all available for download packages, type installer download and press the TAB key. This command runs in interactive mode by default. To run it in non-interactive mode, run with the not-interactive option.  
  To pause a package download, run with the pause option. To resume a package download operation, that has been paused, run with the resume option. |
| download-and-install {<num> | <package>} [not-interactive] | Download and install a package. Provide the package filename - <package>, or number <num>. To see all available for download and installation packages, type installer download-and-install and press the TAB key. This command runs in interactive mode by default. To run it in non-interactive mode, run with the not-interactive option. |
import {cloud<package> | ftp<ip_addr> path<username><password>] | local<path>
[not-interactive] Import the package from one of these:
- cloud - specify the package name, as provided by the Check Point support
- ftp - specify the IP address of the ftp server, the full path of the package, the username, and the password (optional)
- local - specify the full path of the package on the local computer
This command runs in interactive mode by default. To run it in non-interactive mode, run with the not-interactive option.

install {<num> | <package>} [not-interactive] Install a package. Provide the package filename - <package>, or number <num>. To see all available for installation packages, type installer install and press the TAB key. This command runs in interactive mode by default. To run it in non-interactive mode, run with the not-interactive option.

uninstall {<num> | <package>} [not-interactive] Uninstall a package. Provide the package filename - <package>, or number <num>. To see the installed packages, type installer uninstall and press the TAB key. This command runs in interactive mode by default. To run it in non-interactive mode, run with the not-interactive option.

upgrade {<num> | <package>} [not-interactive] Upgrade to a newer version. Provide the package filename - <package>, or number <num>. To see the available upgrade packages, type installer upgrade and press the TAB key. This command runs in interactive mode by default. To run it in non-interactive mode, run with the not-interactive option.

verify {<num> | <package>} [not-interactive] Verify a package before the installation. Provide the package filename - <package>, or number <num>. To see all available for installation packages, type installer verify and press the TAB key. This command runs in interactive mode by default. To run it in non-interactive mode, run with the not-interactive option.

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail-notifications {&lt;num&gt;</td>
<td>Show these email notifications configured for the user number &lt;num&gt; or for</td>
</tr>
<tr>
<td></td>
<td>&lt;email&gt;}</td>
</tr>
<tr>
<td></td>
<td>• For changes in download status</td>
</tr>
<tr>
<td></td>
<td>• For changes in installation status</td>
</tr>
<tr>
<td></td>
<td>• For new available packages</td>
</tr>
<tr>
<td>package &lt;num&gt;</td>
<td>Show this information about the package number &lt;num&gt;, as shown in the list</td>
</tr>
<tr>
<td></td>
<td>of packages:</td>
</tr>
<tr>
<td></td>
<td>• Display name</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Size</td>
</tr>
<tr>
<td></td>
<td>• Type - Version, Wrapper, or Hotfix</td>
</tr>
<tr>
<td></td>
<td>• Status - Download or installation status and reason for failure if</td>
</tr>
<tr>
<td></td>
<td>applicable</td>
</tr>
<tr>
<td></td>
<td>• Requires reboot - Yes or No</td>
</tr>
<tr>
<td></td>
<td>• Recommended - Is the package recommended by Check Point?</td>
</tr>
<tr>
<td></td>
<td>• Contains - List of components (files, archives) inside the package</td>
</tr>
<tr>
<td></td>
<td>• Contained-in - Name of archive containing the package</td>
</tr>
<tr>
<td></td>
<td>• Downloaded on - The date of the download</td>
</tr>
<tr>
<td></td>
<td>• Imported on - The date of the import</td>
</tr>
<tr>
<td></td>
<td>• Installed on - The date of the installation</td>
</tr>
<tr>
<td></td>
<td>• Installation log - The name of the installation log</td>
</tr>
</tbody>
</table>

Note - To see the numbered list of packages, type `show installer package` and hit `Tab`. Make sure to enter a `space` after the word `package`. 
### packages

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

### policy

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

### status

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
Configuring a CPUSE Policy - clish

Description
Configure the CPUSE policy for downloads and installation.

Syntax
```clish
set installer policy {downloads {automatic | manual | scheduled {daily <time> | monthly <day> at <time> | once <date> at <time> | weekly <day_of_the_week> at <time>}}} | periodically-self-update {on | off} | self-test {auto-rollback | install-policy | network-link-up | start-processes} {on | off} | send-cpuse-data {on | off}}
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>downloads</td>
<td>Configure the way to download the Hotfixes:</td>
</tr>
<tr>
<td>automatic</td>
<td>to download packages when they become available</td>
</tr>
<tr>
<td>manual</td>
<td>CPUSE checks for updates every three hours while the computer is up, immediately after the computer boots up, and at the time of access of the Upgrades (CPUSE) page in WebUI.</td>
</tr>
<tr>
<td>scheduled</td>
<td>at a certain time daily, weekly [specify day of the week], monthly [specify day of the month], or once on a specified date</td>
</tr>
<tr>
<td>daily &lt;time&gt;</td>
<td>Note: Full installation packages can only be downloaded manually.</td>
</tr>
<tr>
<td>monthly &lt;day&gt; at &lt;time&gt;</td>
<td></td>
</tr>
<tr>
<td>once &lt;date&gt; at &lt;time&gt;</td>
<td></td>
</tr>
<tr>
<td>weekly &lt;day_of_the_week&gt; at &lt;time&gt;</td>
<td></td>
</tr>
<tr>
<td>periodically-self-update</td>
<td>Turn on to keep the Deployment Agent up to date.</td>
</tr>
<tr>
<td>on</td>
<td></td>
</tr>
<tr>
<td>off</td>
<td></td>
</tr>
<tr>
<td>self-test</td>
<td>Turn on to run sanity checks after upgrading with CPUSE:</td>
</tr>
<tr>
<td>auto-rollback</td>
<td>auto-rollback: 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.</td>
</tr>
<tr>
<td>install-policy</td>
<td>Note: If this option is not selected, only the notification is sent.</td>
</tr>
<tr>
<td>network-link-up</td>
<td>install-policy: to make sure that it is possible to install the policy</td>
</tr>
<tr>
<td>start-processes</td>
<td>network-link-up: to make sure that all the network interfaces on the Gaia computer are up</td>
</tr>
<tr>
<td>on</td>
<td>start-processes: to make sure that Check Point processes are running</td>
</tr>
<tr>
<td>off</td>
<td></td>
</tr>
<tr>
<td>send-cpuse-data</td>
<td>Turn on, to help Check Point collect download and installation data that is used only to improve the CPUSE service.</td>
</tr>
<tr>
<td>on</td>
<td></td>
</tr>
<tr>
<td>off</td>
<td></td>
</tr>
</tbody>
</table>
Configuring CPUSE Mail Notifications - clish

Description
Configure the CPUSE mail notifications.

Syntax
set installer mail-notifications {<num> | <email>}
{download-status | install-status | new-available-packages} {on | off}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail-notifications {&lt;num&gt;</td>
<td>&lt;email&gt;}</td>
</tr>
<tr>
<td>download-status</td>
<td>for changes in download status</td>
</tr>
<tr>
<td>install-status</td>
<td>for changes in installation status</td>
</tr>
<tr>
<td>new-available-packages</td>
<td>for new available packages</td>
</tr>
</tbody>
</table>

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.
Security Management Server and Firewall Commands

In This Section:

- cpca_client .................................................................................................................. 209
- cp_conf ........................................................................................................................ 211
- cpconfig ....................................................................................................................... 215
- cpinfo ........................................................................................................................... 215
- cpstart ......................................................................................................................... 216
- cpstat ........................................................................................................................... 216
- cpstop .......................................................................................................................... 218
- fw ................................................................................................................................. 219
- fwm .............................................................................................................................. 246

**cpca_client**

**Description**  These commands execute operations on the ICA (Internal Certificate Authority).

**Syntax**

```
> cpca_client
```

**cpca_client create_cert**

**Description**  Prompt the ICA to issue a SIC certificate for the Security Management server.

**Syntax**

```
> cpca_client [-d] create_cert [-p <ca_port>] -n "CN=<common name>" -f <PKCS12>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Runs the command in debug mode</td>
</tr>
<tr>
<td>-p &lt;ca_port&gt;</td>
<td>Specifies the port used to connect to the CA (if the CA was not run from the default port 18209)</td>
</tr>
<tr>
<td>-n &quot;CN=&lt;common name&gt;&quot;</td>
<td>Sets the CN to &lt;common name&gt;</td>
</tr>
<tr>
<td>-f &lt;PKCS12&gt;</td>
<td>Specifies the file name, &lt;PKCS12&gt;, that stores the certificate and keys.</td>
</tr>
</tbody>
</table>
# cpca_client revoke_cert

**Description**  
Revoke a certificate issued by the ICA.

**Syntax**

```
> cpca_client [-d] revoke_cert [-p <ca_port>] -n "CN=<common name>"
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Runs the command in debug mode</td>
</tr>
<tr>
<td>-p &lt;ca_port&gt;</td>
<td>Specifies the port which is used to connect to the CA (if the CA was not run from the default port 18209)</td>
</tr>
<tr>
<td>-n &quot;CN=&lt;common name&gt;&quot;</td>
<td>Sets the CN to &lt;common name&gt;</td>
</tr>
</tbody>
</table>

# cpca_client lscert

**Description**  
Show all certificates issued by the ICA.

**Syntax**

```
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Runs the command in debug mode</td>
</tr>
<tr>
<td>-dn substring</td>
<td>Filters results to those with a DN that matches this &lt;substring&gt;</td>
</tr>
<tr>
<td>-stat</td>
<td>Filters results to the specified certificate status: Pending, Valid, Revoke, Expire, or Renewed</td>
</tr>
<tr>
<td>-kind</td>
<td>Filters results for specified kind: SIC, IKE, User, or LDAP</td>
</tr>
<tr>
<td>-ser &lt;serial&gt;</td>
<td>Filters results for this serial number</td>
</tr>
<tr>
<td>-dp &lt;dp&gt;</td>
<td>Filters results from this CDP (certificate distribution point)</td>
</tr>
</tbody>
</table>

# cpca_client set_mgmt_tool

**Description**  
Starts or stops the ICA Management Tool.

**Syntax**

```
> cpca_client [-d] set_mgmt_tool {on|off|add|remove|clean|print} [-p <ca_port>] [-no_ssl] {-a <administrator DN>, -u <user DN>, -c <custom user DN>, ...}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Runs the command in debug mode.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>set_mgmt_tool {on</td>
<td>off</td>
</tr>
<tr>
<td>-p &lt;ca_port&gt;</td>
<td>Specifies the port which is used to connect to the CA. The default port is 18265.</td>
</tr>
<tr>
<td>-no_ssl</td>
<td>Configures the server to use HTTP instead of HTTPS.</td>
</tr>
<tr>
<td>-a &lt;administrator DN&gt;</td>
<td>Sets the DNs of the administrators that are permitted to use the ICA Management Tool.</td>
</tr>
<tr>
<td>-u &lt;user DN&gt;</td>
<td>Sets the DNs of the users that are permitted to use the ICA Management Tool.</td>
</tr>
<tr>
<td>-c &lt;custom user DN&gt;</td>
<td>Sets the DN for custom users that can use the ICA Management Tool.</td>
</tr>
</tbody>
</table>

**Comments**

1. If the command is run without -a or -u the list of the permitted users and administrators isn’t changed. The server can be stopped or started with the previously defined permitted users and administrators.

2. If two consecutive start operations are initiated, the ICA Management Tool will not respond, unless you change the SSL mode. After the SSL mode has been modified, the server can be stopped and restarted.

**cp_conf**

**Description** Configure/reconfigure a Security Gateway installation. The configuration available options for any machine depend on the installed configuration and products.

**Syntax**

>` cp_conf`

**cp_conf sic**

**Description** Use the cp_conf sic commands to manage SIC on the Security Management Server.

**Syntax**

>` cp_conf sic state`
>` cp_conf sic init <key> [norestart]`
>` cp_conf sic cert_pull <management> <object>`
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>state</td>
<td>Shows the SIC trust state.</td>
</tr>
<tr>
<td>init &lt;key&gt;</td>
<td>Restarts SIC with the Activation Key &lt;key&gt;.</td>
</tr>
<tr>
<td>[no restart]</td>
<td>By default, the Security Gateway runs <code>cpstop</code> and <code>cpstart</code> when you restart SIC. Use the <code>norestart</code> parameter to restart SIC and to not run <code>cpstop</code> and <code>cpstart</code>.</td>
</tr>
<tr>
<td>cert_pull</td>
<td>For DAIP Security Gateways, pulls a certificate from the Security Management Server for the &lt;object&gt;</td>
</tr>
<tr>
<td>&lt;management&gt;</td>
<td>Name or IP address of the Security Management Server</td>
</tr>
</tbody>
</table>

### cp_conf admin

**Description**  Manage Check Point system administrators for the Security Management Server

**Syntax**

```plaintext
> cp_conf admin get # Get the list of administrators.
> cp_conf admin add <user> <pass> {a|w|r}
> cp_conf admin del <admin1> <admin2>...
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>Shows a list of the administrators</td>
</tr>
<tr>
<td>add &lt;user&gt; &lt;pass&gt;</td>
<td>Adds a new administrator &lt;user&gt; with password &lt;pass&gt;</td>
</tr>
<tr>
<td>{a</td>
<td>w</td>
</tr>
<tr>
<td></td>
<td>a - Read, write and manage administrators</td>
</tr>
<tr>
<td></td>
<td>w - Read and write</td>
</tr>
<tr>
<td></td>
<td>r - Read only</td>
</tr>
<tr>
<td>del &lt;admin1&gt;</td>
<td>Deletes one or more administrators &lt;admin1&gt;, &lt;admin2&gt;, and so on</td>
</tr>
</tbody>
</table>

### cp_conf ca

**Description**  Initialize the Certificate Authority

**Syntax**

```plaintext
> cp_conf ca init
> cp_conf ca fqdn <name>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>init</td>
<td>Initializes the internal CA</td>
</tr>
<tr>
<td>fqdn &lt;name&gt;</td>
<td>Sets the FQDN of the internal CA to &lt;name&gt;</td>
</tr>
</tbody>
</table>
**cp_conf finger**

**Description**  Displays the fingerprint which will be used on first-time launch to verify the identity of the Security Management server being accessed by the SmartConsole. This fingerprint is a text string derived from the Security Management server’s certificate.

**Syntax**

```
> cp_conf finger get
```

**cp_conf lic**

**Description**  Shows the installed licenses and lets you manually add new ones.

**Syntax**

```
> cp_conf lic get
> cp_conf lic add -f <file>
> cp_conf lic add -m <Host> <Date> <Key> <SKU>
> cp_conf lic del <Signature Key>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>Shows the installed licenses</td>
</tr>
<tr>
<td>add -f &lt;file&gt;</td>
<td>Adds the license from &lt;file&gt;</td>
</tr>
<tr>
<td>add -m</td>
<td>Manually adds a license with these parameters:</td>
</tr>
<tr>
<td></td>
<td>&lt;host&gt; - name of the Security Management Server</td>
</tr>
<tr>
<td></td>
<td>&lt;Date&gt; - Date of the license</td>
</tr>
<tr>
<td></td>
<td>&lt;Key&gt; - License key</td>
</tr>
<tr>
<td></td>
<td>&lt;SKU&gt; - License SKU</td>
</tr>
<tr>
<td>del &lt;Key&gt;</td>
<td>Deletes license &lt;key&gt;</td>
</tr>
</tbody>
</table>

