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=13241

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

For more about this release, see the R75.40 home page (http://supportcontent.checkpoint.com/solutions?id=sk67581).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 September 2012</td>
<td>Added R75.40 Gaia Feature Release (Gaia+):</td>
</tr>
<tr>
<td></td>
<td>• 6in4 Tunnel Interfaces (on page 52)</td>
</tr>
<tr>
<td></td>
<td>• PPPoE Interfaces (on page 53)</td>
</tr>
<tr>
<td></td>
<td>• TACACS+ Authentication Servers (on page 109)</td>
</tr>
<tr>
<td></td>
<td>• System Configuration Backup (on page 142)</td>
</tr>
<tr>
<td></td>
<td>Updated SNMP (on page 75).</td>
</tr>
<tr>
<td></td>
<td>Deleted unsupported commands: vpn accel, vpn compreset, vpn compstat.</td>
</tr>
<tr>
<td>13 May 2012</td>
<td>Updated SNMP (on page 75)</td>
</tr>
<tr>
<td>16 April 2012</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 (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Gaia R75.40 Administration Guide).
Contents

Important Information.................................................................3
Gaia Overview ...................................................................................9
Introduction to the WebUI .................................................................10
  WebUI Overview ............................................................................10
  Logging in to the WebUI ...............................................................11
  Working with the Configuration Lock ..............................................12
  Using the Interface Elements .........................................................12
  Toolbar Accessories .......................................................................12
  Search Tool ..................................................................................13
  Navigation Tree ..............................................................................13
  Status Bar ....................................................................................13
  Configuration Tab ..........................................................................13
  Monitoring Tab ...............................................................................14
Introduction to the Command Line Interface ..................................15
  Saving Configuration Changes .........................................................15
  Commands and Features ................................................................15
  Command Completion .....................................................................17
  Command History ...........................................................................18
  Command Reuse ............................................................................18
  Command Line Movement and Editing ..........................................19
  Obtaining a Configuration Lock ....................................................20
  32 and 64-bit Gaia Editions ............................................................20
  Environment Commands .................................................................21
    Client Environment Output Format ..............................................23
  Expert Mode ................................................................................23
  User Defined (Extended) Commands ..............................................24
System Information Overview .......................................................26
  Showing System Overview Information - WebUI ............................26
  Showing System Overview Information - CLI (uptime, version) ......27
  Changing System Edition ................................................................28
Network Management .......................................................................29
  Network Interfaces ........................................................................29
    Interface Link Status ...................................................................29
    CLI Reference (interface) ............................................................30
    Physical Interfaces .......................................................................33
    Aliases ......................................................................................35
    VLAN Interfaces ..........................................................................36
    Bond Interfaces (Link Aggregation) ................................................39
    Bridge Interfaces .........................................................................45
    Loopback Interfaces ......................................................................46
    VPN Tunnel Interfaces ...................................................................47
    6in4 Tunnel Interfaces ..................................................................52
    PPPoE Interfaces ...........................................................................53
    ARP .............................................................................................55
      Configuring ARP - WebUI ..........................................................55
      Configuring ARP - CLI (arp) .........................................................56
    DHCP Server ................................................................................57
      Configuring a DHCP Server - WebUI ...........................................58
      Configuring a DHCP Server - CLI (dhcp) ......................................58
    Hosts and DNS ............................................................................61
      Host Name ..................................................................................61
      Host Addresses ...........................................................................61
Domain Name Service (DNS) ............................................. 63
IPv4 Static Routes ......................................................... 64
Configuring IPv4 Static Routes - WebUI .......................... 65
Configuring Static Routes - CLI (static-route) .................. 66
IPv6 Static Routes ......................................................... 68
Configuring IPv6 Static Routes - WebUI .......................... 68
Configuring IPv6 Static Routes - CLI (ipv6 static-route) .... 69
IPv6 Neighbor-Entry ...................................................... 71
System Management ................................................................... 72
Time ............................................................................. 72
Setting the Time and Date - WebUI ................................. 72
Configuring NTP - CLI (ntp) ...................................... 73
Showing the Time & Date - CLI (clock) ......................... 74
Setting the Date - CLI (date) ...................................... 74
Setting the Time - CLI (Time) ................................. 74
Setting the Time Zone - CLI (timezone) ......................... 75
SNMP ........................................................................ 75
Configuring SNMP - WebUI ...................................... 77
Configuring SNMP - CLI (snmp) ................................ 79
Interpreting Error Messages ..................................... 83
Job Scheduler ................................................................. 85
Configuring Job Scheduler - WebUI .............................. 85
Configuring Job Scheduler - CLI (cron) ......................... 86
Mail Notification ............................................................. 87
Configuring Mail Notification - WebUI ......................... 88
Configuring Mail Notification - CLI (mail-notification) ...... 88
Messages ..................................................................... 88
Configuring Messages - WebUI ................................ 88
Configuring Messages - CLI (message) ......................... 89
Session ......................................................................... 90
Configuring the Session - WebUI ................................. 90
Configuring the Session - CLI (inactivity-timeout) ........... 90
System Configuration .................................................... 90
Configuring the IPv6 Support - WebUI ......................... 90
Configuring the IPv6 Support - CLI .......................... 90
System Logging ............................................................... 90
Configuring System Logging - WebUI ......................... 91
Configuring System Logging - CLI (syslog) ................. 91
Configuring Log Volume - CLI (volume) ................... 92
Network Access .............................................................. 93
Configuring Telnet Access - WebUI ............................. 93
Configuring Telnet Access - CLI (net-access) ............... 93
Configuring the WebUI Web server ............................ 93
Host Access .................................................................. 95
Configuring Allowed Gaia Clients - WebUI .................. 95
Configuring Allowed Gaia Clients - CLI (allowed-client) ... 96
Advanced Routing .................................................................. 97
User Management .................................................................. 98
Change My Password .................................................... 98
Change My Password - WebUI .................................. 98
Change My Password - CLI (selfpasswd) .................. 98
Users .......................................................................... 98
Managing User Accounts - WebUI .............................. 99
Managing User Accounts - CLI (user) ..................... 100
Roles .......................................................................... 103
Configuring Roles - WebUI ..................................... 103
Configuring Roles - CLI (rba) ................................ 105
Password Policy .............................................................. 106
Password History Checks ........................................... 107
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory Password Change</td>
<td>107</td>
</tr>
<tr>
<td>Configuring Password Policy - WebUI</td>
<td>107</td>
</tr>
<tr>
<td>Configuring Password Policy - CLI (password-controls)</td>
<td>108</td>
</tr>
<tr>
<td>Authentication Servers</td>
<td>109</td>
</tr>
<tr>
<td>Configuring RADIUS Servers - WebUI</td>
<td>110</td>
</tr>
<tr>
<td>Configuring RADIUS Servers - CLI (aaa)</td>
<td>111</td>
</tr>
<tr>
<td>Configuring Gaia as a RADIUS Client</td>
<td>112</td>
</tr>
<tr>
<td>Configuring RADIUS Servers for Non-Local Users</td>
<td>112</td>
</tr>
<tr>
<td>Configuring TACACS+ Servers - WebUI</td>
<td>112</td>
</tr>
<tr>
<td>Configuring TACACS+ Servers - CLI (aaa)</td>
<td>112</td>
</tr>
<tr>
<td>Configuring Gaia as a TACACS+ Client</td>
<td>113</td>
</tr>
<tr>
<td>Configuring TACACS+ Servers for Non-Local Users</td>
<td>114</td>
</tr>
<tr>
<td>System Groups</td>
<td>114</td>
</tr>
<tr>
<td>Configuring System Groups - WebUI</td>
<td>114</td>
</tr>
<tr>
<td>Configuring System Groups - CLI (group)</td>
<td>115</td>
</tr>
<tr>
<td>GUI Clients</td>
<td>115</td>
</tr>
<tr>
<td>Security Management GUI Clients - WebUI</td>
<td>116</td>
</tr>
<tr>
<td>GUI Clients - CLI (cpconfig)</td>
<td>116</td>
</tr>
<tr>
<td>High Availability</td>
<td>117</td>
</tr>
<tr>
<td>VRRP</td>
<td>117</td>
</tr>
<tr>
<td>Terminology</td>
<td>117</td>
</tr>
<tr>
<td>How VRRP Works</td>
<td>118</td>
</tr>
<tr>
<td>Before Configuring VRRP</td>
<td>120</td>
</tr>
<tr>
<td>Configuring a Virtual Router - WebUI</td>
<td>122</td>
</tr>
<tr>
<td>Configuring a Virtual Router - CLI (mcrv)</td>
<td>123</td>
</tr>
<tr>
<td>Advanced VRRP</td>
<td>126</td>
</tr>
<tr>
<td>Configuring Advanced VRRP - WebUI</td>
<td>126</td>
</tr>
<tr>
<td>Configuring Advanced VRRP - CLI (vrrp)</td>
<td>128</td>
</tr>
<tr>
<td>Troubleshooting VRRP</td>
<td>130</td>
</tr>
<tr>
<td>General Configuration Considerations</td>
<td>130</td>
</tr>
<tr>
<td>Firewall Policies</td>
<td>131</td>
</tr>
<tr>
<td>Monitored-Circuit VRRP in Switched Environments</td>
<td>131</td>
</tr>
<tr>
<td>Maintenance</td>
<td>132</td>
</tr>
<tr>
<td>Licenses</td>
<td>132</td>
</tr>
<tr>
<td>Configuring Licenses - WebUI</td>
<td>132</td>
</tr>
<tr>
<td>Configuring Licenses - CLI (cplic)</td>
<td>133</td>
</tr>
<tr>
<td>Image Management</td>
<td>140</td>
</tr>
<tr>
<td>Configuring Image Management - WebUI</td>
<td>140</td>
</tr>
<tr>
<td>Configuring Image Management - CLI (snapshot)</td>
<td>141</td>
</tr>
<tr>
<td>System Configuration Backup</td>
<td>142</td>
</tr>
<tr>
<td>Backing Up and Restoring the System - WebUI</td>
<td>143</td>
</tr>
<tr>
<td>Backing and Restoring the System - CLI (Backup)</td>
<td>143</td>
</tr>
<tr>
<td>Configuring Scheduled Backups - WebUI</td>
<td>144</td>
</tr>
<tr>
<td>Configuring Scheduled Backups - CLI (backup-scheduled)</td>
<td>145</td>
</tr>
<tr>
<td>Working with System Configuration - CLI (configuration)</td>
<td>146</td>
</tr>
<tr>
<td>Download SmartConsole</td>
<td>147</td>
</tr>
<tr>
<td>Download SmartConsole - WebUI</td>
<td>147</td>
</tr>
<tr>
<td>Hardware Health Monitoring</td>
<td>147</td>
</tr>
<tr>
<td>Showing Hardware Health Monitoring Information - WebUI</td>
<td>147</td>
</tr>
<tr>
<td>Showing Hardware Monitoring Information - CLI (sysenv)</td>
<td>148</td>
</tr>
<tr>
<td>Shutdown</td>
<td>148</td>
</tr>
<tr>
<td>Shutting Down - WebUI</td>
<td>148</td>
</tr>
<tr>
<td>Shutting Down - CLI (halt, reboot)</td>
<td>149</td>
</tr>
<tr>
<td>Software Updates</td>
<td>150</td>
</tr>
<tr>
<td>Configuring a Software Deployment Policy - WebUI</td>
<td>150</td>
</tr>
<tr>
<td>Configuring Software Update Notifications - WebUI</td>
<td>151</td>
</tr>
<tr>
<td>Configuring Software Deployment - WebUI</td>
<td>151</td>
</tr>
<tr>
<td>Configuring Software Deployment – clish (installation)</td>
<td>152</td>
</tr>
<tr>
<td>CLI Procedures - Software Updates</td>
<td>153</td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>cpca_client</td>
<td>156</td>
</tr>
<tr>
<td>cpca_client create_cert</td>
<td>156</td>
</tr>
<tr>
<td>cpca_client revoke_cert</td>
<td>156</td>
</tr>
<tr>
<td>cpca_client lsCert</td>
<td>157</td>
</tr>
<tr>
<td>cpca_client set_mgmt_tools</td>
<td>157</td>
</tr>
<tr>
<td>cp_conf</td>
<td>158</td>
</tr>
<tr>
<td>cp_conf sic</td>
<td>158</td>
</tr>
<tr>
<td>cp_conf admin</td>
<td>158</td>
</tr>
<tr>
<td>cp_conf ca</td>
<td>158</td>
</tr>
<tr>
<td>cp_conf finger</td>
<td>158</td>
</tr>
<tr>
<td>cp_conf lic</td>
<td>158</td>
</tr>
<tr>
<td>cp_conf client</td>
<td>159</td>
</tr>
<tr>
<td>cp_conf ha</td>
<td>159</td>
</tr>
<tr>
<td>cp_conf snmp</td>
<td>159</td>
</tr>
<tr>
<td>cp_conf auto</td>
<td>159</td>
</tr>
<tr>
<td>cp_conf sxl</td>
<td>159</td>
</tr>
<tr>
<td>cpconfig</td>
<td>159</td>
</tr>
<tr>
<td>cpinfo</td>
<td>160</td>
</tr>
<tr>
<td>cpstart</td>
<td>160</td>
</tr>
<tr>
<td>cpstat</td>
<td>161</td>
</tr>
<tr>
<td>cpstop</td>
<td>162</td>
</tr>
<tr>
<td>fw</td>
<td>163</td>
</tr>
<tr>
<td>fw -i</td>
<td>163</td>
</tr>
<tr>
<td>fw ctl</td>
<td>163</td>
</tr>
<tr>
<td>fw ctl debug</td>
<td>164</td>
</tr>
<tr>
<td>fw ctl affinity</td>
<td>166</td>
</tr>
<tr>
<td>fw ctl engine</td>
<td>167</td>
</tr>
<tr>
<td>fw ctl multik stat</td>
<td>168</td>
</tr>
<tr>
<td>fw ctl sdstat</td>
<td>168</td>
</tr>
<tr>
<td>fw fetch</td>
<td>169</td>
</tr>
<tr>
<td>fw fetchlogs</td>
<td>170</td>
</tr>
<tr>
<td>fw hastat</td>
<td>170</td>
</tr>
<tr>
<td>fw isp_link</td>
<td>171</td>
</tr>
<tr>
<td>fw kill</td>
<td>171</td>
</tr>
<tr>
<td>fw lea_notify</td>
<td>172</td>
</tr>
<tr>
<td>fw lichosts</td>
<td>172</td>
</tr>
<tr>
<td>fw log</td>
<td>172</td>
</tr>
<tr>
<td>fw logswitch</td>
<td>174</td>
</tr>
<tr>
<td>fw mergefiles</td>
<td>175</td>
</tr>
<tr>
<td>fw monitor</td>
<td>176</td>
</tr>
<tr>
<td>fw lslogs</td>
<td>179</td>
</tr>
<tr>
<td>fw putkey</td>
<td>180</td>
</tr>
<tr>
<td>fw repairlog</td>
<td>181</td>
</tr>
<tr>
<td>fw sam</td>
<td>181</td>
</tr>
<tr>
<td>fw stat</td>
<td>185</td>
</tr>
<tr>
<td>fw tab</td>
<td>185</td>
</tr>
<tr>
<td>fw ver</td>
<td>186</td>
</tr>
<tr>
<td>fwm</td>
<td>187</td>
</tr>
<tr>
<td>fwm dbimport</td>
<td>187</td>
</tr>
<tr>
<td>fwm expdate</td>
<td>188</td>
</tr>
<tr>
<td>fwm dbexport</td>
<td>188</td>
</tr>
<tr>
<td>fwm dbload</td>
<td>190</td>
</tr>
<tr>
<td>fwm ikencrypt</td>
<td>190</td>
</tr>
<tr>
<td>fwm getcap</td>
<td>190</td>
</tr>
<tr>
<td>fwm load</td>
<td>191</td>
</tr>
<tr>
<td>fwm lock_admin</td>
<td>191</td>
</tr>
<tr>
<td>fwm logexport</td>
<td>192</td>
</tr>
<tr>
<td>fwm sic_reset</td>
<td>193</td>
</tr>
</tbody>
</table>
fwm unload <targets> ................................................................. 193
fwm ver ................................................................. 193
fwm verify <policy-name> ................................................................. 193