**cp_conf client**

**Description**  Manage the GUI clients that can use SmartConsoles to connect to the Security Management Server.

**Syntax**

```
> cp_conf client get # Get the GUI clients list
> cp_conf client add <GUI client> # Add one GUI Client
> cp_conf client del < GUI client 1> < GUI client 2>... # Delete GUI Clients
> cp_conf client createlist < GUI client 1> < GUI client 2>... # Create new list.
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>Shows the IP addresses of the allowed GUI clients.</td>
</tr>
<tr>
<td>add &lt;GUI client&gt;</td>
<td>Adds the &lt;GUI client&gt; IP address to the list of allowed GUI clients.</td>
</tr>
</tbody>
</table>
### cp_conf ha

**Description**  
Enable or disable High Availability.

**Syntax**  
> cp_conf ha {enable|disable} [norestart]

### cp_conf snmp

**Description**  
Activate or deactivate SNMP.

**Syntax**  
> cp_conf snmp get  
> cp_conf snmp {activate|deactivate} [norestart]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>Shows the SNMP status.</td>
</tr>
<tr>
<td>{activate</td>
<td>deactivate</td>
</tr>
<tr>
<td>[no restart]</td>
<td>By default, the Security Gateway runs cpstop and cpstart when you enable or disable SNMP. Use the norestart parameter to configure SNMP and to not run cpstop and cpstart.</td>
</tr>
</tbody>
</table>

### cp_conf auto

**Description**  
Configure the Security Gateway and Security Management Server products that start automatically when the appliance or server reboots.

**Syntax**  
> cp_conf auto get [fw1] [fg1] [rm] [all]  
> cp_conf auto {enable|disable} <product1> <product2>...

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>Shows which products start automatically</td>
</tr>
<tr>
<td>{enable</td>
<td>disable} &lt;product1&gt; &lt;product2&gt;</td>
</tr>
</tbody>
</table>
**cp_conf sxl**

**Description**  
Enable or disable SecureXL acceleration.

**Syntax**

```
> cp_conf sxl {enable|disable}
```
Syntax

```
> cpinfo [-v] [-l] [-n] [-o ] [-r | -t [tablename]] [-c <domain> ... | -x <vs>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-v</td>
<td>Prints version information</td>
</tr>
<tr>
<td>-l</td>
<td>Embeds log records (very large output)</td>
</tr>
<tr>
<td>-n</td>
<td>Does not resolve network addresses (faster)</td>
</tr>
<tr>
<td>-o</td>
<td>Output to a file and to the screen</td>
</tr>
<tr>
<td>-r</td>
<td>Includes the registry (for Windows servers - shows a large output)</td>
</tr>
<tr>
<td>-z</td>
<td>Output gzipped (effective with -o option)</td>
</tr>
<tr>
<td>-c &lt;domain&gt;</td>
<td>Get information about the specified &lt;domain&gt; Domain Management Server (Multi-Domain Security Management)</td>
</tr>
<tr>
<td>-x &lt;vs&gt;</td>
<td>Get information about the specified &lt;vs&gt; Virtual System (VSX)</td>
</tr>
</tbody>
</table>

Further Info: SecureKnowledge solution sk30567

**cpstart**

**Description**
Start all Check Point processes and applications running on an appliance or server.

**Syntax**
```
> cpstart
```

**Comments**
This command cannot be used to start cprid. cprid is invoked when the machine is booted and it runs independently.

**cpstat**

**Description**
`cpstat` displays the status of Check Point applications, either on the local or on another appliance or server, in various formats.

**Syntax**
```
> cpstat [-h <host>][-p <port>][-s <SICname>][-f <flavor>][-o <polling>][-c <count>][-e <period>][-d] <application_flag>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h &lt;host&gt;</td>
<td>A resolvable hostname, a dot-notation address (for example: 192.0.2.23), or a DAIP object name. The default is localhost.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>-p &lt;port&gt;</td>
<td>Port number of the AMON server. The default is the standard AMON port (18192).</td>
</tr>
<tr>
<td>-s &lt;SICname&gt;</td>
<td>Secure Internal Communication (SIC) name of the AMON server.</td>
</tr>
<tr>
<td>-f &lt;flavor&gt;</td>
<td>The flavor of the output (as it appears in the configuration file). The default is the first flavor found in the configuration file.</td>
</tr>
<tr>
<td>-o &lt;polling&gt;</td>
<td>Polling interval (seconds) specifies the pace of the results. The default is 0, meaning the results are shown only once.</td>
</tr>
<tr>
<td>-c &lt;count&gt;</td>
<td>Specifies how many times the results are shown. The default is 0, meaning the results are repeatedly shown.</td>
</tr>
<tr>
<td>-e &lt;period&gt;</td>
<td>Specifies the interval (seconds) over which 'statistical' olds are computed. Ignored for regular olds.</td>
</tr>
<tr>
<td>-d</td>
<td>Debug mode.</td>
</tr>
</tbody>
</table>
| <application_flag> | One of the following:  
- fw — Firewall component of the Security Gateway  
- vpn — VPN component of the Security Gateway  
- fg — QoS (formerly FloodGate-1)  
- ha — ClusterXL (High Availability)  
- os — OS Status  
- mg — for the Security Management server  
- persistency - for historical status values  
- polysrv  
- uas  
- svr  
- cpsemd  
- cpsead  
- asm  
- ls  
- ca |

The following parameters can be added to the application flags:  
\begin{itemize}
  \item \texttt{vpn} — "default", "product", "IKE", "ipsec", "traffic", "compression",
    "accelerator",
    "nic", "statistics", "watermarks", "all"
  \item \texttt{fg} — "all"
  \item \texttt{ha} — "default", "all"
  \item \texttt{os} — "default", "ifconfig", "routing", "memory", "old_memory", "cpu",
    "disk", "perf",
    "multi_cpu", "multi_disk", "all", "average_cpu", "average_memory",
    "statistics"
  \item \texttt{mg} — "default"
  \item \texttt{persistency} — "product", "Tableconfig", "SourceConfig"
  \item \texttt{polsrv} — "default", "all"
  \item \texttt{uas} — "default"
  \item \texttt{svr} — "default"
  \item \texttt{cpsemd} — "default"
  \item \texttt{cpsead} — "default"
  \item \texttt{asm} — "default", "WS"
  \item \texttt{ls} — "default"
  \item \texttt{ca} — "default", "crl", "cert", "user", "all"
\end{itemize}

\textbf{Example}

\begin{verbatim}
> cpstat fw
Policy name: Standard
Install time: Wed Nov  1 15:25:03 2000

Interface table
-----------------------------------------------------------------
|Name|Dir|Total *|Accept**|Deny|Log|
-----------------------------------------------------------------
|hme0|in |739041*|738990**|51 *|7**|
-----------------------------------------------------------------
|hme0|out|463525*|463525**| 0 *|0**|
-----------------------------------------------------------------
**********|1202566|1202515*|51**|7**|
\end{verbatim}

\textbf{cpstop}

\textbf{Description} \hspace{1em} Terminate all Check Point processes and applications, running on an appliance or server.

\textbf{Syntax}

\begin{verbatim}
> cpstop
> cpstop -fwflag {-proc|-default}
\end{verbatim}
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-fwflag -proc</td>
<td>Kills Check Point daemons and Security servers while maintaining the active Security Policy running in the kernel. Rules with generic allow/reject/drop rules, based on services continue to work.</td>
</tr>
<tr>
<td>-fwflag -default</td>
<td>Kills Check Point daemons and Security servers. The active Security Policy running in the kernel is replaced with the default filter.</td>
</tr>
</tbody>
</table>

**Comments** This command cannot be used to terminate cprid. cprid is invoked when the appliance or server is booted and it runs independently.

**fw**

**Description** The `fw` commands are used for working with various aspects of the firewall. All `fw` commands are executed on the Check Point Security Gateway.

Typing `fw` at the command prompt sends a list of available `fw` commands to the standard output.

**Syntax**

```
> fw
```

**fw -i**

**Description** Generally, when Check Point Security gateway commands are executed on a Security gateway they will relate to the gateway as a whole, rather than to an individual kernel instance. For example, the `fw tab` command will enable viewing or editing of a single table of information aggregated for all kernel instances.

This command specifies that certain commands apply to an individual kernel instance. By adding `-i <kern>` after `fw` in the command, where `<kern>` is the kernel instance’s number.

**Syntax**

```
> fw -i applies to the following commands:
  > fw ctl debug (when used without the -buf parameter)
  > fw ctl get
  > fw ctl set
  > fw ctl leak
  > fw ctl pstat
  > fw monitor
  > fw tab
```

For details and additional parameters for any of these commands, refer to the command’s entry.

**Example** To view the connections table for kernel instance #1 use the following command:

```
> fw -i 1 tab -t connections
```
fw ctl

**Description**  The `fw ctl` command controls the Firewall kernel module.

**Syntax**

```
fw ctl {install|uninstall}
fw ctl debug [-m <module>] [+|-] {options | all | 0}
fw ctl debug -buf {buffer size}
fw ctl kdebug
fw ctl pstat [-h][-k][-s][-n][-l]
fw ctl iflist
fw ctl arp [-n]
fw ctl block {on|off}
fw ctl chain
fw ctl conn
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `{Install|Uninstall}` | • **Uninstall** — tells the operating system to stop passing packets to the Security Gateway, and unloads the Security Policy. The networks behind it become unprotected.  
  • **Install** — tells the operating system to start passing packets to the Security Gateway. The command `fw ctl install` runs automatically when `cpstart` is performed.  
  **Note** - If you run `fw ctl uninstall` followed by `fw ctl install`, the Security Policy is not restored. |
| `debug`       | Generate debug messages to a buffer. See `fw ctl debug` (on page 221).       |
| `kdebug`      | Reads the debug buffer and obtains the debug messages. If there is no debug buffer, the command will fail.  
  • `[-f]` read the buffer every second and print the messages, until `Ctrl-C` is pressed. Otherwise, read the current buffer contents and end.  
  • `[-t/-T]` print the time field (seconds/microseconds)  
  • `[-p]` to print specific fields: `all|proc|pid|date|mid|type|freq|topic|time|ticks|tid|text|err|host|vsid|cpu`  
  • `[-m]` - number of cyclic files, `[-s]` - size of each |
| `pstat [-h][-k][-s][-n][-l]` | Displays Security Gateway internal statistics:  
  • `-h` — Generates additional hmem details.  
  • `-k` — Generates additional kmem details.  
  • `-s` — Generates additional smem details.  
  • `-n` — Generates NDIS information (Windows only).  
  • `-l` — Generates general Security Gateway statistics. |
| `iflist`      | Displays the IP interfaces known to the kernel, by name and internal number. |
| `arp [-n]`    | Displays ARP proxy table.  
  • `-n` — Do not perform name resolution. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>block {on</td>
<td>off}</td>
</tr>
<tr>
<td>chain</td>
<td>Prints the names of internal Security Gateways that deal with packets. Use to ensure that a gateway is loaded. The names of these gateways can be used in the <code>fw monitor -p</code> command.</td>
</tr>
<tr>
<td>conn</td>
<td>Prints the names of the connection modules.</td>
</tr>
</tbody>
</table>

**fw ctl debug**

**Description** Generate debug messages to a buffer.

**Syntax** A number of debug options are available:

```markdown
fw ctl debug -buf [buffer size]
fw ctl debug [-m <module>] [+ | -] {options|all|0}
fw ctl debug 0
fw ctl debug [-d <comma separated list of strings>]
fw ctl debug [-s <string>]
fw ctl debug -h
fw ctl debug -x
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-buf [buffer size]</td>
<td>Allocates a buffer of size kilobytes (default 128) and starts collecting messages there. If the -buf argument is not set, the debug messages are printed to the console.</td>
</tr>
<tr>
<td>-m &lt;module&gt;</td>
<td>Specify the Security Gateway module you wish to debug. The default module is fw. For example: <code>fw ctl debug -m VPN all</code></td>
</tr>
<tr>
<td>[+</td>
<td>-] &lt;options</td>
</tr>
<tr>
<td></td>
<td>• If + is used, the specified flags are set, and the rest remain as they were.</td>
</tr>
<tr>
<td></td>
<td>• If - is used, the specified flags are reset, and the rest remain as they were.</td>
</tr>
<tr>
<td></td>
<td>• If neither + nor - are used, the specified flags are set and the rest are reset.</td>
</tr>
<tr>
<td>-h</td>
<td>Print a list of debug modules and flags.</td>
</tr>
<tr>
<td>0</td>
<td>Returns all flags in all gateways to their default values, releases the debug buffer (if there was one).</td>
</tr>
<tr>
<td>-d &lt;comma separated list of strings&gt;</td>
<td>Only lines containing these strings are included in the output. [Available in R70 or higher]</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `-d <comma separated list of ^strings>` | Lines containing these strings are omitted from the output (Available in R70 or higher)  
For example:  
`fw ctl debug -d error,failed,^packet`  
Output shows only lines containing the words "error" or "failed" and not the word "packet" |
| `-s <string>`                      | Stop debug messages when a certain string is issues (Available in R70 or higher)  
For example: `fw ctl debug -s error`                                                                                     |
| `-x`                               | Shuts down the debug.                                                                                                                     |

---

**fw ctl affinity**

**fw ctl affinity -s**

**Description**  Sets CoreXL affinities when using multiple processors. For an explanation of kernel, daemon and interface affinities, see the *R77 Performance Tuning Administration Guide* [http://supportcontent.checkpoint.com/documentation_download?ID=24808].

`fw ctl affinity -s` settings are not persistent through a restart of the Security Gateway. If you want the settings to be persistent, either use:

- `sim affinity` (a Performance Pack command)
- Or edit the `fwaffinity.conf` configuration file

To set interface affinities, you should use `fw ctl affinity` only if Performance Pack is not running. If Performance Pack is running, you should set affinities by using the Performance Pack sim affinity command. These settings will be persistent. If Performance Pack’s sim affinity is set to Automatic mode (even if Performance Pack was subsequently disabled), you will not be able to set interface affinities by using `fw ctl affinity -s`.

**Note** - The `fw ctl affinity` command is different for a VSX Gateway and a Security Gateway:

- **VSX Gateway** - Use the `-d` parameter to save the CoreXL affinity settings after you reboot it
- **Security Gateway** - The CoreXL affinity settings are not saved after you reboot it

**Syntax**

```
> fw ctl affinity -s <proc_selection> <cpuid>
```
<proc_selection> is one of the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p &lt;pid&gt;</td>
<td>Sets affinity for a particular process, where &lt;pid&gt; is the process ID#.</td>
</tr>
<tr>
<td>-n &lt;cpdname&gt;</td>
<td>Sets affinity for a Check Point daemon, where &lt;cpdname&gt; is the Check Point daemon name (for example: fwd).</td>
</tr>
<tr>
<td>-k &lt;instance&gt;</td>
<td>Sets affinity for a kernel instance, where &lt;instance&gt; is the instance’s number.</td>
</tr>
<tr>
<td>-i &lt;interfacename&gt;</td>
<td>Sets affinity for an interface, where &lt;interfacename&gt; is the interface name (for example: eth0).</td>
</tr>
</tbody>
</table>

<cpuid> should be a processing core number or a list of processing core numbers. To have no affinity to any specific processing core, <cpuid> should be: all.

Note - Setting an Interface Affinity will set the affinities of all interfaces sharing the same IRQ to the same processing core. To view the IRQs of all interfaces, run: fw ctl affinity -l -v -a.

Example To set kernel instance #3 to run on processing core #5, run:
> fw ctl affinity -s -k 3 5

fw ctl affinity -l

Description Lists existing CoreXL affinities when using multiple processors. For an explanation of kernel, daemon and interface affinities, see the R77 Performance Tuning Administration Guide http://supportcontent.checkpoint.com/documentation_download?ID=24808.

Syntax
> fw ctl affinity -l [<proc_selection>] [<listtype>]

If <proc_selection> is omitted, fw ctl affinity -l lists affinities of all Check Point daemons, kernel instances and interfaces. Otherwise, <proc_selection> is one of the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p &lt;pid&gt;</td>
<td>Displays the affinity of a particular process, where &lt;pid&gt; is the process ID#.</td>
</tr>
<tr>
<td>-n &lt;cpdname&gt;</td>
<td>Displays the affinity of a Check Point daemon, where &lt;cpdname&gt; is the Check Point daemon name (for example: fwd).</td>
</tr>
<tr>
<td>-k &lt;instance&gt;</td>
<td>Displays the affinity of a kernel instance, where &lt;instance&gt; is the instance’s number.</td>
</tr>
<tr>
<td>-i &lt;interfacename&gt;</td>
<td>Displays the affinity of an interface, where &lt;interfacename&gt; is the interface name (for example: eth0).</td>
</tr>
</tbody>
</table>
If `<listtype>` is omitted, `fw ctl affinity -l` lists items with specific affinities, and their affinities. Otherwise, `<listtype>` is one or more of the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-a</code></td>
<td>All: includes items without specific affinities.</td>
</tr>
<tr>
<td><code>-r</code></td>
<td>Reverse: lists each processing core and the items that have it as their affinity.</td>
</tr>
<tr>
<td><code>-v</code></td>
<td>Verbose: list includes additional information.</td>
</tr>
</tbody>
</table>

**Example**  
To list complete affinity information for all Check Point daemons, kernel instances and interfaces, including items without specific affinities, and with additional information, run:

```
> fw ctl affinity -l -a -v
```

### fw ctl engine

**Description**  
Enables the INSPECT2C engine, which dynamically converts INSPECT code to C code.

Run the command on the Check Point Security Gateway.

**Syntax**

```
> fw ctl engine {on|off|stat|setdefault}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `on`      | Compile the engine if necessary, and activate it.  
Because the engine may not have been previously compiled, turning the engine ON may not activate it immediately. Instead, the engine is activated in the background after the compilation.  
After turning the engine ON, the engine recompiles and reactivates itself every policy installation regardless of the values of `inspect2c_compile` and `inspect2c_activate`. |
<p>| <code>off</code>     | Deactivates the engine if active. Subsequent policy installation on the gateway does NOT auto-activate the engine unless the command is used again. |
| <code>stat</code>    | Print the status of the engine. For example: &quot;During compilation&quot;, &quot;Before auto-activation&quot;, &quot;Deactivated&quot;. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>setdefault</td>
<td>Restore control to database settings. Security Management server settings are ignored.</td>
</tr>
<tr>
<td></td>
<td>At the next policy installation, return the control of the engine to the values of the following gateway database attributes:</td>
</tr>
<tr>
<td></td>
<td>- <code>inspect2c_compile [true/false]</code> - controls whether or not the engine is compiled on the gateway during policy installation. Compilation is performed in the background and may take a few minutes.</td>
</tr>
<tr>
<td></td>
<td>- <code>inspect2c_activate [true/false]</code> - controls whether the engine is automatically activated after it is compiled. When set to true, the engine is compiled regardless of the value of <code>inspect2c_compile</code>.</td>
</tr>
<tr>
<td></td>
<td>Use GuiDBEdit to change the values of the attributes.</td>
</tr>
</tbody>
</table>

**fw ctl multik stat**

**Description**  Displays multi-kernel statistics for each kernel instance. The state and processing core number of each instance is displayed, along with:

- The number of connections currently being handled
- The peak number of concurrent connections the instance has handled since its inception

**fw ctl sdstat**

**Description**  The IPS performance counters measure the percentage of CPU consumed by each IPS protection. The measurement itself is divided according to the type of protection: Pattern based protections or INSPECT based protections. In addition, the IPS counters measure the percentage of CPU used by each section (“context”) of the protocol, and each protocol parser.

**Syntax**

```
> fw ctl zdebug >& outputfile
> fw ctl sdstat start
> fw ctl sdstat stop
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fw ctl zdebug &gt;&amp; outputfile</td>
<td>Turn on debug mode and specify an output file.</td>
</tr>
<tr>
<td>fw ctl sdstat start</td>
<td>Activate the IPS counters</td>
</tr>
<tr>
<td>fw ctl sdstat stop</td>
<td>Print a report and stop the counters.</td>
</tr>
</tbody>
</table>

**Example**  The workflow is as follows:

Run the following commands on the Check Point Security Gateway (version R70 or higher):

On the Check Point Security Gateway:

- Run `fw ctl zdebug >& outputfile`
- Run `fw ctl sdstat start`

Let the counters run. However- do not leave the counters on for more than 10 minutes.
• Run `fw ctl sdstat stop`

It is important to stop the counters explicitly, otherwise there may be performance penalty.

This generates the output file `outputfile` that must be processed on the (SecurePlatform only) Security Management Server.

On the Security Management Server:
• From `$FWDIR/script`, run the script
  `./sdstat_analyse.csh outputfile`

The output of the script is a report in csv format that can be viewed in Microsoft Excel.

If there is a problem in the report, or if more details are needed, a debug flag is available which prints extra information to `outputfile`.

• Run `fw ctl zdebug + spii >& outputfile`

<table>
<thead>
<tr>
<th>Example Debug Message</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>`sdstat_get_stats_all Instances : Smart Defense</td>
<td>User tried to create a report without initializing the counters, or an error occurred during initialization and the user then tried to print a report.</td>
</tr>
<tr>
<td>report objects are not initialized, hence no report can be done.</td>
<td></td>
</tr>
<tr>
<td><code>FW-1 - sdstats_print_report: Failed to calculate Smart Defense (total_smart_defense is 0)</code></td>
<td>The measurement process failed and the total time units for IPS is zero.</td>
</tr>
</tbody>
</table>

**Comments**

1. A value in the report of "< 1" means that the percentage of CPU used by a protection is less than 1%.
2. The report generated by the `sdstat_analyse` script may contain a number instead of a protection name. This is because the original output contains a signature id, but the id is missing from the Security Policy on the Gateway.

**fw fetch**

**Description**  Fetches the Inspection Code from the specified host and installs it to the kernel.

**Syntax**

```
> fw fetch [-n] [-f <filename>] [-c] [-i] master1 [master2] ...
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-n</code></td>
<td>Fetch the Security Policy from the Security Management server to the local state directory, and install the Policy only if the fetched Policy is different from the Policy already installed.</td>
</tr>
<tr>
<td><code>-f &lt;filename&gt;</code></td>
<td>Fetch the Security Policy from the Security Management server listed in <code>&lt;filename&gt;</code>. If filename is not specified, the list in conf/masters is used.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>-c</td>
<td>Cluster mode, get policy from one of the cluster members, from the Check Point High Availability (CPHA) kernel list.</td>
</tr>
<tr>
<td>-i</td>
<td>Ignore SIC information (for example, SIC name) in the database and use the information in conf/masters. This option is used when a Security Policy is fetched for the first time by a DAIP gateway from a Security Management server with a changed SIC name.</td>
</tr>
<tr>
<td>master1</td>
<td>Execute command on the designated master. The IP address of the Security Management Server from which to fetch the Policy. You can specify one or more servers, which will be searched in the order listed. If no targets is not specified, or if targets is inaccessible, the Policy is fetched from localhost.</td>
</tr>
</tbody>
</table>

**fw fetchlogs**

**Description**  
`fw fetchlogs` fetches Log Files from a remote machine. You can use the `fw fetchlogs` command to transfer Log Files to the machine on which the `fw fetchlogs` command is executed. The Log Files are read from and written to the directory `$FWDIR/log`.

**Syntax**

```
> fw fetchlogs [[-f <file name>] ... ] <module>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f</td>
<td>The Log Files to be transferred. The file name can include wildcards. In Solaris, any file containing wildcards should be enclosed in quotes. The default parameter is *.log. Related pointer files will automatically be fetched.</td>
</tr>
<tr>
<td>&lt;module&gt;</td>
<td>The name of the remote machine from where you transfer the Log Files.</td>
</tr>
</tbody>
</table>

**Comments**  
The files transferred by the `fw fetchlogs` command are MOVED from the source machine to the target machine. This means that they are deleted from the source machine once they have been successfully copied.

**Fetching Current Log Data**

The active Log File (`fw.log`) cannot be fetched. If you want to fetch the most recent log data, proceed as follows:

- Run `|` to close the currently active Log File and open a new one.
- Run `fw lslogs` to see the newly-generated file name.
- Run `fw fetchlogs -f filename` to transfer the file to the machine on which the `fw fetchlogs` command is executed. The file is now available for viewing in the SmartView Tracker.
After a file has been fetched, it is renamed. The gateway name and the original Log File name are concatenated to create a new file name. The new file name consists of the gateway name and the original file name separated by two (underscore) \_\_ characters.

**Example**

The following command:

```
> fw fetchlogs -f 2001-12-31_123414.log module3
```

fetches the Log File `2001-12-31_123414.log` from Module3.

After the file has been fetched, the Log File is renamed:

```
module3_\_2001-12-31_123414.log
```

**fw hastat**

**Description**

The `fw hastat` command displays information about High Availability machines and their states.

**Syntax**

```
> fw hastat [target]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;target&gt;</td>
<td>A list of machines whose status will be displayed. If <code>target</code> is not specified, the status of the local machine will be displayed.</td>
</tr>
</tbody>
</table>

**fw isp_link**

**Description**

Takes down (or up) a redundant ISP link.

**Syntax**

```
> fw isp_link [target] <link-name> {up|down}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>The name of the Check Point Security Gateway.</td>
</tr>
<tr>
<td>link-name</td>
<td>The name of the ISP link as defined in the ISP-redundancy tab.</td>
</tr>
</tbody>
</table>

**Comments**

This command can be executed locally on the Check Point Security Gateway or remotely from the Security Management server. In the latter case, the target argument must be supplied. For this command to work, the Check Point Security Gateway should be using the ISP redundancy feature.

**fw kill**

**Description**

Prompts the kernel to shut down all firewall daemon processes. The command is located in the `$FWDIR/bin` directory on the Security Management server or gateway machine.

The firewall daemons and Security servers write their pids to files in the `$FWDIR/tmp` directory upon startup. These files are named `$FWDIR/tmp/daemon_name.pid`. For example, the file containing the pid of the firewall `snmp` daemon is: `$FWDIR/tmp/snmpd.pid`.

**Syntax**

```
> fw kill [-t <sig_no>] <proc-name>
```
### Security Management Server and Firewall Commands

#### Parameter  Description

- **-t** `<sig_no>`
  - This Unix only command specifies that if the file `$FWDIR/tmp/proc-name.pid` exists, send signal `sig_no` to the pid given in the file.
  - If no signal is specified, signal 15 (`sigterm` or the terminate command) is sent.

- `<proc-name>`
  - Prompt the kernel to shut down specified firewall daemon processes.

**Comments**
- In Windows, only the default syntax is supported: `fw kill proc_name`. If the `-t` option is used it is ignored.

### fw lea_notify

**Description**
- Send a `LEA_COL_LOGS` event to all connected lea clients, see the *LEA Specification* documentation. It should be used after new log files have been imported (manually or automatically) to the `$FWDIR/log` directory in order to avoid the scheduled update which takes 30 minutes.

- This command should be run from the Security Management server.

**Syntax**

```
> fw lea_notify
```

### fw lichosts

**Description**
- Print a list of hosts protected by Security Gateway products. The list of hosts is in the file `$fwdir/database/fwd.h`

**Syntax**

```
> fw lichosts [-x] [-l]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-x</code></td>
<td>Use hexadecimal format</td>
</tr>
<tr>
<td><code>-l</code></td>
<td>Use long format</td>
</tr>
</tbody>
</table>

### fw log

**Description**
- `fw log` displays the content of Log files.

**Syntax**

```
> fw log [-f [-t]] [-n] [-l] [-o] [-c <action>] [-h <host>] [-s <starttime>] [-e <endtime>] [-b <starttime> <endtime>] [-u <unification_scheme_file>] [-m {initial|semi|raw}] [-a] [-k {alert_name|all}] [-g] [logfile]
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-f [-t]</code></td>
<td>After reaching the end of the currently displayed file, do not exit (the default behavior), but continue to monitor the Log file indefinitely and display it while it is being written. The <code>-t</code> parameter indicates that the display is to begin at the end of the file, in other words, the display will initially be empty and only new records added later will be displayed. <code>-t</code> must come with a <code>-f</code> flag. These flags are relevant only for active files.</td>
</tr>
<tr>
<td><code>-n</code></td>
<td>Do not perform DNS resolution of the IP addresses in the Log file (the default behavior). This option significantly speeds up the processing.</td>
</tr>
<tr>
<td><code>-l</code></td>
<td>Display both the date and the time for each log record (the default is to show the date only once above the relevant records, and then specify the time per log record).</td>
</tr>
<tr>
<td><code>-o</code></td>
<td>Show detailed log chains (all the log segments a log record consists of).</td>
</tr>
<tr>
<td><code>-c &lt;action&gt;</code></td>
<td>Display only events whose action is action, that is, accept, drop, reject, authorize, deauthorize, encrypt and decrypt. Control actions are always displayed.</td>
</tr>
<tr>
<td><code>-h &lt;host&gt;</code></td>
<td>Display only log whose origin is the specified IP address or name.</td>
</tr>
<tr>
<td><code>-s &lt;starttime&gt;</code></td>
<td>Display only events that were logged after the specified time (see time format below). <code>starttime</code> may be a date, a time, or both. If date is omitted, then today’s date is assumed.</td>
</tr>
<tr>
<td><code>-e &lt;endtime&gt;</code></td>
<td>Display only events that were logged before the specified time (see time format below). <code>endtime</code> may be a date, a time, or both.</td>
</tr>
<tr>
<td><code>-b &lt;starttime&gt; &lt;endtime&gt;</code></td>
<td>Display only events that were logged between the specified start and end times (see time format below), each of which may be a date, a time, or both. If date is omitted, then today’s date is assumed. The start and end times are expected after the flag.</td>
</tr>
<tr>
<td><code>-u &lt;unification_scheme_file&gt;</code></td>
<td>Unification scheme file name.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>-m</td>
<td>This flag specifies the unification mode.</td>
</tr>
<tr>
<td></td>
<td>• initial - the default mode, specifying complete unification of log records; that is, output one unified record for each id. This is the default. When used together with -f, no updates will be displayed, but only entries relating to the start of new connections. To display updates, use the semi parameter.</td>
</tr>
<tr>
<td></td>
<td>• semi - step-by-step unification, that is, for each log record, output a record that unifies this record with all previously-encountered records with the same id.</td>
</tr>
<tr>
<td></td>
<td>• raw - output all records, with no unification.</td>
</tr>
<tr>
<td>-a</td>
<td>Output account log records only.</td>
</tr>
<tr>
<td>-k</td>
<td>Display only events that match a specific alert type. The default is all, for any alert type.</td>
</tr>
<tr>
<td>{&lt;alert_name&gt;</td>
<td>all}</td>
</tr>
<tr>
<td>-g</td>
<td>Do not use a delimited style. The default is:</td>
</tr>
<tr>
<td></td>
<td>• : after field name</td>
</tr>
<tr>
<td></td>
<td>• ; after field value</td>
</tr>
</tbody>
</table>

logfile  
Use logfile instead of the default Log file. The default Log File is $FWDIR/log/fw.log.

Where the full date and time format is: MMM DD, YYYY HH:MM:SS. For example: May 26, 1999 14:20:00

It is possible to specify date only in the format MMM DD, YYYY, or time only, in the format: HH:MM:SS, where time only is specified, the current date is assumed.

Example

```bash
> fw log
> fw log | more
> fw log -c reject
> fw log -s "May 26, 1999"
> fw log -f -s 16:00:00
```

Output [<date>] <time> <action> <origin> <interface dir and name> [alert] [field name: field value;] ...

Each output line consists of a single log record, whose fields appear in the format shown above.

Example Output