**VPN Commands** ........................................................................... 195
Overview .................................................................................. 195
vpn crl_zap ........................................................................ 195
vpn crlview ........................................................................ 195
vpn debug ........................................................................... 196
vpn drv ........................................................................ 197
vpn export_p12 ....................................................................... 197
vpn macutil ........................................................................ 197
vpn nssm_toplogy ..................................................................... 198
vpn overlap_encdom .................................................................. 198
vpn sw_topology ......................................................................... 199
vpn tu ..................................................................................... 199
vpn ver ................................................................................. 200

**SmartView Monitor Commands** ......................................................... 201
Overview .................................................................................. 201
rtm debug ............................................................................. 201
rtm drv ................................................................................... 201
rtm monitor <module_name>{<interface_name>|filter "<complex filter>"} ... 202
rtm monitor <module_name>-v<virtual_link_name> ....................... 204
rtm rtmd ............................................................................... 205
rtm stat .................................................................................. 205
rtm ver ................................................................................... 205
rtmstart .................................................................................. 205
rtmstop .................................................................................. 206

**ClusterXL Commands** .................................................................... 207
cphaconf ............................................................................... 207
cphaprob ............................................................................... 208
cphastart ............................................................................... 208
cphastop ............................................................................... 208

Index .................................................................................................. 209
Chapter 1

Gaia Overview

Gaia is Check Point's 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 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 Software Updates

- 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.
Chapter 2

Introduction to the WebUI

In This Chapter

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebUI Overview</td>
<td>10</td>
</tr>
<tr>
<td>Logging in to the WebUI</td>
<td>11</td>
</tr>
<tr>
<td>Using the Interface Elements</td>
<td>12</td>
</tr>
</tbody>
</table>

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.
Introduction to the WebUI

The WebUI interface

<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 timeout 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 103).

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 using the WebUI:

- Click the small lock icon (Configuration lock) above the toolbar. The pencil icon (Read/Write enabled) replaces the lock.
  or
- If you are already using a configuration settings page, click the **Click here to obtain lock** link. This can occur 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><img src="icon" alt="Read/Write mode enabled" /></td>
<td>Read/Write mode enabled.</td>
</tr>
<tr>
<td><img src="icon" alt="Configuration locked" /></td>
<td>Configuration locked (Read Only mode).</td>
</tr>
<tr>
<td><img src="icon" alt="Console accessory" /></td>
<td>Opens the Console accessory for CLI commands. Available in the Read/Write mode only.</td>
</tr>
<tr>
<td><img src="icon" alt="Scratch Pad accessory" /></td>
<td>Opens the Scratch Pad accessory for writing notes or for quick copy/paste operations. Available in the Read/Write mode only.</td>
</tr>
<tr>
<td><img src="icon" alt="Send feedback" /></td>
<td>Send detailed Gaia feedback to Check Point.</td>
</tr>
<tr>
<td><img src="icon" alt="I like this page" /></td>
<td>I like this page - send positive feedback</td>
</tr>
<tr>
<td><img src="icon" alt="I do not like this page" /></td>
<td>I do not like this page - send negative feedback</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.
Chapter 3

Introduction to the Command Line Interface

In This Chapter

- Saving Configuration Changes 15
- Commands and Features 15
- Command Completion 17
- Command History 18
- Command Line Movement and Editing 19
- Obtaining a Configuration Lock 20
- 32 and 64-bit Gaia Editions 20
- Environment Commands 21
- Expert Mode 23
- User Defined (Extended) Commands 24

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

Configuration changes you enter using the CLI are applied immediately to the running system. To ensure that these changes remain after you reboot, that is, to save your changes permanently, run save config at the CLI prompt.

Commands and Features

Gaia commands are organized into features. A feature is a group of related commands.

Commands have the syntax

```
Operation feature parameter
```

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

<table>
<thead>
<tr>
<th>The 4 main operations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>Sets a value in the system.</td>
</tr>
<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>
<tr>
<td>The 4 main operations</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>add</strong></td>
<td>Adds a new value to the system.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other operations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>save</strong></td>
<td>Saves the configuration changes made since the last save operation.</td>
</tr>
<tr>
<td><strong>reboot</strong></td>
<td>Restart the system.</td>
</tr>
<tr>
<td><strong>halt</strong></td>
<td>Turns the computer off.</td>
</tr>
<tr>
<td><strong>quit</strong></td>
<td>Exits from the CLI.</td>
</tr>
<tr>
<td><strong>exit</strong></td>
<td>Exits from the shell.</td>
</tr>
</tbody>
</table>

**Start**

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.

- **commit**
  Ends transaction by committing changes.
- **rollback**
  Ends transaction by discarding changes.
- **expert**
  Enter the expert shell. Allows low-level access to the system, including the file system.
- **ver**
  Shows the version of the active Gaia image
- **revert**
  Revert the database
- **help**
  Get help on navigating the CLI and some useful commands.

**To do this**

<table>
<thead>
<tr>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show commands</strong></td>
</tr>
</tbody>
</table>

**Show a list of all features**

**show commands feature <TAB>**

**Shows all commands for a specific feature**

**show commands feature VALUE**

**For example**

Gaia> **show commands feature arp**
add arp static ipv4-address VALUE macaddress VALUE
delete arp dynamic all
delete arp static ipv4-address VALUE
set arp table cache-size VALUE
set arp table validity-timeout VALUE
show arp dynamic all
show arp static all
show arp table cache-size
show arp table validity-timeout
**Introduction to the Command Line Interface**

<table>
<thead>
<tr>
<th>To do this</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show all the possible operations</td>
<td><code>show commands op &lt;SPACE&gt; &lt;TAB&gt;</code></td>
</tr>
<tr>
<td>For example</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>show commands op</code></td>
</tr>
<tr>
<td></td>
<td>revert</td>
</tr>
<tr>
<td></td>
<td>enable</td>
</tr>
<tr>
<td></td>
<td>load</td>
</tr>
<tr>
<td></td>
<td>exit</td>
</tr>
</tbody>
</table>

| Show all commands per operation, per feature   | `show commands [op VALUE] [feature VALUE]`                           |
| For example                                    |                                                                      |
|                                                 | `Gaia> show commands op show feature arp`                           |
|                                                 | show arp dynamic all                                              |
|                                                 | show arp static all                                               |
|                                                 | show arp table cache-size                                         |
|                                                 | show arp table validity-timeout                                    |
|                                                 | `Gaia>`                                                            |

**At the --More-- prompt:**

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>To see the next page.</td>
<td><code>&lt;SPACE&gt;</code></td>
</tr>
<tr>
<td>To see the next line.</td>
<td><code>&lt;ENTER&gt;</code></td>
</tr>
<tr>
<td>To exit to the CLI prompt</td>
<td><code>&lt;Q&gt;</code> or <code>&lt;q&gt;</code></td>
</tr>
</tbody>
</table>

**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><code>&lt;TAB&gt;</code></td>
<td>Complete or fetch the keyword. For example</td>
</tr>
<tr>
<td></td>
<td><code>Gaia&gt; set in&lt;TAB&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>inactivity-timeout</code> - Set inactivity timeout</td>
</tr>
<tr>
<td></td>
<td><code>interface</code> - Displays the interface related parameters</td>
</tr>
<tr>
<td></td>
<td><code>Gaia&gt; set in</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><code>&lt;SPACE&gt; &lt;TAB&gt;</code></th>
<th>Show the arguments that the command for that feature accepts. For example:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>Gaia&gt; set interface &lt;SPACE&gt; &lt;TAB&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>eth0 eth1 lo</code></td>
</tr>
<tr>
<td></td>
<td><code>Gaia&gt; set interface</code></td>
</tr>
</tbody>
</table>
Press ... | To do this...
---|---
<ESC><ESC> | See possible command completions. For example