```
14:56:39 reject jam.checkpoint.com >daemon alert src: veredr.checkpoint.com; dst: jam.checkpoint.com; user: a; rule: 0; reason: Client Encryption: Access denied - wrong user name or password ; scheme: IKE; reject_category: Authentication error; product: Security Gateway
14:57:49 authcrypt jam.checkpoint.com >daemon src: veredr.checkpoint.com; user: a; rule: 0; reason: Client Encryption: Authenticated by Internal Password; scheme: IKE; methods: AES-256,IKE,SHA1; product: Security Gateway; peer gateway: veredr.checkpoint.com; scheme: IKE; IKE: Main Mode completion.; CookieI: 32f09ca38aeeaf4a3; CookieR: 73b91d59b378958c; msgid: 47ad4a8d; methods: AES-256 + SHA1, Internal Password; user: a; product: Security Gateway;
```
**fw logswitch**

**Description**  
`fw logswitch` creates a new active Log File. The current active Log File is closed and renamed by default `$FWDIR/log/<current_time_stamp>.log` unless you define an alternative name that is unique. The format of the default name `<current_time_stamp>.log` is `YYYY-MM-DD_HHMMSS.log`. For example: `2003-03-26_041200.log`

**Warning:**
- The Logswitch operation fails if a log file is given a pre-existing file name.
- The rename operation fails on Windows if the active log that is being renamed, is open at the same time that the rename operation is taking place; however; the Logswitch will succeed and the file will be given the default name `$FWDIR/log/current_time_stamp.log`.

The new Log File that is created is given the default name `$FWDIR/log/fw.log`. Old Log Files are located in the same directory.

A Security Management server can use `fw logswitch` to change a Log File on a remote machine and transfer the Log File to the Security Management server. This same operation can be performed for a remote machine using `fw lslogs` (on page 237) and `fw fetchlogs` (on page 227).

When a log file is sent to the Security Management server, the data is compressed.

**Syntax**

```
> fw logswitch [-audit] [<filename>]
> fw logswitch -h <hostage> [+|-][<filename>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-audit</code></td>
<td>Does logswitch for the Security Management server audit file. This is relevant for local activation.</td>
</tr>
<tr>
<td><code>&lt;filename&gt;</code></td>
<td>The name of the file to which the log is saved. If no name is specified, a default name is provided.</td>
</tr>
<tr>
<td><code>-h &lt;hostage&gt;</code></td>
<td>The resolvable name or IP address of the remote machine (running either a Security Gateway or a Security Management server) on which the Log File is located. The Security Management server (on which the <code>fw logswitch</code> command is executed) must be defined as one of host’s Security Management servers. In addition, you must initialize SIC between the Security Management server and the host.</td>
</tr>
<tr>
<td><code>+</code></td>
<td>Change a remote log and copy it to the local machine.</td>
</tr>
<tr>
<td><code>-</code></td>
<td>Change a remote log and move it to the local machine thereby deleting the log from the remote machine.</td>
</tr>
</tbody>
</table>

**Comments**

Files are created in the `$FWDIR/log` directory on both `host` and the Security Management server when the `+` or `−` parameters are specified. Note that if `−` is specified, the Log File on the host is deleted rather than renamed.

- `hostage` specified:
  - `filename` specified - On `hostage`, the old Log File is renamed to `old_log`. On the Security Management Server, the copied file will have the same name, prefixed by `hostage`’s name.
For example, the command `fw logswitch -h venus +xyz` creates a file named `venus_xyz.log` on the Security Management Server.

- **filename** not specified - On *hostage*, the new name is the current date, for example: `2003-03-26_041200.log`. On the Security Management Server, the copied file will have the same name, but prefixed by `hostage_`. For example, `target_2003-03-26_041200.log`.

*hostage* not specified:
- **filename** specified - On the Security Management Server, the old Log File is renamed to `old_log`.
- **filename** not specified - On the Security Management Server, the old Log File is renamed to the current date.

**Compression**

When log files are transmitted from one machine to another, they are compressed using the **zlib** package, a standard package used in the Unix **gzip** command [see RFC 1950 to RFC 1952 for details]. The algorithm is a variation of LZ77 method.

The compression ratio varies with the content of the log records and is difficult to predict. Binary data are not compressed, but string data such as user names and URLs are compressed.

**fw mergefiles**

**Description**  
Merge several Log Files into a single Log File. The merged file can be sorted according to the creation time of the Log entries, and the times can be “fixed” according to the time zones of the origin Log servers.

Logs entries with the same Unique-ID are unified. If a Log switch was performed before all the segments of a specific log were received, this command will merge the records with the same Unique-ID from two different files, into one fully detailed record.

**Syntax**

```
fw mergefiles [-s] [-t <time_conversion_file>] <log_file_name_1> [...
<log_file_name_n>] <output_file>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-s</code></td>
<td>Sort merged file by log records time field.</td>
</tr>
</tbody>
</table>
| `-t` <time_conversion_file> | Fix different GMT zone log records time in the event that the log files originated from Log Servers in different time zone.  
The time_conversion_file format is as follows:  
`ip-address signed_date_time_in_seconds`  
`ip-address signed_date_time_in_seconds` |
| `<log_file_name_n>` | Full pathnames of the Log File(s).                                         |
| `<output_file>`  | Full pathname of the output Log File.                                       |

**Comments**

It is not recommended to merge the current active `fw.log` file with other Log Files. Instead, run the `fw logswitch` command and then run `fw mergefiles`. 
fw monitor

Description  Inspecting network traffic is an essential part of troubleshooting network deployments. `fw monitor` is a powerful built-in tool to simplify the task of capturing network packets at multiple capture points within the firewall chain. These packets can be inspected using industry-standard tools later on.

In many deployment and support scenarios capturing network packets is an essential functionality. `tcpdump` or `snoop` are tools normally used for this task. `fw monitor` provides an even better functionality but omits many requirements and risks of these tools.

- **No Security Flaws** — `tcpdump` and `snoop` are normally used with network interface cards in promiscuous mode. Unfortunately the promiscuous mode allows remote attacks against these tools. `fw monitor` does not use the promiscuous mode to capture packets. In addition most firewall operating systems are hardened. In most cases this hardening includes the removal of tools like `tcpdump` or `snoop` because of their security risk.

- **Available on all Security Gateway installations** — `fw monitor` is a built-in firewall tool which needs no separate installation in case capturing packets is needed. It is a functionality provided with the installation of the Firewall package.

- **Multiple capture positions within the firewall kernel module chain** — `fw monitor` allows you to capture packets at multiple capture positions within the firewall kernel module chain; both for inbound and outbound packets. This enables you to trace a packet through the different functionalities of the Firewall.

- **Same tool and syntax on all platforms** — Another important fact is the availability of `fw monitor` on different platforms. Tools like `snoop` or `tcpdump` are often platform dependent or have specific “enhancements” on certain platforms. `fw monitor` and all its related functionality and syntax is absolutely identical across all platforms. There is no need to learn any new “tricks” on an unknown platform.

Normally the Check Point kernel modules are used to perform several functions on packets (like filtering, encrypting and decrypting, QoS ...). `fw monitor` adds its own modules to capture packets. Therefore `fw monitor` can capture all packets which are seen and/or forwarded by the Firewall.

Only one instance of `fw monitor` can be run at a time.

Use `^C` (that is Control + C) to stop `fw monitor` from capturing packets.

Syntax

```plaintext
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`-u</td>
<td>s`</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>-i</td>
<td><strong>Flushing the standard output:</strong> Use to make sure that captured data for each packet is at once written to standard output. This is especially useful if you want to kill a running fw monitor process and want to be sure that all data is written to a file.</td>
</tr>
<tr>
<td>[-d] [-D]</td>
<td><strong>Debugging fw monitor:</strong> The -d option is used to start fw monitor in debug mode. This will give you an insight into fw monitor’s inner workings. This option is only rarely used outside Check Point. It is also possible to use –D to create an even more verbose output.</td>
</tr>
</tbody>
</table>
| {-e <expr>|-f <filter-file>|-} | **Filtering fw monitor packets:** fw monitor has the ability to capture only packets in which you are interested. fw monitor filters use a subset of INSPECT to specify the packets to be captured. Set the filter expression:  
  - on the command line using the –e switch.  
  - by reading it from a file using the –f switch.  
  - by reading it from standard input using the –f – switch. |
<p>| -l &lt;len&gt;  | <strong>Limiting the packet length:</strong> fw monitor lets you limit the packet data which will be read from the kernel with -l. This is especially useful if you have to debug high sensitive communication. It lets you to capture only the headers of a packet (e.g. IP and TCP header) while omitting the actual payload. Therefore you can debug the communication without seeing the actual data transmitted. Another possibility is to keep the amount of data low. If you don’t need the actual payload for debugging you can decrease the file site by omitting the payload. It’s also very useful to reduce packet loss on high-loaded machines. fw monitor uses a buffer to transfer the packets from kernel to user space. If you reduce the size of a single packet this buffer won’t fill up so fast. |
| -m &lt;mask&gt; | <strong>Setting capture masks:</strong> By default fw monitor captures packets before and after the virtual machine in both directions. These positions can be changed. This option allows you to specify in which of the four positions you are interested. |
| -x &lt;offset&gt;[,&lt;len&gt;] | <strong>Printing packet/payload data:</strong> In addition to the IP and Transport header fw monitor can also print the packets’ raw data using the –x option. Optionally it is also possible to send all data that is written only to the screen the data written. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| -o <file> | **Write output to file:** Save the raw packet data to a file in a standard (RFC 1761) format. The file can be examined using by tools like snoop, tcpdump or Ethereal.  
**Note** - The snoop file format is normally used to store Layer 2 frames. For “normal” capture files this means that the frame includes data like a source and a destination MAC address. `fw monitor` operates in the firewall kernel and therefore has no access to Layer 2 information like MAC addresses. Instead of writing random MAC addresses, `fw monitor` includes information like interface name, direction and chain position as "MAC addresses". |
| -T | Print time stamp in microseconds. `-T` is needed only when `-o` is not used. When `-o` is used the exact time is written to the snoop file by default as of Corsica. |
| `[-pi <pos>] [-pI <pos>] [-po <pos>] [-pO <pos>] | `[-p all]` | **Insert fw monitor chain module at a specific position:** In addition to capture masks (which give the ability to look at packets in a specific position) `fw monitor` has the ability to define where exactly in the firewall chain the packets should be captured. This can be defined using these options. |
| -a | **Use absolute chain positions:** If you use `fw monitor` to output the capture into a file (option `-o`), one of the fields written down to the capture file is the chain position of the `fw monitor` chain module. Together with a simultaneous execution of `fw ctl chain` you can determine where the packet was captured. Especially when using `-p all` you will find the same packet captured multiples times at different chain positions. The option `-a` changes the chain ID from a relative value (which only makes sense with the matching `fw ctl chain` output) to an absolute value. These absolute values are known to CPEthereal and can be displayed by it. |
| `[-ci <count>] [-co <count>] | **Capture a specific number of packets:** `fw monitor` enables you to limit the number of packets being captured. This is especially useful in situations where the firewall is filtering high amounts of traffic. In such situations `fw monitor` may bind so many resources (for writing to the console or to a file) that recognizing the break sequence (Control-C) might take very long. |
| -h | Displays the usage. |

**Example** The easiest way to use `fw monitor` is to invoke it without any parameter. This will output every packet from every interface that passes (or at least reaches) the Check Point Security Gateway. The same packet appears several times (two times in the example below). This is caused by `fw monitor` capturing the packets at different capture points.
Output

cpmodule> fw monitor
  monitor: getting filter (from command line)
  monitor: compiling
  monitorfilter:
  Compiled OK.
  monitor: loading
  monitor: monitoring (control-C to stop)
eth0:i[285]: 192.0.2.133 -> 192.0.2.2 (TCP) len=285 id=1075
  TCP: 1050 -> 18190 ...PA. seq=bf8bc98e ack=941b05bc
eth0:I[285]: 192.0.2.133 -> 192.0.2.2 (TCP) len=285 id=1075
  TCP: 1050 -> 18190 ...PA. seq=bf8bc98e ack=941b05bc
eth0:o[197]: 192.0.2.2 -> 192.0.2.133 (TCP) len=197 id=44599
  TCP: 18190 -> 1050 ...PA. seq=941b05bc ack=bf8bca83
eth0:O[197]: 192.0.2.2 -> 192.0.2.133 (TCP) len=197 id=44599
  TCP: 18190 -> 1050 ...PA. seq=941b05bc ack=bf8bca83
eth0:o[1500]: 192.0.2.2 -> 192.0.2.133 (TCP) len=1500 id=44600
  TCP
  ^C
  : 18190 -> 1050 ....A. seq=941b0659 ack=bf8bca83
  monitor: caught sig 2
  monitor: unloading

The first line of the fw monitor output is

cpmodule> fw monitor
eth0:i[285]: 192.0.2.133 -> 192.0.2.2 (TCP) len=285 id=1075

This packet was captured on the first network interface (eth0) in inbound direction before the
virtual machine (lowercase i). The packet length is 285 bytes (in square parenthesis; repeated at
the end of the line. Note that these two values may be different. The packets ID is 1075. The packet
was sent from 192.0.2.133 to 192.0.2.2 and carries a TCP header/payload.

The second line of the fw monitor output is

TCP: 1050 -> 18190 ...PA. seq=bf8bc98e ack=941b05bc

The second line tells us that this is a TCP payload inside the IP packet which was sent from port
1050 to port 18190. The following element displays the TCP flags set (in this case PUSH and ACK).
The last two elements are showing the sequence number (seq=bf8bc98e) of the TCP packet and
the acknowledged sequence number (ack=941b05bc). You will see similar information for UDP
packets.

You will only see a second line if the transport protocol used is known to fw monitor. Known
protocols are for example TCP, UDP and ICMP. If the transport protocol is unknown or cannot be
analyzed because it is encrypted (e.g. ESP or encapsulated (e.g. GRE) the second line is missing.

Further Info.  See SecureKnowledge solution sk30583

fw lslgs

Description  Display a list of Log Files residing on a remote or local machine. You must initialize
SIC between the Security Management server and the remote machine.

Syntax

> fw lslgs [[-f <filename>] ...] [-e] [-s {<name>|<size>|<stime>|<etime>}] [-r] [<machine>]
**Security Management Server and Firewall Commands**

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f &lt;filename&gt;</td>
<td>The list of files to be displayed. The file name can include wildcards. In Unix, any file containing wildcards should be enclosed in quotes. The default parameter is *.log.</td>
</tr>
</tbody>
</table>
| -e | Display an extended file list. It includes the following data:  
  - **Size** - The size of the file and its related pointer files together.  
  - **Creation Time** - The time the Log File was created.  
  - **Closing Time** - The time the Log File was closed.  
  - **Log File Name** - The file name. |
| -s | Specify the sort order of the Log Files using one of the following sort options:  
  - **name** - The file name.  
  - **size** - The file size.  
  - **stime** - The time the Log File was created.  
  - **etime** - The time the Log File was closed.  
  The default is stime. |
| -r | Reverse the sort order (descending order). |
| <machine> | The name of the machine on which the files are located. It can be a gateway or a Log Server. The default is localhost. |

**Example**

This example shows the extended file list you see when you use the `fw lslogs -e` command:

```
> fw lslogs -e module3
Size  Creation Time       Closing Time         Log file name
16KB  10Jan2002 18:36:05  --                    fw.log
```

**fw putkey**

**Description**

Install a Check Point authentication password on a host. This password is used to authenticate internal communications between Security Gateways and between a Check Point Security Gateway and its Security Management server. A password is used to authenticate the control channel the first time communication is established. This command is required for backward compatibility scenarios.