Gaia> set in<ESC><ESC>
set interface VALUE ipv4-address VALUE mask-length VALUE
set interface VALUE ipv4-address VALUE subnet-mask VALUE
set interface VALUE ipv6-address VALUE mask-length VALUE
set interface VALUE { comments VALUE mac-addr VALUE mtu VALUE
state VALUE speed VALUE duplex VALUE auto-negotiation VALUE }
set interface VALUE { ipv6-autoconfig VALUE }
Gaia> set inter

? | Get help on a feature or keyword. For example

Gaia> set interface <?>
interface: {show/add/delete} interface "interface-name"
Gaia> set interface

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

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

<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>
<tr>
<td>history</td>
<td>Show the last 100 commands.</td>
</tr>
<tr>
<td>!!</td>
<td>Run the last command.</td>
</tr>
<tr>
<td>!nn</td>
<td>Run a specific previous command: The nn command.</td>
</tr>
<tr>
<td>!-nn</td>
<td>Run the nth previous command. For example, entering !-3 runs the third from last command.</td>
</tr>
<tr>
<td>!str</td>
<td>Run the most recent command that starts with str.</td>
</tr>
<tr>
<td>?str?</td>
<td>Run the most recent command containing str. The trailing ? may be omitted if str is followed immediately by a new line.</td>
</tr>
<tr>
<td>!!:s/str1/str2</td>
<td>Repeat the last command, replacing str1 with str2</td>
</tr>
</tbody>
</table>

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 n:th 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 new for the first occurrence of old 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 s, as in gs/str1/str2.</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>
</tbody>
</table>
Keystroke combination | Meaning
--- | ---
Ctrl-U | Delete the current line.

## Obtaining a Configuration Lock

Only one user can have Read/Write access to Gaia configuration settings at a time. All other users can log in with Read-Only access to see configuration settings, as specified by their assigned roles (on page 103).

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 database feature has two commands:

- **lock database [override].**
- **unlock database**

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
- set config-lock on [timeout VALUE override]
- show config-lock
- show config-state

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>on 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 R75.40 Release notes (http://supportcontent.checkpoint.com/solutions?id=sk67581).

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 between 32 and 64-bit versions of Gaia.

### Syntax
```bash
set edition default <VALUE>
```

<table>
<thead>
<tr>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-bit</td>
<td>Sets the default edition to 32-bit</td>
</tr>
<tr>
<td>64-bit</td>
<td>Sets the default edition to 64-bit</td>
</tr>
</tbody>
</table>

### 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.
- Or
- 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**
```bash
show clienv all
show clienv config-lock
show clienv debug
show clienv echo-cmd
show clienv on-failure
show clienv output
show clienv prompt
show clienv rows
show clienv syntax-check
```

**To set the client environment**
```bash
set clienv config-lock VALUE
set clienv debug VALUE
set clienv echo-cmd VALUE
set clienv on-failure VALUE
set clienv output VALUE
set clienv prompt VALUE
set clienv rows VALUE
set clienv syntax-check VALUE
```

**To save the client environment permanently**
```bash
save clienv
```
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Show all the client environment settings.</td>
</tr>
<tr>
<td>config-lock</td>
<td>The default value of the config-lock parameter. If it is set to 'on'; clish will acquire config-lock when invoked otherwise continue without a config-lock. The value can be 'on' or 'off'.</td>
</tr>
<tr>
<td>debug &lt;0-6&gt;</td>
<td>The debug level. Level 0 (lowest) to level 6 (highest). Predefined levels are:</td>
</tr>
<tr>
<td></td>
<td>0  Do not do debugging. Display error messages only.</td>
</tr>
<tr>
<td></td>
<td>5  Show confd requests, responses.</td>
</tr>
<tr>
<td></td>
<td>6  Show handler invocation parameters, results.</td>
</tr>
<tr>
<td>ech-cmd</td>
<td>Echo all commands. When using the load commands command, all commands are echoed before being executed. Default: off</td>
</tr>
<tr>
<td>on-failure</td>
<td>• Continue - continue running commands from a file or a script and only display error messages.</td>
</tr>
<tr>
<td></td>
<td>• Stop - stop running commands from a file or a script when the system encounters an error. Default: stop</td>
</tr>
<tr>
<td>output</td>
<td>The command line output format (&quot;Client Environment Output Format&quot; on page 23). Default: pretty</td>
</tr>
<tr>
<td>prompt VALUE</td>
<td>The appearance of the command prompt. To set the prompt back to the default, use the keyword default. Any printable character is allowed, as well as combinations of the following variables:</td>
</tr>
<tr>
<td></td>
<td>%H : Replaced with the Command number.</td>
</tr>
<tr>
<td></td>
<td>%I : Replaced with the User ID.</td>
</tr>
<tr>
<td></td>
<td>%M : Replaced with the Hostname.</td>
</tr>
<tr>
<td></td>
<td>%P : Replaced with the Product ID.</td>
</tr>
<tr>
<td></td>
<td>%U : Replaced with the User Name.</td>
</tr>
<tr>
<td>rows integer</td>
<td>The number of rows to show on your console or xterm. If the window size is changed the value will also change, unless the value set is to 0 (zero).</td>
</tr>
<tr>
<td>syntax-check</td>
<td>Put the shell into syntax-check mode. Commands you enter are checked syntactically and are not executed, but values are validated. Default: off</td>
</tr>
<tr>
<td>save clienv</td>
<td>Permanently save the environment variables that were modified using the set clienv commands.</td>
</tr>
</tbody>
</table>
**Client Environment Output Format**

**Description**
The CLI supports three output formats: pretty, structured, and xml.

**Syntax**
To show the output format

```
show clienv output VALUE
```

To set the output format

```
set clienv output VALUE
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pretty</td>
<td>Output is formatted to be clear. For example</td>
</tr>
<tr>
<td></td>
<td>Gaia&gt; set clienv output pretty</td>
</tr>
<tr>
<td></td>
<td>Gaia&gt; show user admin</td>
</tr>
<tr>
<td></td>
<td>Uid  Gid  Home Dir.  Shell    Real Name</td>
</tr>
<tr>
<td></td>
<td>0      0      /home/admin  /etc/cli.sh  n/a</td>
</tr>
</tbody>
</table>

Structured

Output is delimited by semi-colons. For example

```
Gaia> set clienv output structured
Gaia> show user admin
Uid;Gid;Home Dir.;Shell;Real Name;
0;0;/home/admin;/etc/cli.sh;;
```

xml

Adds XML tags to the output. For example

```
Gaia> set clienv output xml
Gaia> show user admin
<?xml version="1.0"?>
<CMDRESPONSE>
<CMDTEXT>show user admin</CMDTEXT>
<RESPONSE><System_User>
<Row>
<Uid>0</Uid>
<Gid>0</Gid>
<Home_Dir.>/home/admin</Home_Dir.>
<Shell>/etc/cli.sh</Shell>
<Real_Name></Real_Name>
</Row>
</System_User>
</RESPONSE>
</CMDRESPONSE>
```

**Expert Mode**

The default shell of the CLI is called clish. Clish is a restrictive shell (role-based administration controls the number of commands available in the shell). While 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 plain
- 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. Use this option when upgrading or restoring using backup scripts.</td>
</tr>
<tr>
<td>plain</td>
<td>The password in plain text</td>
</tr>
</tbody>
</table>

Example:

gw> set expert-password plain
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
   add command free path /usr/bin/free description "Display amount of free and used memory in the system"

2. Save the configuration. Run
   save config

3. Log out of Gaia and log in again.

4. To add the free command to the systemDiagnosis role, run
   add rba role systemDiagnosis domain-type System readwrite-features ext_free

5. To assign user john with the systemDiagnosis role, run
   add rba user john roles systemDiagnosis
This chapter shows you how to see system information using the WebUI and some CLI commands.

**Showing System Overview Information - WebUI**

The **Overview** page contains a configurable collection of status display elements, called **widgets**. You can add or remove widgets from the page, move them around the page and minimize or expand them.

Currently these widgets are available:
<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Overview</td>
<td>Shows system information, including:</td>
</tr>
<tr>
<td></td>
<td>• Installed product</td>
</tr>
<tr>
<td></td>
<td>• Product version number</td>
</tr>
<tr>
<td></td>
<td>• Kernel build</td>
</tr>
<tr>
<td></td>
<td>• Product build</td>
</tr>
<tr>
<td></td>
<td>• Edition (32 bit or 64 bit)</td>
</tr>
<tr>
<td></td>
<td>• Platform on which Gaia is installed</td>
</tr>
<tr>
<td></td>
<td>• Computer serial number (if applicable)</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>Shows 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>
<tr>
<td>Security Configuration</td>
<td>Lets you download the SmartConsole applications (Security Management server installations only)</td>
</tr>
</tbody>
</table>

To add a widget to 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 (uptime, version)

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, run:

```
show version all
```

To show version information for OS components, run:

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

To show name of the installed product

```
show version product
```
System Information Overview

### Description
Show the name and versions of the OS components

### 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 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.
- 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**

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

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

```plaintext
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.
Chapter 5

Network Management

In This Chapter

- Network Interfaces
- ARP
- DHCP Server
- Hosts and DNS
- IPv4 Static Routes
- IPv6 Static Routes
- IPv6 Neighbor-Entry

This chapter includes configuration procedures and examples for configuring:

- Network interfaces
- ARP
- DHCP server
- Hosts and DNS
- Static routes (IPv4 and IPv6)

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>IP4 Address</th>
<th>IPv6 Address</th>
<th>Link Status</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>bond40</td>
<td>Bond</td>
<td>10.0.0.1</td>
<td>2001:0db8:1</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>br20</td>
<td>Bridge</td>
<td>192.168.1.1</td>
<td>2001:0db8:1</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>eth0</td>
<td>Ethernet</td>
<td>10.0.0.1</td>
<td></td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>eth1</td>
<td>Ethernet</td>
<td>10.0.0.1</td>
<td></td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>eth1:1</td>
<td>Alias</td>
<td>10.0.0.1</td>
<td></td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>eth1:2</td>
<td>Alias</td>
<td>10.0.0.1</td>
<td></td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>eth2</td>
<td>Ethernet</td>
<td>10.0.0.1</td>
<td></td>
<td>No Link</td>
<td></td>
</tr>
<tr>
<td>eth3</td>
<td>Ethernet</td>
<td>10.0.0.1</td>
<td></td>
<td>Down</td>
<td></td>
</tr>
<tr>
<td>eth4</td>
<td>Ethernet</td>
<td>10.0.0.1</td>
<td></td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>eth5</td>
<td>Ethernet</td>
<td>10.0.0.1</td>
<td></td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>eth6</td>
<td>Ethernet</td>
<td>10.0.0.1</td>
<td></td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>eth7</td>
<td>Ethernet</td>
<td>10.0.0.1</td>
<td></td>
<td>Up</td>
<td></td>
</tr>
</tbody>
</table>

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>
<tr>
<td>Green (Up)</td>
<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`

**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>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Configures a physical or virtual interface</td>
</tr>
<tr>
<td>6in4</td>
<td>Configures a 6in4 tunnel for IPv6 traffic over an IPv4 network</td>
</tr>
<tr>
<td>6to4</td>
<td>Configures a 6to4 tunnel for IPv6 traffic over an IPv4 network</td>
</tr>
<tr>
<td>remote</td>
<td>Sets the remote IP address for a 6in4 or 6to4 tunnel</td>
</tr>
<tr>
<td>ttl</td>
<td>Sets the time-to-live value for a 6in4 or 6to4 tunnel</td>
</tr>
<tr>
<td>alias</td>
<td>Assigns more than one IP addresses to a physical interface (IPv4 only)</td>
</tr>
<tr>
<td>loopback</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>vlan</td>
<td>Assigns a VLAN tag to an existing physical interface to create a logical subnet.</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>
### 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:</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

See the interface configuration section.