**Syntax**

```bash
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-opsec</td>
<td>Only control connections are enabled.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-no_opsec</td>
<td>Only OPSEC control connections are enabled.</td>
</tr>
<tr>
<td>-ssl</td>
<td>The key is used for an SSL connection.</td>
</tr>
<tr>
<td>-no_ssl</td>
<td>The key is not used for an SSL connection.</td>
</tr>
<tr>
<td>-k &lt;num&gt;</td>
<td>The length of the first S/Key password chain for fwa1 authentication (Check Point’s proprietary authentication protocol). The default is 7. When fewer than 5 passwords remain, the hosts renegotiate a chain of length 100, based on a long random secret key. The relatively small default value ensures that the first chain, based on a short password entered by the user, is quickly exhausted.</td>
</tr>
<tr>
<td>-n &lt;myname&gt;</td>
<td>The IP address (in dot notation) to be used by the Check Point Security Gateway when identifying this host to all other hosts, instead of, for example, the resolution of the hostname command.</td>
</tr>
<tr>
<td>-p &lt;psw&gt;</td>
<td>The key (password). If you do not enter the password on the command line, you will be prompted for it.</td>
</tr>
<tr>
<td>&lt;host&gt;</td>
<td>The IP address(es) or the resolvable name(s) of the other host(s) on which you are installing the key (password). This should be the IP address of the interface “closest” to the host on which the command is run. If it is not, you will get error messages such as the following: “./fwd: Authentication with hostname for command sync failed”</td>
</tr>
</tbody>
</table>

**Comments**  
This command is never used in a script.

**fw repairlog**

**Description**  
`fw repairlog` rebuilds a Log file’s pointer files. The three files: `name.logptr`, `name.loginitial_ptr` and `name.logaccount_ptr` are recreated from data in the specified Log file. The Log file itself is modified only if the -u flag is specified.

**Syntax**  
`fw repairlog [-u] <logfile>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-u</td>
<td>Indicates that the unification chains in the Log file should be rebuilt.</td>
</tr>
<tr>
<td>&lt;logfile&gt;</td>
<td>The name of the Log file to repair.</td>
</tr>
</tbody>
</table>

**fw sam**

**Description**  
Manage the Suspicious Activity Monitoring (SAM) server. Use the SAM server to block connections to and from IP addresses without the need to change the Security Policy.

SAM commands are logged. Use this command to (also) monitor active SAM requests (see -M option).

To configure the SAM server on the Security Management server or Security Gateway, use SmartDashboard to edit the Advanced > SAM page of the Check Point Security Gateway object.
Syntax

Add/Cancel SAM rule according to criteria:

> fw sam [-v] [-s <sam server>][-S <server sic name>][-f <fw host>][-t <timeout>][-1 <log>][-C] -{n|i|I|j|J} <Criteria>

Delete all SAM rules:

> fw sam [-v] [-s <sam server>][-S <server sic name>][-f <fw host>] -D

Monitor all SAM rules:

> fw sam [-v] [-s <sam server>][-S <server sic name>][-f <fw host>] -M {-i|j|n} all

Monitor SAM rules according to criteria:

> fw sam [-v] [-s <sam server>][-S <server sic name>][-f <fw host>] -M {-i|j|n} <Criteria>

Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-v</td>
<td>Verbose mode. Writes one message (describing whether the command was successful or not) to stderr for each Security Gateway machine on which the command is enforced.</td>
</tr>
<tr>
<td>-s &lt;sam_server&gt;</td>
<td>The IP address (in dot format) or the resolvable name of the FireWalled host that will enforce the command. The default is localhost.</td>
</tr>
<tr>
<td>-S &lt;server_sic_name&gt;</td>
<td>The SIC name for the SAM server to be contacted. It is expected that the SAM server will have this SIC name, otherwise the connection will fail. If no server SIC name is supplied the connection will proceed without SIC names comparison. For more information about enabling SIC refer to the OPSEC API Specification.</td>
</tr>
</tbody>
</table>
| -f <fw host>       | Specify the host, the Security Gateway machine on which to enforce the action. host can be one of the following (default is All):
<p>|                    | • localhost—Specify the computer running the SAM server to enforce the action on it.                                                      |
|                    | • The name of the object or group—the action is enforced on this object; if this object is a group, on every object in the group.                |
|                    | • Gateways—Action enforced on FireWalls defined as gateways and managed by Security Management server where the SAM server runs.               |
|                    | • All—Enforced on FireWalls managed by Smart-Center server where SAM server runs.                                                           |
| -D                 | Cancel all inhibit [-i, -j, -I, -J] and notify [-n] commands. To “uninhibit” inhibited connections, execute fw sam with the -C or -D parameters. It is also possible to use this command for active SAM requests. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-C</td>
<td>Cancel the command to inhibit connections with the specified parameters. These connections will no longer be inhibited (rejected or dropped). The command parameters must match the ones in the original command, except for the <code>-t [timeout]</code> parameter.</td>
</tr>
<tr>
<td>-t &lt;timeout&gt;</td>
<td>The time period (in seconds) for which the action will be enforced. The default is forever or until cancelled.</td>
</tr>
<tr>
<td>-l &lt;log&gt;</td>
<td>The type of the log for enforced actions can be one of the following: <code>nolog</code>, <code>long_noalert</code>, <code>long_alert</code>. The default is <code>long_alert</code>.</td>
</tr>
<tr>
<td>-n</td>
<td>Notify, or generate, a long-format log entry. Generates an alert when connections that match the specified services or IP addresses pass through the FireWall. This action does not inhibit or close connections.</td>
</tr>
<tr>
<td>-i</td>
<td>Inhibit (do not allow) new connections with the specified parameters. Each inhibited connection is logged according to log type. Matching connections will be rejected.</td>
</tr>
<tr>
<td>-I</td>
<td>Inhibit new connections with the specified parameters, and close all existing connections with the specified parameters. Each inhibited connection is logged according to the log type. Matching connections will be rejected.</td>
</tr>
<tr>
<td>-j</td>
<td>Inhibit new connections with the specified parameters. Each inhibited connection is logged according to the log type. Connections will be dropped.</td>
</tr>
<tr>
<td>-J</td>
<td>Inhibit new connections with the specified parameters, and close all existing connections with the specified parameters. Each inhibited connection is logged according to the log type. Connections will be dropped.</td>
</tr>
<tr>
<td>-M</td>
<td>Monitor the active SAM requests with the specified actions and criteria.</td>
</tr>
<tr>
<td>all</td>
<td>Get all active requests. For monitoring purposes only.</td>
</tr>
</tbody>
</table>

**Usage** Criteria are used to match connections, and are composed of various combinations of the following parameters:

```
<src ip><src netmask><dst ip><dst netmask>
<service><protocol>
```
Possible combinations are:

```
src <ip>
dst <ip>
any <ip>
subsrc <ip><netmask>
subdst <ip><netmask>
subany <ip><netmask>
srv <src ip><dest ip><service><protocol>
subsrv <src ip><src netmask><dest ip><dest netmask><service><protocol>
subsrvd <src ip><dest ip><dest netmask><service><protocol>
dstsrv <dest ip><service><protocol>
subdstsrv <dest ip><dest netmask><service><protocol>
srccpr <ip><protocol>
dstpr <ip><protocol>
subsrccpr <ip><netmask><protocol>
subdstpr <ip><netmask><protocol>

Syntax
```

<table>
<thead>
<tr>
<th>Criteria Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>src &lt;ip&gt;</td>
<td>Match the source IP address of the connection.</td>
</tr>
<tr>
<td>dst &lt;ip&gt;</td>
<td>Match the destination IP address of the connection.</td>
</tr>
<tr>
<td>any &lt;ip&gt;</td>
<td>Match either the source IP address or the destination IP address of the connection.</td>
</tr>
<tr>
<td>subsrc &lt;ip&gt; &lt;netmask&gt;</td>
<td>Match the source IP address of the connections according to the netmask.</td>
</tr>
<tr>
<td>subdst &lt;ip&gt; &lt;netmask&gt;</td>
<td>Match the destination IP address of the connections according to the netmask.</td>
</tr>
<tr>
<td>subany &lt;ip&gt; &lt;netmask&gt;</td>
<td>Match either the source IP address or destination IP address of connections according to the netmask.</td>
</tr>
<tr>
<td>srv &lt;src ip&gt; &lt;dst ip&gt; &lt;service&gt; &lt;protocol&gt;</td>
<td>Match the specific source IP address, destination IP address, service and protocol.</td>
</tr>
<tr>
<td>subsrv &lt;src ip&gt; &lt;netmask&gt; &lt;dst ip&gt; &lt;netmask&gt; &lt;service&gt; &lt;protocol&gt;</td>
<td>Match the specific source IP address, destination IP address, service and protocol. Source and destination IP addresses are assigned according to the netmask.</td>
</tr>
<tr>
<td>subsrvs &lt;src ip&gt; &lt;src netmask&gt; &lt;dest ip&gt; &lt;service&gt; &lt;protocol&gt;</td>
<td>Match the specific source IP address, source netmask, destination netmask, service and protocol.</td>
</tr>
<tr>
<td>subsrved &lt;src ip&gt; &lt;dest ip&gt; &lt;dest netmask&gt; &lt;service&gt; &lt;protocol&gt;</td>
<td>Match specific source IP address, destination IP, destination netmask, service and protocol.</td>
</tr>
<tr>
<td>dstsrv &lt;dest ip&gt; &lt;service&gt; &lt;protocol&gt;</td>
<td>Match specific destination IP address, service and protocol.</td>
</tr>
</tbody>
</table>
Criteria Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>subdstsrv &lt;dst ip&gt; &lt;netmask&gt; &lt;service&gt; &lt;protocol&gt;</td>
<td>Match specific destination IP address, service and protocol. Destination IP address is assigned according to the netmask.</td>
</tr>
<tr>
<td>srcpr &lt;ip&gt; &lt;protocol&gt;</td>
<td>Match the source IP address and protocol.</td>
</tr>
<tr>
<td>dstpr &lt;ip&gt; &lt;protocol&gt;</td>
<td>Match the destination IP address and protocol.</td>
</tr>
<tr>
<td>subsrsrcr &lt;ip&gt; &lt;netmask&gt; &lt;protocol&gt;</td>
<td>Match the source IP address and protocol of connections. Source IP address is assigned according to the netmask.</td>
</tr>
<tr>
<td>substpr &lt;ip&gt; &lt;netmask&gt; &lt;protocol&gt;</td>
<td>Match the destination IP address and protocol of connections. Destination IP address is assigned according to the netmask.</td>
</tr>
</tbody>
</table>

Example

This command inhibits all connections originating on louvre for 10 minutes. Connections made during this time will be rejected:

> fw sam -t 600 -i src louvre

This command inhibits all FTP connections from the louvre subnet to the eifel subnet. All existing open connections will be closed. New connection will be dropped, a log is kept and an alert is sent:

> fw sam -l long_alert -J subsrvs louvre 255.255.255.0 eifel 21 6

The previous command will be enforced forever - or until canceled by the following command:

> fw sam -C -l long_alert -J subsrvs louvre 255.255.255.0 eifel 21 6

This command monitors all active “inhibit” or “notify SAM” requests for which lourve is the source or destination address:

> fw sam -M -nij any lourve

This command cancels the command in the first example:

> fw sam -C -i src louvre

fw stat

Description

Use **fw stat** to view the policy installed on the gateway, and which interfaces are being protected.

Note - The **cpstat** command is an enhanced version of **fw stat**

Syntax

> fw stat -l
> fw stat -s

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-l</td>
<td>Show a long, detailed listing of the installed policies.</td>
</tr>
<tr>
<td>-s</td>
<td>Shows a short summary of the installed policies.</td>
</tr>
</tbody>
</table>
Examples

```bash
> fw stat
HOST    POLICY    DATE
localhost Standard  18Apr2012 15:01:51 : [>eth0] [<eth0]
```

Two interfaces are being protected. The arrows show the direction of the packets.

After the policy is uninstalled, the output becomes:

```bash
> fw stat
HOST    POLICY     DATE
localhost -         -                :   >eth0   <eth0
```

This shows that there is no policy installed, and the interfaces are not protected.

**fw tab**

**Description**  The `fw tab` command shows data from the kernel tables, and lets you change the content of dynamic kernel tables. You cannot change the content of static kernel tables.

Kernel tables (also known as State tables) store data that the Firewall and other modules in the Security Gateway use to inspect packets. These kernel tables are the “memory” of the virtual computer in the kernel and are a critical component of Stateful Inspection. The kernel tables are dynamic hash tables in the kernel memories.

**Syntax**

```
fw tab [-t <table>] [-s] [-c] [-f] [-o <filename>] [-r] [-u | -m <maxval>] [{-a|-x} -e <entry>] [-y] [<hostname>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-t &lt;table&gt;</code></td>
<td>Specifies a table for the command.</td>
</tr>
<tr>
<td><code>-s</code></td>
<td>Shows a short summary of the table(s) data.</td>
</tr>
<tr>
<td><code>-c</code></td>
<td>Shows formatted table information in common format.</td>
</tr>
<tr>
<td><code>-f</code></td>
<td>Shows a formatted version of the table data. Each table can use a different style.</td>
</tr>
<tr>
<td><code>-o &lt;filename&gt;</code></td>
<td>Outputs CL formatted file called <code>&lt;filename&gt;</code>. You can open the file with <code>fw log</code> and other commands or processes that can read FW log formats.</td>
</tr>
<tr>
<td><code>-r</code></td>
<td>Resolves IP addresses in formatted output.</td>
</tr>
<tr>
<td><code>-u</code></td>
<td>Show unlimited table entries.</td>
</tr>
<tr>
<td><code>-m &lt;maxval&gt;</code></td>
<td>Sets the maximum table entries that are shown to <code>&lt;maxval&gt;</code>.</td>
</tr>
</tbody>
</table>
### Security Management Server and Firewall Commands

#### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>-x</td>
</tr>
<tr>
<td>-e <code>&lt;entry&gt;</code></td>
<td>One or more entries that you add or remove from the table.</td>
</tr>
<tr>
<td>-y</td>
<td>Do not show a prompt to users before they run commands.</td>
</tr>
<tr>
<td><code>&lt;hostname&gt;</code></td>
<td>One or more target appliances or servers for the <code>fw tab</code> command. If you do not use this parameter, the default setting is localhost.</td>
</tr>
</tbody>
</table>

**Example**

```
> fw tab -t arp_table -a -e "1,2,3,4,5"
```

Adds an entry: `<00000001,00000002,00000003,00000004,00000005,>` to `arp_table`

```
fw tab - m 100 -r sample-gw
```

**Comments**

If a table has the `expire` attribute, when you use the `-a` parameter to add entries, the default table timeout is added.

This feature only works on local machine kernel tables and does not work on a remote machine’s tables like additional `fw tab` commands.

The `-x` flag can be used independently of the `-e` flag in which case the entire table content is deleted.

This feature should only be used for debug purposes. It is not advisable to arbitrarily change the content of any kernel table since doing so may have unexpected results including unexpected security and connectivity impacts.

### fw ver

**Description**

Display the Security Gateway major and minor version number and build number.