### Comments

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

---

### 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:
   - Select **Obtain IPv4 address automatically** to get the IP address from the DHCP server.
   - Or
• Enter the IP address and subnet mask in the applicable fields.

5. On the IPv6 tab:
   • Select **Obtain IPv6 address automatically** to get the IP address from the DHCP server.
     Or
   • Enter the IP address and mask length in the applicable fields.

6. On the Ethernet tab configure the link speed and duplex setting:
   • Select **Auto Negotiation** to automatically configure the link speed and duplex setting.
     Or
   • 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 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 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.

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 **Interface 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**. She second alias added is **eth1:1**, and so on.

To delete an interface alias:
1. In the navigation tree, select **Interface 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><code>&lt;IP&gt;</code></td>
<td>IPv4 address</td>
</tr>
<tr>
<td><code>&lt;IF&gt;</code></td>
<td>Interface name</td>
</tr>
<tr>
<td><code>&lt;Mask&gt;</code></td>
<td>IPv4 subnet mask length using CIDR (/xx) notation</td>
</tr>
<tr>
<td><code>&lt;Alias IF&gt;</code></td>
<td>Interface alias name in the format <code>&lt;IF&gt;:XX</code>, where <code>XX</code> 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 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.

---

## 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 **Interface 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.

![VLAN Configuration Interface](image)

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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>Configure an interface</td>
</tr>
<tr>
<td><code>ipv4-address</code></td>
<td>Assign an IPv4 address</td>
</tr>
<tr>
<td><code>ipv6-address</code></td>
<td>Assign an IPv6 address</td>
</tr>
<tr>
<td><code>ipv6-autoconfig</code></td>
<td>Automatically configure an IPv6 address</td>
</tr>
<tr>
<td><code>on</code></td>
<td>Enable automatic configuration</td>
</tr>
<tr>
<td><code>off</code></td>
<td>Disable automatic configuration</td>
</tr>
</tbody>
</table>

**Values**

- `<IF>`: Physical interface related to this VLAN
- `<VLAN ID>`: VLAN identifier (integer range 1-4094)
- `<IP>`: IP address (IPv4 or IPv6)
- `<Length>`: Mask length (integer value)
Description  Use these commands to configure bridge interfaces.

Example

add interface vlan eth1

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

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

delete interface eth1 vlan 99

Important - After 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.

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. You can configure High Availability to work one of in these modes:
  - **Round Robin** - Selects the active slave interface sequentially.
  - **Active/Backup** - If the active slave interface goes 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.

- **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, select a **Link Monitoring** option and its frequency in milliseconds:
   - **Media Monitoring Interval** - This sets the frequency of requests sent to the Media Independent Interface (MMI) to confirm that a slave interface is up. The valid range is 1-5000 ms and the default is 100 ms.
- **ARP Monitoring** - This defines the frequency of ARP requests sent to confirm that a slave interface is up. ARP requests are sent to as many as five external MAC addresses.

![Add Bond dialog box](image)

10. Select the **UP** and **Down** intervals in milliseconds. This parameter defines the waiting time, in milliseconds, to confirm the slave interface status before taking the specified action.

11. Select the **Primary Interface** (for Active/Backup bonds only).

12. Select the **Transmit Hash Policy** (XOR only). This parameter selects the algorithm for slave selection according to the specified TCP/IP layer.

13. Select the **LACP Rate**. This parameter sets the LACPDU packet transmission rate.

### Configuring Bond Interfaces - CLI

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

When using the CLI to create a bond interface, do these procedures in order:

1. Create the bond interface.
2. Define the slave interfaces and set them to the **UP (on)** State.
3. Define the bond operating mode.
4. Define other bond parameters as necessary.
5. Make sure that the bond interface is working correctly.

**Note** - Before running the CLI commands, make sure that the slave interfaces do not have an IP Address already assigned.

### 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.

**Description**  
Use these commands to configure link aggregation.
Syntax

add bonding group <Bond ID> interface <Slave>
delete bonding group <Bond ID> interface <Slave>
set bonding group <Bond ID>
  primary VALUE
  mii-interval VALUE
  up-delay VALUE
  down-delay VALUE
  arp-polling-interval VALUE
  mode VALUE
  lacp-rate VALUE
  xmit-hash-policy VALUE
show bonding group <Bond ID>
show bonding groups

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Bond ID&gt;</td>
<td>ID of bond, an integer between 1 and 1024</td>
</tr>
<tr>
<td>&lt;Slave&gt;</td>
<td>Slave interface name</td>
</tr>
<tr>
<td>primary</td>
<td>Name of primary slave interface</td>
</tr>
<tr>
<td>mii-interval</td>
<td>Frequency that the system polls the Media Independent Interface (MMI) to get status</td>
</tr>
<tr>
<td>up-delay</td>
<td>Waiting time to confirm the slave interface status before taking the specified action (0-5000 ms default = 200 ms).</td>
</tr>
<tr>
<td>down-delay</td>
<td>Waiting time to confirm the slave interface status before taking the specified action (0-5000 ms default = 200 ms).</td>
</tr>
<tr>
<td>arp-polling-interval</td>
<td>Frequency of ARP requests sent to confirm a that slave interface is up</td>
</tr>
<tr>
<td>mode</td>
<td>Bond interface operating mode:</td>
</tr>
<tr>
<td></td>
<td>- round-robin: Selects the active slave interface sequentially.</td>
</tr>
<tr>
<td></td>
<td>- active-backup: If the active slave interface goes 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.</td>
</tr>
<tr>
<td></td>
<td>- xor: Selects the algorithm for slave selection according to the TCP/IP layer.</td>
</tr>
<tr>
<td></td>
<td>- 8023AD: 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.</td>
</tr>
<tr>
<td>lacp-rate</td>
<td>Sets the LACPDU packet transmission rate</td>
</tr>
<tr>
<td>xmit-hash-policy</td>
<td>Selects the algorithm for slave selection according to the specified 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
arp-polling-interval 0
Bond Interfaces
eth2
eth3
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.