**Syntax**

```
> fw ver [-k][-f <filename>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-k</td>
<td>Print the version name and build number of the Kernel module.</td>
</tr>
<tr>
<td>-f <code>&lt;filename&gt;</code></td>
<td>Print the version name and build number to the specified file.</td>
</tr>
</tbody>
</table>
fwm

**Description**  Perform management operations on the Security Gateway. It controls fwd and all Check Point daemons.

**Syntax**

> fwm

fwm dbimport

**Description**  Imports users into the Check Point User Database from an external file. You can create this file yourself, or use a file generated by fwm dbexport.

**Syntax**

> fwm dbimport [-m] [-s] [-v] [-r] [-k <errors>] [-f <file>] [-d <delim>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-m</td>
<td>If an existing user is encountered in the import file, the user’s default values will be replaced by the values in the template (the default template or the one given in the attribute list for that user in the import file), and the original values will be ignored.</td>
</tr>
<tr>
<td>-s</td>
<td>Suppress the warning messages issued when an existing user’s values are changed by values in the import file.</td>
</tr>
<tr>
<td>-v</td>
<td>verbose mode</td>
</tr>
<tr>
<td>-r</td>
<td>fwm dbimport will delete all existing users in the database.</td>
</tr>
<tr>
<td>-k &lt;errors&gt;</td>
<td>Continue processing until nerror errors are encountered. The line count in the error messages starts from 1 including the attributes line and counting empty or commented out lines.</td>
</tr>
<tr>
<td>-f &lt;file&gt;</td>
<td>The name of the import file. The default import file is $FWDIR/conf/user_def_file.</td>
</tr>
<tr>
<td>-d &lt;delim&gt;</td>
<td>Specifies a delimiter different from the default value (;).</td>
</tr>
</tbody>
</table>

**Comments**  The IKE pre shared secret does not work when exporting from one machine and importing to another.

To ensure that there is no dependency on the previous database values, use the -r flag together with the -m flag.

**File Format**

The import file must conform to the following Usage:

- The first line in the file is an attribute list.
- The attribute list can be any partial set of the following attribute set, as long as name is included:
The attributes must be separated by a delimiter character.

- The default delimiter is the ; character. However, you can use a different character by specifying the -d option in the command line.

- The rest of the file contains lines specifying the values of the attributes per user. The values are separated by the same delimiter character used for the attribute list. An empty value for an attribute means use the default value.

- For attributes that contain a list of values (for example, days), enclose the values in curly braces, that is, {}. Values in a list must be separated by commas. If there is only one value in a list, the braces may be omitted. A + or – character appended to a value list means to add or delete the values in the list from the current default user values. Otherwise the default action is to replace the existing values.

- Legal values for the days attribute are: MON, TUE, WED, THU, FRI, SAT, SUN.

- Legal values for the authentication method are: Undefined, S/Key, SecurID, Unix Password, VPN-1 & FireWall-1 Password, RADIUS, Defender.

- Time format is hh:mm.

- Date format is dd-mmm-yy, where mmm is one of {Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec}.

- If the S/Key authentication method is used, all the other attributes regarding this method must be provided.

- If the Check Point password authentication method is used, a valid Check Point password should be given as well. The password should be encrypted with the C language encrypt function.

- Values regarding authentication methods other than the one specified are ignored.

- The userc field specifies the parameters of the user’s SecuRemote connections, and has three parameters, as follows:
  - key encryption method – DES, CLEAR, Any
  - data encryption method – DES, CLEAR, Any
  - integrity method - MD5,[blank] = no data integrity.

- "Any" means the best method available for the connection. This depends on the encryption methods available to both sides of the connection. For example,

  {DES,CLEAR,} means: key encryption method is DES; no data encryption; no data integrity.

- A line beginning with the ! character is considered a comment.

**fwm expdate**

**Description**  Modify the expiration date of all users and administrators.

**Syntax**

> fw expdate dd-mmm-1976
fwm dbexport

**Description**  
Export the Check Point User Database to a file. The file may be in one of the following formats:

- The same syntax as the import file for fwm dbimport
- LDIF format, which can be imported into an LDAP server using ldapmodify

**Syntax**

To export the User Database to a file that can be used with fwm dbimport:

```
> fwm dbexport [ [-g group | -u user] [-d delim] [-a {attrib1, attrib2, ...} ] [-f file] ]
```

To export the User Database as an LDIF file:

```
> fwm dbexport -l -p [-d] -s subtree [-f file] [-k IKE-shared-secret]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-g group</code></td>
<td>Specifies a group (group) to be exported. The users in the group are not exported.</td>
</tr>
<tr>
<td><code>-u user</code></td>
<td>Specifies that only one user (user) is to be exported.</td>
</tr>
<tr>
<td><code>-d</code></td>
<td>Debug flag</td>
</tr>
<tr>
<td><code>-a {attrib1, attrib2, ...}</code></td>
<td>Specifies the attributes to export, in the form of a comma-separated list, between {} characters, for example, <code>-a {name,days}</code>. If there is only one attribute, the {} may be omitted.</td>
</tr>
<tr>
<td><code>-f file</code></td>
<td>file specifies the name of the output file. The default output file is $FWDIR/conf/user_def_file.</td>
</tr>
<tr>
<td><code>-l</code></td>
<td>Create an LDIF format file for importation by an LDAP server.</td>
</tr>
<tr>
<td><code>-p</code></td>
<td>The profile name.</td>
</tr>
<tr>
<td><code>-s</code></td>
<td>The branch under which the users are to be added.</td>
</tr>
<tr>
<td><code>-k</code></td>
<td>This is the Account Unit’s IKE shared secret (IKE Key in the Encryption tab of the Account Unit Properties window.)</td>
</tr>
</tbody>
</table>

**Comments**  
Note:

- The IKE pre shared secret does not work when exporting from one machine and importing to another.
- If you use the `-a` parameter to specify a list of attributes, and then import the created file using fwm dbimport, the attributes not exported will be deleted from the user database.
fwm dbexport and fwm dbimport (non-LDIF Usage) cannot export and import user groups. To export and import a user database, including groups, proceed as follows:

* Run `fwm dbexport` on the source Security Management server.

* On the destination Security Management server, create the groups manually.

* Run `fwm dbimport` on the destination Security Management server.

The users will be added to the groups to which they belonged on the source Security Management server.

If you wish to import different groups of users into different branches, run `fwm dbexport` once for each subtree, for example:

```
fwm dbexport -f f1 -l -s ou=marketing,o=WidgetCorp,c=us
fwm dbexport -f f2 -l -s ou=rnd,o=WidgetCorp,c=uk
```

Next, import the individual files into the LDAP server one after the other. For information on how to do this, refer to the documentation for your LDAP server.

The LDIF file is a text file which you may wish to edit before importing it into an LDAP server. For example, in the Check Point user database, user names may be what are in effect login names (such as “maryj”) while in the LDAP server, the DN should be the user’s full name (“Mary Jones”) and “maryj” should be the login name.

**Example**

Suppose the User Database contains two users, “maryj” and “ben”.

```
fwm dbexport -l -s o=WidgetCorp,c=us
```

creates a LDIF file consisting of two entries with the following DNs:

```
cn=ben,o=WidgetCorp,c=us
cn=maryj,o=WidgetCorp,c=us
```

### fwm dbload

**Description**  Download the user database and network objects information to selected targets. If no target is specified, then the database is downloaded to localhost.

**Syntax**

```
gw> fwm dbload [-a|-c <conffile>] [<targets>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a &lt;conffile&gt;</td>
<td>Execute command on all targets specified in the default system configuration file ($FWDIR/conf/sys.conf). This file must be manually created.</td>
</tr>
<tr>
<td>-c &lt;conffile&gt;</td>
<td>Only OPSEC control connections in the file are enabled.</td>
</tr>
<tr>
<td>&lt;targets&gt;</td>
<td>Execute command on the designated targets.</td>
</tr>
</tbody>
</table>

### fwm ikecrypt

**Description**  `fwm ikecrypt` command line encrypts the password of a SecuRemote user using IKE. The resulting string must then be stored in the LDAP database.
Syntax

> fwm ikecrypt <shared-secret> <user-password>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;shared-secret&gt;</td>
<td>The IKE Key defined in the Encryption tab of the LDAP Account Unit Properties window.</td>
</tr>
<tr>
<td>&lt;user-password&gt;</td>
<td>The SecuRemote user’s password.</td>
</tr>
</tbody>
</table>

Comments  An internal CA must be created before implementing IKE encryption. An Internal CA is created during the initial configuration of the Security Management server, following installation.

fwm getpcap

Description  fwm getpcap command line fetches the packet capture.

Syntax  

> fwm getpcap -g <gw> -u <cap id> [-p <path>] [-c <domain>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-g &lt;gw&gt;</td>
<td>Host name of the gateway</td>
</tr>
<tr>
<td>-u &lt;cap id&gt;</td>
<td>Capture UID</td>
</tr>
<tr>
<td>-p &lt;path&gt;</td>
<td>Output path name</td>
</tr>
<tr>
<td>-c &lt;domain&gt;</td>
<td>Host name of the Domain Management Server</td>
</tr>
</tbody>
</table>

Note  This command only works with IPS packet captures stored on the Gateway in $FWDIR//opt/CPsuite-R77/fw1/log/captures_repository. It does not work with other blades such as Anti-Bot and Anti-Virus that store packet captures in $FWDIR/log/blob.

fwm load

Description  Compile and install a Security Policy or a specific version of the Security Policy on the target’s Security Gateways. This is done in one of two ways:

- fwm load compiles and installs an Inspection Script (*.pf) file on the designated Security Gateways.
- fwm load converts a Rule Base (*.W) file created by the GUI into an Inspection Script (*.pf) file then installs it to the designated Security Gateways.

Versions of the Security Policy and databases are maintained in a version repository on the Security Management server. Using this command, specific versions of the Security Policy can be installed on a gateway (local or remote) without changing the definition of the current active database version on the Security Management server.

To protect a target, you must load a Policy that contains rules whose scope matches the target. If none of the rules are enforced on the target, then all traffic through the target is blocked.

Syntax  

> fwm load [-p <plug-in>] [-S] <rulebase> <targets>
### fwm load

**Description**
View and unlock locked administrators.

**Syntax**
```
fwm load Standard johnny
```

### Example
The following command installs the Security Policy `standard` in the target gateway `johnny`.

```
fwm load Standard johnny
```

### fwm lock_admin

**Description**
View and unlock locked administrators.

**Syntax**
```
fwm lock_admin [-v] [-u <administrator>] [-ua]
```

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-v</td>
<td>View the names of all locked administrators.</td>
</tr>
<tr>
<td>-u &lt;administrator&gt;</td>
<td>Unlock a single administrator.</td>
</tr>
<tr>
<td>-ua</td>
<td>Unlock all locked administrators.</td>
</tr>
</tbody>
</table>

### fwm logexport

**Description**
fwm logexport exports the Log file to an ASCII file.

**Syntax**
```
```

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d &lt;delimiter&gt;</td>
<td>Set the output delimiter. The default is a semicolon (;).</td>
</tr>
<tr>
<td>-i &lt;filename&gt;</td>
<td>The name of the input Log file. The default is the active Log file,fw.log</td>
</tr>
<tr>
<td>-o &lt;outputfile&gt;</td>
<td>The name of the output file. The default is printing to the screen.</td>
</tr>
<tr>
<td>-n</td>
<td>Do not perform DNS resolution of the IP addresses in the Log file (this option significantly speeds the processing).</td>
</tr>
<tr>
<td>-p</td>
<td>Do not perform service resolution. A service port number is displayed.</td>
</tr>
<tr>
<td>-f</td>
<td>If this is the active Log file (fw.log), wait for new records and export them to the ASCII output file as they occur.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| -m        | This flag specifies the unification mode.  
  - initial - the default mode. Complete the unification of log records; that is, output one unified record for each id.  
  - semi - step-by-step unification, that is, for each log record, output a record that unifies this record with all previously-encountered records with the same id.  
  - raw - output all records, with no unification. |
| -a        | Show account records only (the default is to show all records). |

### Comments

**Controlling the Output of fwm logexport using logexport.ini**

The output of `fwm logexport` can be controlled by creating a file called `logexport.ini` and placing it in the `conf` directory: `$FWDIR/conf`. The `logexport.ini` file should be in the following format:

```
[Fields_Info]
included_fields = field1,field2,field3,<REST_OF_FIELDS>,field100
excluded_fields = field10,field11
```

**note that:**

- the `num` field will always appear first, and cannot be manipulated using `logexport.ini`
- `<REST_OF_FIELDS>` is a reserved token that refers to a list of fields. It is optional. If `-f` option is set, `<REST_OF_FIELDS>` is based on a list of fields taken from the file `logexport_default.C`.
- If `-f` is not set, `<REST_OF_FIELDS>` will be based on the given input log file.
- It is not mandatory to specify both `included_fields` and `excluded_fields`.

**Format:**

The `fwm logexport` output appears in tabular format. The first row lists the names of all fields included in the subsequent records. Each of the subsequent rows consists of a single log record, whose fields are sorted in the same order as the first row. If a record has no information on a specific field, this field remains empty (as indicated by two successive semi-colons).

**Example**

```
num;date;time;orig;type;action;alert;i/f_name;i/f_dir;product;sys_message;service;s_port;src;dst;  
0; 5Dec2002;9:08:44;jam.checkpoint.com;control; ;;daemon;inbound;VPN-1 & FireWall-1;The hme0 interface is not protected by the anti-spoofing feature. Your network may be at risk;;;;  
1; 5Dec2002;9:08:44;jam.checkpoint.com;control; ;;daemon;inbound;VPN-1 & FireWall-1;;  
ftp;23456;1.2.3.4;3.4.5.6;
```
**fwm sic_reset**

**Description**  Reset the Internal CA and delete all the certificates from the Internal CA and the Internal CA itself. After running `sic_reset`, the ICA should be initialized through the `cpconfig` command. If this command is run all the certified IKE from the Internal CA should be removed (using the SmartConsole).

**Syntax**  

```
> fwm sic_reset
```

**fwm unload <targets>**

**Description**  Uninstall the currently loaded Inspection Code from selected targets.

**Syntax**  

```
> fwm unload <targets> [-all|-c <conffile>]
```

**Parameter**  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;targets&gt;</td>
<td>Execute command on the designated targets.</td>
</tr>
<tr>
<td>-all</td>
<td>Execute command on all targets specified in the default system configuration file ($FWDIR/conf/sys.conf). This file must be manually created.</td>
</tr>
<tr>
<td>-c conffile</td>
<td>Execute command on targets specified in the conffile.</td>
</tr>
</tbody>
</table>

**fwm ver**

**Description**  `fwm ver` shows the build number.

**Syntax**  

```
> fwm ver [-f <filename>]
```

**Parameter**  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f &lt;filename&gt;</td>
<td>Exports the build number data to a file</td>
</tr>
</tbody>
</table>

**fwm verify**

**Description**  The `fwm verify` command verifies the specified policy package without installing it.

**Syntax**  

```
> fwm verify <policy>
```

**Parameter**  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;policy&gt;</td>
<td>The name of an available policy package.</td>
</tr>
</tbody>
</table>
VPN Commands

**In This Section:**

- Overview ...................................................................................................................... 254
- vpn crl_zap .................................................................................................................. 254
- vpn crlview .................................................................................................................. 254
- vpn debug .................................................................................................................... 255
- vpn drv ......................................................................................................................... 256
- vpn export_p12 ............................................................................................................ 256
- vpn macutil .................................................................................................................. 257
- vpn nssm_toplogy ....................................................................................................... 257
- vpn overlap_encdom .................................................................................................. 258
- vpn sw_toplogy .......................................................................................................... 259
- vpn tu ........................................................................................................................... 259
- vpn ver ......................................................................................................................... 260

**Overview**

**Description**  
VPN commands generate status information regarding VPN processes, or are used to stop and start specific VPN services. All VPN commands are executed on the Security Gateway. The `vpn` command sends to the standard output a list of available commands.

**Usage**  
`vpn`

**Comments**  
Sends to the standard output a list of available commands.

**vpn crl_zap**

**Description**  
Erase all Certificate Revocation Lists (CRLs) from the cache.

**Syntax**

```
> vpn crl_zap
```

**Return Value**  
0 for success; any other value equals failure.

**vpn crlview**

**Description**  
Retrieve the Certificate Revocation List (CRL) from various distribution points and displays it for the user. The command comes in three flavors:

- `vpn crlview -obj <MyCA> -cert <MyCert>`. The VPN daemon contacts the Certificate Authority called **MyCA** and locates the certificate called **MyCert**. The VPN daemon extracts the certificate distribution point from the certificate then goes to the distribution point, which might be an LDAP or HTTP server. From the distribution point, the VPN daemon retrieves the CRL and displays it to the standard output.
• **vpn crlview -f d:\temp\MyCert.** The VPN daemon extracts the certificate distribution point from the certificate, goes to the distribution point, retrieves the CRL, and displays the CRL to the standard output.

• **vpn crlview -view <lastest_CRL>.** If the CRL has already been retrieved, this command instructs the VPN daemon to display the contents to the standard output.

**Syntax**

`> vpn crlview -obj <object name> -cert <certificate name>`

`> vpn crlview -f <filename>`

`> vpn crlview -view`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| -obj -cert | • -obj refers to the name of the CA network object  
• -cert refers to the name of the certificate |
| -f | Refers to the filename of the certificate |
| -view | Views the CRL |
| -d | Debug option |

**Return Value** 0 for success; any other value equals failure.

**vpn debug**

**Description**  
Instruct the VPN daemon to write debug messages to the VPN log file: in $FWDIR/log/vpnd.elg. Debugging of the VPN daemon takes place according to topics and levels. A topic is a specific area on which to perform debugging, for example if the topic is LDAP, all traffic between the VPN daemon and the LDAP server are written to the log file. Levels range from 1-5, where 5 means “write all debug messages”.

This command makes use of TdError, a Check Point infrastructure for reporting messages and debug information. There is no legal list of topics. It depends on the application or module being debugged.

To debug all available topics, use: ALL for the debug topic.

IKE traffic can also be logged. IKE traffic is logged to $FWDIR/log/IKE.elg

**Syntax**

`> vpn debug < on [ DEBUG_TOPIC=level ] | off | ikeon | ikeoff | trunc | timeon <SECONDS>]|timeoff`

`> vpn debug on DEBUG_TOPIC=level |off timeon<SECONDS>]|timeoff`

`> vpn debug ikeon | ikeoff timeon|timeoff`

`> vpn debug trunc`
### VPN Commands

#### Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Turns on high level VPN debugging.</td>
</tr>
<tr>
<td>on topic=level</td>
<td>Turns on the specified debug topic on the specified level. Log messages</td>
</tr>
<tr>
<td></td>
<td>associated with this topic at the specified level (or higher) are sent to</td>
</tr>
<tr>
<td></td>
<td>$FWDIR/log/vpnd.elg</td>
</tr>
<tr>
<td>off</td>
<td>Turns off all VPN debugging.</td>
</tr>
<tr>
<td>timeon/timeoff</td>
<td>Number of seconds to run the debug command</td>
</tr>
<tr>
<td>ikeon</td>
<td>Turns on IKE packet logging to: $FWDIR/log/IKE.elg</td>
</tr>
<tr>
<td>ikeoff</td>
<td>Turns of IKE logging</td>
</tr>
<tr>
<td>trunc</td>
<td>Truncates the $FWDIR/log/IKE.elg file, switches the cyclic vpnd.elg</td>
</tr>
<tr>
<td></td>
<td>(changes the current vpnd.elg file to vpnd0.elg and creates a new</td>
</tr>
<tr>
<td></td>
<td>vpnd.elg), enables VPND and IKE debugging and adds a timestamp to the vpnd.</td>
</tr>
<tr>
<td></td>
<td>elg file.</td>
</tr>
</tbody>
</table>

**Return Value** 0= success, failure is some other value, typically -1 or 1.

**Example**

```plaintext
vpn debug on all=5 timeon 5
```

This writes all debugging information for all topics to the vpnd.elg file for five seconds.

**Comments** IKE logs are analyzed using the support utility IKEView.exe.

#### vpn drv

**Description** Install the VPN kernel (vpnk) and connects to the firewall kernel (fwk), attaching the VPN driver to the Firewall driver.

**Syntax**

```plaintext
> vpn drv on|off
> vpn drv stat
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on/off</td>
<td>Starts/stops the VPN kernel</td>
</tr>
<tr>
<td>stat</td>
<td>Returns the status of the VPN kernel, whether the</td>
</tr>
<tr>
<td></td>
<td>kernel is on or off</td>
</tr>
</tbody>
</table>

#### vpn export_p12

**Description** Export information contained in the network objects database and writes it in the PKCS#12 format to a file with the p12 extension.
### VPN Commands

#### Syntax

```bash
> vpn export_p12 -obj <network object> -cert <certificate object> -file <filename> -passwd <password>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-obj</td>
<td>Name of the gateway network object</td>
</tr>
<tr>
<td>-cert</td>
<td>Name of the certificate</td>
</tr>
<tr>
<td>-file</td>
<td>What the file with the p12 should be called</td>
</tr>
<tr>
<td>-passwd</td>
<td>Password required to open the encrypted p12 file</td>
</tr>
</tbody>
</table>

**Return Value** 0 for success; any other value equals failure.

**Example**

```bash
vpn export_p12 -obj Gateway1 -cert MyCert -file mycert.p12 -passwd kdd432
```

#### vpn macutil

This command is related to Remote Access VPN, specifically Office mode, generating a MAC address per remote user. This command is relevant only when allocating IP addresses via DHCP.

Remote access users in Office mode receive an IP address which is mapped to a hardware or MAC address. This command displays a generated hardware or MAC address for each name you enter.

**Syntax**

```bash
> vpn macutil <username>
```

**Example**

```bash
vpn macutil John
```

**Output**

```
20-0C-EB-26-80-7D, "John"
```

#### vpn nssm_toplogy

**Description** Generate and upload a topology (in NSSM format) to NSSM server for use by clients.

**Syntax**

```bash
> vpn nssm_toplogy -url <"url"> -dn <"dn"> -name <"name"> -pass <"password"> [-action <bypass|drop>][-print_xml]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-url</td>
<td>URL of the NSSM server</td>
</tr>
<tr>
<td>-dn</td>
<td>Distinguished name of the NSSM server needed to establish an SSL connection</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-name</td>
<td>Valid Login name for NSSM server</td>
</tr>
<tr>
<td>-pass</td>
<td>Valid password for NSSM server</td>
</tr>
<tr>
<td>-action</td>
<td>Specifies the action the Symbian client should take if the packet is not destined for an IP address in the VPN domain. Legal options are <strong>Bypass</strong> (default) or <strong>Drop</strong></td>
</tr>
<tr>
<td>-print_xml</td>
<td>The topology is in XML format. This flag writes that topology to a file in XML format.</td>
</tr>
</tbody>
</table>

### vpn overlap_encdom

**Description**  Display all overlapping VPN domains. Some IP addresses might belong to two or more VPN domains. The command alerts for overlapping encryption domains if one or both of the following conditions exist:

- The same VPN domain is defined for both gateway
- If the gateway has multiple interfaces, and one or more of the interfaces has the same IP address and netmask.

If the gateway has multiple interfaces, and one or more of the interfaces have the same IP address and netmask

**Syntax**

```
> vpn overlap_encdom [communities | traditional]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communities</td>
<td>With this flag, all pairs of objects with overlapping VPN domains are displayed -- but only if the objects (that represent VPN sites) are included in the same VPN community. This flag is also used if the same destination IP can be reached via more than one community.</td>
</tr>
<tr>
<td>Traditional</td>
<td>Default flag. All pairs of objects with overlapping VPN domains are displayed.</td>
</tr>
</tbody>
</table>

**Example**  `vpn overlap_encdom communities`
Output

c:\> vpn overlap_encdom communitie
The objects Paris and London have overlapping encryption domains.
The overlapping domain is:
10.8.8.1 - 10.8.8.1
10.10.8.0 - 10.10.9.255
- This overlapping encryption domain generates a multiple entry points configuration in MyIntranet and RemoteAccess communities.
- Same destination address can be reached in more than one community (Meshed, Star). This configuration is not supported.

The objects Paris and Chicago have overlapping encryption domains. The overlapping domain is:
10.8.8.1 - 10.8.8.1
- Same destination address can be reached in more than one community (MyIntranet, NewStar). This configuration is not supported.

The objects Washington and Tokyo have overlapping encryption domains.
The overlapping domain is:
10.12.10.68 - 10.12.10.68
- This overlapping encryption domain generates a multiple entry points configuration in Meshed, Star and NewStar communities.

**vpn sw_topology**

**Description**  
Download the topology for a Safe@ or Edge gateway.

**Syntax**

```
> vpn [-d] sw_toplogy -dir <directory> -name <name> -profile <profile> [-filename <filename>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Debug flag</td>
</tr>
<tr>
<td>-dir</td>
<td>Output directory for file</td>
</tr>
<tr>
<td>-name</td>
<td>Nickname of site which appears in remote client</td>
</tr>
<tr>
<td>-profile</td>
<td>Name of the Safe@ or Edge profile for which the topology is created</td>
</tr>
<tr>
<td>-filename</td>
<td>Name of the output file</td>
</tr>
</tbody>
</table>

**vpn tu**

**Description**  
Launch the TunnelUtil tool which is used to control VPN tunnels.

**Syntax**

```
> vpn tu
> vpn tunnelutil
```
Example: `vpn tu`

Output:

```
********** Select Option **********
(1)             List all IKE SAs
(2)             List all IPsec SAs
(3)             List all IKE SAs for a given peer (GW) or user (Client)
(4)             List all IPsec SAs for a given peer (GW) or user (Client)
(5)             Delete all IPsec SAs for a given peer (GW)
(6)             Delete all IPsec SAs for a given User (Client)
(7)             Delete all IPsec+IKE SAs for a given peer (GW)
(8)             Delete all IPsec+IKE SAs for a given User (Client)
(9)             Delete all IPsec SAs for ALL peers and users
(0)             Delete all IPsec+IKE SAs for ALL peers and users
(Q)             Quit
```

Further Info. When viewing Security Associations for a specific peer, the IP address must be given in dotted decimal notation.

### `vpn ver`

**Description**: Display the VPN major version number and build number.

**Syntax**

```
> vpn ver [-k] -f <filename>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ver</code></td>
<td>Displays the version name and version build number</td>
</tr>
<tr>
<td><code>-k</code></td>
<td>Displays the version name and build number and the kernel build number</td>
</tr>
<tr>
<td><code>-f</code></td>
<td>Prints the version number and build number to a text file.</td>
</tr>
</tbody>
</table>
Overview

**Description** The `rtm` command and all its derivatives are used to execute SmartView Monitor operations.

### rtm debug

**Description** Send debug printouts to the $FWDIR/log/rtmd.elg file.

**Usage**

```
rtm debug <on | off> [OPSEC_DEBUG_LEVEL | TDERROR_<AppName>_<Topic>=<ErrLevel>]
```

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Start debug mode</td>
</tr>
<tr>
<td>off</td>
<td>Stop debug mode</td>
</tr>
<tr>
<td>OPSEC_DEBUG_LEVEL</td>
<td>Turn on OPSEC debug printouts</td>
</tr>
<tr>
<td>TDERROR_RTM_ALL</td>
<td>Turn on SmartView Monitor debug printouts</td>
</tr>
</tbody>
</table>

### rtm drv

**Description** Start, stop or check the status of the SmartView Monitor kernel driver.

**Usage**

```
rtm drv <on | off | stat>
```
### SmartView Monitor Commands

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Start the SmartView Monitor kernel driver</td>
</tr>
<tr>
<td>off</td>
<td>Stop the SmartView Monitor kernel driver</td>
</tr>
<tr>
<td>stat</td>
<td>SmartView Monitor kernel driver status</td>
</tr>
</tbody>
</table>

### rtm monitor

**Description**

Starts the monitoring process for an interface or a virtual link.

If options and grouping are not used, this command monitors all traffic, on all interfaces, in both directions.

**Syntax**

```plaintext
rtm monitor {<module_name> [<interface_name>] | <module_name>-filter ["<complex filter>"] | -v <virtual_link_name> [ <options> ] [-g <grouping> <entity-1>...<entity-n>] }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>module-name</td>
<td>The name of the SmartView Monitor module.</td>
</tr>
<tr>
<td>interface-name</td>
<td>The name of the monitored interface.</td>
</tr>
<tr>
<td>&quot;&lt;complex filter&gt;&quot;</td>
<td>Boolean regular expression to match traffic to be monitored.</td>
</tr>
<tr>
<td>virtual_link_name</td>
<td>The name of the monitored Virtual Link.</td>
</tr>
<tr>
<td>grouping</td>
<td>svc</td>
</tr>
<tr>
<td>svc</td>
<td>Monitors according to a service.</td>
</tr>
<tr>
<td>src</td>
<td>Monitors according to a network object (source only).</td>
</tr>
<tr>
<td>dst</td>
<td>Monitors according to a network object (destination only).</td>
</tr>
<tr>
<td>ip</td>
<td>Monitors according to a network object (source and destination).</td>
</tr>
<tr>
<td>fgrule</td>
<td>Monitors according to a QoS Policy rule.</td>
</tr>
<tr>
<td>topsvc</td>
<td>Monitors the traffic of the top 50 services.</td>
</tr>
<tr>
<td>topsrc</td>
<td>Monitors the traffic of the top 50 sources.</td>
</tr>
</tbody>
</table>
### SmartView Monitor Commands

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>topdst</code></td>
<td>Monitors the traffic of the top 50 destinations.</td>
</tr>
<tr>
<td><code>topdst</code></td>
<td>Monitors traffic to and from the top 50 IP addresses (source of destination).</td>
</tr>
<tr>
<td><code>topfwn</code></td>
<td>Monitors according to the top 50 Firewall rules.</td>
</tr>
<tr>
<td><code>topfgrule</code></td>
<td>Monitors according to the top 50 QoS Policy rules.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-a</code></td>
<td><code>aggregate</code> (default) - Shows connections as a group.</td>
</tr>
<tr>
<td></td>
<td><code>individual</code> - Shows individual connections.</td>
</tr>
<tr>
<td><code>-w</code></td>
<td><code>bandwidth</code> (default) - Shows effective bandwidth.</td>
</tr>
<tr>
<td></td>
<td><code>loss</code> - Shows the difference between the transmission rate and the receiving rate.</td>
</tr>
<tr>
<td></td>
<td><code>rtt</code> - Shows the time required to travel between two endpoints.</td>
</tr>
<tr>
<td><code>-t</code></td>
<td><code>wire</code> - Shows the data on the wire after compression or encryption.</td>
</tr>
<tr>
<td></td>
<td><code>application</code> - Shows the data as the application sees it (not compressed and not encrypted).</td>
</tr>
<tr>
<td><code>-i</code></td>
<td><code>&lt;number of seconds&gt;</code></td>
</tr>
<tr>
<td></td>
<td>Default: 2</td>
</tr>
<tr>
<td><code>@@</code></td>
<td>Specifies a sub-rule (for example, <code>rule@@subrule</code>)</td>
</tr>
<tr>
<td><code>-d</code></td>
<td>Specifies the monitor direction.</td>
</tr>
<tr>
<td></td>
<td>Valid values for an interface:</td>
</tr>
<tr>
<td></td>
<td>- <code>inbound</code></td>
</tr>
<tr>
<td></td>
<td>- <code>outbound</code></td>
</tr>
<tr>
<td></td>
<td>- <code>eitherbound</code></td>
</tr>
<tr>
<td></td>
<td>Valid values for a virtual link:</td>
</tr>
<tr>
<td></td>
<td>- <code>a2b</code> - endpoint A to endpoint B</td>
</tr>
<tr>
<td></td>
<td>- <code>b2a</code> - endpoint B to endpoint A</td>
</tr>
<tr>
<td></td>
<td>- <code>a2b_b2a</code> - both directions</td>
</tr>
<tr>
<td><code>-y</code></td>
<td>Specifies the units of bandwidth (when <code>-w = bandwidth</code>)</td>
</tr>
<tr>
<td></td>
<td>- <code>bytes</code> [default]</td>
</tr>
<tr>
<td></td>
<td>- <code>pkts</code></td>
</tr>
<tr>
<td></td>
<td>- <code>line</code></td>
</tr>
<tr>
<td><code>c</code></td>
<td>Indicates the number of new connections opened per second.</td>
</tr>
</tbody>
</table>
### SmartView Monitor Commands

#### Options

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Average concurrent connections (use with a grouping value).</td>
</tr>
<tr>
<td>-p</td>
<td>Specifies whether or not thousands will be separated by commas.</td>
</tr>
</tbody>
</table>

#### Examples

This command shows monitoring data in bytes-per-second for the top 50 services passed on all interfaces in both directions:

```
rtm monitor localhost -filter -g topsvc
```

This command shows monitoring data in concurrent connections for the top 50 sources inbound to interface eth0:

```
rtm monitor localhost -filter "[and[[interface 0 [eth0in]]][svc 1 [telnet http]]]" -y C -g topsrc
```

This command shows monitoring data in bytes-per-sec for the top 50 services passed on interface hme1:

```
rtm monitor localhost hme1 -g topsvc -y b
```

#### Comments

The specified entities correspond to the specified grouping option. For example, if the monitoring process works according to a service [svc], add all the monitored services, separated by a space.

To monitor for the QoS Policy, use `rule@fgrule`

---

**rtm rtmd**

**Description**  
Start the SmartView Monitor daemon manually. This also occurs manually when `rtmstart` is run.

**Usage** `rtm rtmd`

---

**rtm stat**

**Description**  
Display the general SmartView Monitor status. In addition, it displays the status of the daemon, driver, opened views and active virtual links.

**Usage** `rtm stat [flavor(s)] [-h] [-v[v][v]]`

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>Help</td>
</tr>
<tr>
<td>-v</td>
<td>Verbose</td>
</tr>
<tr>
<td>vl</td>
<td>Current virtual links</td>
</tr>
<tr>
<td>view</td>
<td>Current views</td>
</tr>
</tbody>
</table>
rtm ver

**Description**  Display the SmartView Monitor version.

**Usage**  `rtm ver [-k]`

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-k</td>
<td>Displays the SmartView Monitor kernel version.</td>
</tr>
</tbody>
</table>

rtmstart

**Description**  Load the SmartView Monitor kernel module and starts the SmartView Monitor daemon.

**Usage**  `rtmstart`

rtmstop

**Description**  Kill the SmartView Monitor daemon and unloads the SmartView Monitor kernel module.

**Usage**  `rtmstop`
ClusterXL Commands

In This Section:

- cphaconf ......................................................................................................................266
- cphaprob .....................................................................................................................267
- cphastart .....................................................................................................................267
- cphastop ......................................................................................................................268

cphaconf

Description  The cphaconf command configures ClusterXL.

⚠️ Important - Running this command is not recommended. It should be run automatically, only by the Security Gateway or by Check Point support. The only exception to this rule is running this command with set_cpp option, as described below.

Usage

cphaconf [-i <computer id>] [-p <policy id>] [-b <db id>] [-n <ClusterXL num>] [-c <ClusterXL size>] [-m <service>] [-t <secured IF 1>...] start

cphaconf [-t <secured IF 1>...] [-d <disconnected IF 1>...] add

cphaconf clear-secured
cphaconf clear-disconnected
cphaconf stop
cphaconf init
cphaconf forward <on/off>
cphaconf debug <on/off>
cphaconf set_ccp <broadcast/multicast>
cphaconf mc_reload
cphaconf debug_data
cphaconf stop_all_vs

Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| set_ccp <broadcast/multicast> | Sets whether ClusterXL Control Protocol (CCP) packets should be sent with a broadcast or multicast destination MAC address. The default behavior is multicast. The setting created using this command will survive reboot.  
**Note:** The same value (either broadcast or multicast) should be set on all ClusterXL members. |
| stop_all_vs                | Stops the ClusterXL product on all Virtual Systems on a VSX Gateway.                                                                           |
**cphaprob**

**Description**  The `cphaprob` command verifies that the cluster and the cluster members are working properly.

**Usage**

```
cphaprob -d <device> -t <timeout(sec)> -s <ok|init|problem> [-p] register
cphaprob -f <file> register
```

- `cphaprob -d <device> [-p] unregister`
- `cphaprob -d <device> -s <ok|init|problem> report`
- `cphaprob [-i[a]] [-e] list`
- `cphaprob state`
- `cphaprob [-a] if`

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`cphaprob -d &lt;device&gt; -t &lt;timeout(sec)&gt; -s &lt;ok</td>
<td>init</td>
</tr>
<tr>
<td><code>cphaprob -f &lt;file&gt; register</code></td>
<td>Register all the user defined critical devices listed in <code>&lt;file&gt;</code>.</td>
</tr>
<tr>
<td><code>cphaprob -d &lt;device&gt; [-p] unregister</code></td>
<td>Unregister a user defined <code>&lt;device&gt;</code> as a critical process. This means that this device is no longer considered critical.</td>
</tr>
<tr>
<td><code>cphaprob -a unregister</code></td>
<td>Unregister all the user defined <code>&lt;device&gt;</code>.</td>
</tr>
<tr>
<td>`cphaprob -d &lt;device&gt; -s &lt;ok</td>
<td>init</td>
</tr>
<tr>
<td><code>cphaprob [-i[a]] [-e] list</code></td>
<td>View the list of critical devices on a cluster member, and of all the other machines in the cluster.</td>
</tr>
<tr>
<td><code>cphaprob state</code></td>
<td>View the status of a cluster member, and of all the other members of the cluster.</td>
</tr>
<tr>
<td><code>cphaprob [-a] if</code></td>
<td>View the state of the cluster member interfaces and the virtual cluster interfaces.</td>
</tr>
</tbody>
</table>

**cphastart**

**Description**  Running `cphastart` on a cluster member activates ClusterXL on the member. It does not initiate full synchronization. `cpstart` is the recommended way to start a cluster member.
**cphastop**

**Description**  Running *cphastop* on a cluster member stops the cluster member from passing traffic. State synchronization also stops. It is still possible to open connections directly to the cluster member. In High Availability Legacy mode, running *cphastop* may cause the entire cluster to stop functioning.
CoreXL and Multi-queue Commands

For CoreXL and Multi-queue commands, see the *R77 Performance Tuning Administration Guide* http://supportcontent.checkpoint.com/documentation_download?ID=24808.
Index

3
32 and 64-bit Gaia Editions • 25

A
Advanced Routing • 121
Advanced VRRP • 164
Aliases • 40
ARP • 59
Authentication Servers • 140

B
Backing Up and Restoring the System - CLI (Backup) • 188
Backing Up and Restoring the System - WebUI • 187
Bond Interfaces (Link Aggregation) • 43
Booting from the Emergendisk Removable Device • 193
Bridge Interfaces • 48
Bridging group commands • 49

C
Change My Password • 122
Change My Password - CLI (selfpasswd) • 122
Change My Password - WebUI • 122
Changing System Edition • 19
CLI Configuration Procedures for VPN Tunnel Interfaces • 54
CLI Procedures • 43, 74, 130
CLI Procedures - CPUSE • 205
CLI Procedures - IPv6 Static Routes • 77
CLI Reference (interface) • 57
Client Environment Output Format • 27
Cloning Groups • 88
ClusterXL Commands • 266
Command Completion • 22
Command History • 22
Command Line Movement and Editing • 24
Command Reuse • 23
Commands and Features • 20
Completing the VTI Configuration • 56
config_system • 32
Configuration Tab • 15
Configuration Using the CLI • 42
Configuration using the WebUI • 40
Configuring a CPUSE Policy - clish • 204
Configuring a CPUSE Policy - WebUI • 198
Configuring a DHCP Server - CLI (dhcp) • 64
Configuring a DHCP Server - WebUI • 62
Configuring Advanced VRRP - CLI (vrrp) • 166
Configuring Advanced VRRP - WebUI • 165
Configuring Aliases - CLI (interface) • 41
Configuring Allowed Gaia Clients - CLI (allowed-client) • 120
Configuring Allowed Gaia Clients - WebUI • 120
Configuring ARP - CLI (arp) • 60
Configuring ARP - WebUI • 59
Configuring Bond Interfaces - CLI • 44
Configuring Bond Interfaces - WebUI • 44
Configuring Bridge Interfaces - WebUI • 49
Configuring Bridge Mode with the CLI • 49
Configuring Cloning Groups - CLI (Cloning Groups) • 90
Configuring Cloning Groups - WebUI • 89
Configuring Core Dumps - WebUI • 113
Configuring Core Dumps - CLI (core-dump) • 113
Configuring CPUSE - WebUI • 196
Configuring CPUSE Mail Notifications - clish • 205
Configuring CPUSE Mail Notifications - WebUI • 199
Configuring DNS - CLI (dns) • 69
Configuring DNS - WebUI • 68
Configuring Gaia as a RADIUS Client • 144
Configuring Gaia as a TACACS+ Client • 148
Configuring Gaia for the First Time • 31
Configuring Global Settings for VRRP • 159
Configuring Host Name - CLI (hostname) • 66
Configuring Host Name - WebUI • 66
Configuring Hosts - CLI (host) • 67
Configuring Hosts - WebUI • 67
Configuring IPv4 Static Routes - WebUI • 71
Configuring IPv6 Static Routes - CLI (ipv6 static-route) • 76
Configuring IPv6 Static Routes - WebUI • 75
Configuring IPv6 Support - CLI • 114
Configuring IPv6 Support - WebUI • 114
Configuring Job Scheduler - CLI (crontab) • 108
Configuring Job Scheduler - WebUI • 107
Configuring Licenses - CLI (lplic) • 172
Configuring Licenses - WebUI • 171
Configuring Log Volume - CLI (volume) • 116
Configuring Loopback Interfaces - CLI (interface) • 51
Configuring Loopback Interfaces - WebUI • 50
Configuring Mail Notification - CLI (mail-notification) • 110
Configuring Mail Notification - WebUI • 110
Configuring Many Static Routes at Once • 71
Configuring Messages - CLI (message) • 111
Configuring Messages - WebUI • 111
Configuring Netflow Export - CLI (netflow) • 80
Configuring Netflow Export - WebUI • 79
Configuring Network Switches • 158
Configuring NTP - CLI (ntp) • 85
Configuring Password Policy - CLI (password-controls) • 135
Configuring Password Policy - WebUI • 132
Configuring Performance Optimization - CLI (cpconfig) • 83
Configuring Performance Optimization - WebUI • 82
Configuring Physical Interfaces - CLI (interface) • 39
Configuring Physical Interfaces - WebUI • 38
Configuring RADIUS Servers - CLI (aaa) • 142
Configuring RADIUS Servers - WebUI • 141
Configuring RADIUS Servers for Non-Local Gaia Users • 144
Configuring Roles - CLI (rba) • 129
Configuring Roles - WebUI • 128
Configuring Scheduled Backups - CLI (backup-scheduled) • 190
Configuring Scheduled Backups - WebUI • 189
Configuring Simplified/Monitored Circuit VRRP - CLI (mcvr) • 161
Configuring Simplified/Monitored Circuit VRRP - WebUI • 160
Configuring Snapshot Management - CLI (snapshot) • 182
Configuring Snapshot Management - WebUI • 181
Configuring SNMP - CLI (snmp) • 101
Configuring SNMP - WebUI • 98
Configuring Static Routes - CLI (static-route) • 72
Configuring System Groups - CLI (group) • 151
Configuring System Groups - WebUI • 150
Configuring System Logging - CLI (syslog) • 116
Configuring System Logging - WebUI • 115
Configuring TACACS+ Servers - CLI (aaa) • 146
Configuring TACACS+ Servers - WebUI • 145
Configuring TACACS+ Servers for Non-Local Gaia Users • 149
Configuring Telnet Access - CLI (net-access) • 118
Configuring Telnet Access - WebUI • 117
Configuring the Session - CLI (inactivity-timeout) • 112
Configuring the Session - WebUI • 112
Configuring the VRRP Security Gateway Cluster in SmartDashboard • 163
Configuring the WebUI Web server • 118
Configuring VLAN Interfaces - WebUI • 41
Configuring VPN Tunnel Interfaces • 52
Configuring VPN Tunnel Interfaces - CLI (vpn tunnel) • 53
Configuring VPN Tunnel Interfaces - WebUI • 53
Configuring VRRP Clusters in SmartDashboard • 168
Configuring VRRP Rules for the Security Gateway • 164
Core Dumps • 112
CoreXL and Multi-queue Commands • 269

cp_conf • 211
cp_conf admin • 212
cp_conf auto • 214
cp_conf ca • 212
cp_conf client • 213
cp_conf finger • 213
cp_conf ha • 214
cp_conf lic • 213
cp_conf sic • 211
cp_conf snmp • 214
cp_conf sxl • 215
cpca_client • 209
cpca_client create_cert • 209
cpca_client lscert • 210
cpca_client revoke_cert • 210
cpca_client set_mgmt_tool • 210
cpconfig • 215
cphacnf • 266
cphaprob • 267
cphastart • 267
cphastop • 268
cpinfo • 215
cplic check • 172
cplic db_add • 173
cplic db_print • 173
cplic db_rm • 174
cplic del • 174
cplic del <object name> • 175
cplic get • 175
cplic print • 178
cplic put • 176
cplic put <object name> ... • 177
cplic upgrade • 179
cpstart • 216
cpstat • 216
cpstop • 218
CPUSE • 196
Creating or Deleting a Bond Interface • 46
Creating the Emergendisk Removable Device • 193

D
Defining Directional Matching VPN Rules • 55
Defining Interfaces • 46
Defining Rules to Allow OSPF Traffic • 56
Defining the Bond Operating Mode • 47
Defining the Media Monitoring Interval • 47
Defining the Primary Slave Interface • 47
Defining the UP and Down Delay Times • 48
Defining the VPN Community • 52
Defining VPN Rules • 55
Deny Access After Failed Login Attempts • 134, 138
Deny Access to Unused Accounts • 134, 137
DHCP Server • 62
Domain Name Service (DNS) • 68
Download SmartConsole • 183
Download SmartConsole - WebUI • 184
Downloading and Installing with CPUSE - clish • 199
Netflow Export • 78
Network Access • 117
Network Interfaces • 37
Network Management • 37

O
Obtaining a Configuration Lock • 24
Overview • 254, 261

P
Password History • 133, 136
Password Policy • 131
Password Strength • 132, 135
Performance Optimization • 81
Physical Interfaces • 38
Preparing a VRRP Cluster • 158

R
Resetting the Administrator Password • 194
Reviewing CPUSE – clish • 201
Roles • 127
rtm debug • 261
rtm drv • 261
rtm monitor • 262
rtm rtmd • 264
rtm stat • 264
rtm ver • 265
rtmstart • 265
rtmstop • 265
Running the First Time Configuration Wizard in CLI • 31
Running the First Time Configuration Wizard in WebUI • 31

S
Saving Configuration Changes • 20
Search Tool • 15
Security Management GUI Clients - WebUI • 151
Security Management Server and Firewall Commands • 209
Session • 112
Setting the Date - CLI (date) • 86
Setting the Time - CLI (Time) • 87
Setting the Time and Date - WebUI • 85
Setting the Time Zone - CLI (timezone) • 87
Showing Hardware Health Monitoring Information - WebUI • 184
Showing Hardware Information - CLI (show asset) • 185
Showing Hardware Monitoring Information - CLI (sysenv) • 184
Showing RAID Information - CLI • 186
Showing RAID Information - WebUI • 186
Showing System Overview Information - CLI • 18
Showing System Overview Information - WebUI • 17
Showing the Time & Date - CLI (clock) • 86
Shutdown • 186
Shutting Down - CLI (halt, reboot) • 187
Shutting Down - WebUI • 186
SmartView Monitor Commands • 261
Snapshot Image Management • 180
SNMP • 95
Status Bar • 15
System Configuration • 114
System Configuration Backup • 187
System Groups • 149
System Information Overview • 17
System Logging • 115
System Management • 84

T
Terminology • 153
Time • 84
Toolbar Accessories • 15
Troubleshooting VRRP • 168
Typical VRRP Use Cases • 156

U
Understanding VRRP • 153
User Account Fields - WebUI • 124
User Defined (Extended) Commands • 29
User Management • 122
Users • 123
Using the Interface Elements • 15

V
VLAN Interfaces • 41
VPN Commands • 254
vpn crl_zap • 254
vpn crlview • 254
vpn debug • 255
vpn drv • 256
vpn export_p12 • 256
vpn macutil • 257
vpn nssm_toplogy • 257
vpn overlap_encdom • 258
vpn sw_topology • 259
vpn tu • 259
VPN Tunnel Interfaces • 51
vpn ver • 260
VRRP • 153
VRRP Types • 154

W
WebUI Overview • 13
Working with System Configuration - CLI (configuration) • 191
Working with the Configuration Lock • 14