Creating or Deleting a Bond Interface

To add a new bond interface:

Run `add bonding group <Bond_id>`.

*<Bond ID>* - Bond name (integer between 1 and 1024)

Example:

`add bonding group 777`

To delete a bond interface:

1. Make sure that you remove all slave interfaces from the bond.
2. Run `delete bonding group <bond_id>`.

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.

Defining the Bond Operating Mode

You can define bond interfaces using one of these operating modes:

- **Round Robin** - Selects the active slave interface sequentially.
- **Active/Backup** - If the active slave interface goes down, the connection automatically fails over to the primary slave interface. If the primary slave interfaces is not available, the connection fails over to a different slave.
- **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.

To define the bond operating mode:

Run `set bonding group <Bond_id> mode <mode>`.

*<Bond ID>* - Bond name

*Mode* - One of these key words:

- `round-robin`
- `active-backup`
- `xor`
- `8023AD`

The default is `active-backup`

Example:

`set bonding group 777 mode round-robin`

Defining Slave 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, run:

```
add bonding group <Bond ID> interface <IF Name>
```

*<Bond ID>* - Bond name

*<IF Name>* - Slave interface name
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, run:**
delete bonding group <Bond ID> interface <IF Name>

**Example:**
delete bonding group 777 interface eth4

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

**Defining the Primary Slave Interface**

When using 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, run:**
set bonding group <Bond ID> primary <IF>

- **Bond ID** - Bond name
- **IF** - Interface name

**Example**
set bonding group 777 primary eth4

**Defining the Media Monitoring Interval**

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

**To configure the MMI, run:**
set bonding group <Bond ID> mii-interval <Interval>

- **Bond ID** - Bond name
- **Interval** - Frequency range (1-5000 ms default = 100 ms)

**Example:**
set bonding group 777 mii-interval 500

**To disable MMI monitoring, run:**
set bonding group <Bond ID> mii-interval 0

**Defining the ARP monitoring interval**

This defines the frequency of ARP requests sent to confirm that a slave interface is up. ARP requests are sent to as many as five external MAC addresses.

**To configure the ARP interval, run:**
set bonding group <Bond ID> arp-polling-interval <Interval>

- **Bond ID** - Bond name
- **Interval** - Frequency (1-5000 ms default = 100 ms)

**Example:**
Set bonding group 777 arp-polling-interval 500

To disable the ARP interval, run:
set bonding group <Bond ID> arp-polling-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.

To configure the UP and Down delay times, run:
set bonding group <Bond ID> down-delay <Delay time>
set bonding group <Bond ID> up-delay <Delay time>

- **Bond ID** - Bond name
- **Delay Time** - Delay (0-5000 ms default = 200 ms)

Example:
set bonding group 777 down-delay 500

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

- **LACP Rate** - This parameter sets the LACPDU packet transmission rate.
- **Transmit Hash Policy** (802.3ad only) - This parameter selects the algorithm for slave selection according to the specified TCP/IP layer.

To set the LACP rate, run
set bonding group <Bond ID> lacp-rate [slow | fast]

- **Bond ID** - Bond name
- **Fast** - LACPDU packets sent every second
- **Slow** - LACPDU packets sent every 30 seconds

Example:
set bonding group 777 lacp-rate

To set the Transmit Hash Policy, run:
set bonding group <Bond ID> xmit-hash-policy <layer>

- **Bond ID** - Bond name
- **Layer** - TCP/IP layer
  - **layer2** - Uses XOR of the physical interface MAC address
  - **layer3+4** - Uses upper layer protocol information

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

Making Sure that Link Aggregation is Working
To make sure that a link aggregation is working for a specified bond interface, run this command from the expert mode:
cat /proc/net/bonding/<Bond ID>

Example with output:
### 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. The interfaces then send traffic using Layer-2 addressing. You can configure some interfaces as bridge interfaces, while other interfaces on the same device work as layer-3 devices. 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**.

#### Configuring Bridge Interfaces - CLI (bridging)

This is a quick reference for bridge interface commands. The next section is procedures for different tasks, with configuration options.

**Description** Use these commands to configure bridge interfaces.

**Syntax**

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

**Values**

<table>
<thead>
<tr>
<th>&lt;Group Name&gt;</th>
<th>Name of bridging group</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IF&gt;</td>
<td>Interface name</td>
</tr>
</tbody>
</table>

**Example**

- `set bridging group 666 interface eth1`
**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.

**Configuration using the CLI**

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

**To create a new bridge interface:**

Run:
```
add bridging group <Group Name> interface <IF>
```
- `<Group Name>` - Bridging Group name (unique integer between 0 and 1024)
- `<IF>` - Physical interface name

Run this command once for each physical interface included in the bridge interface.

**To delete a bridge interface:**

1. Run:
```
delete bridging group <Group Name> interface <IF>.
```
   This command deletes the physical interface. Run this command once for each physical interface included in the bridge interface.

2. Run:
```
delete bridging group <Group Name>.
```
   This command deletes the bridge interface itself.

**To add or change a bridge interface IP address:**

- For an IPv4 IP address, run
```
set interface <Group Name> ipv4-address <IP> subnet-mask <Mask>.
```
- For an IPv6 IP address, run
```
set interface <Group Name> ipv6-address <IP> mask-length <Prefix>.
```
  - `<Group Name>` - Bridging group name
  - `<IP>` - IP address - IPv4 or IPv6 as required
  - `<Mask>` - IPv4 subnet mask in dotted decimal format
  - `<Prefix>` - IPv6 prefix length

  Example:
```
set interface 777 ipv6-address 3000:40::1 mask-length 64
```

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

**Parameters and Values**

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

A Virtual Tunnel Interface (VTI) is a virtual interface on a Security Gateway that is related to an existing, Route Based VPN tunnel. The Route Based VPN tunnel works as a point-to-point connection between two peer Security Gateways in a VPN community. 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 **R75.40 VPN Administration Guide** ([http://supportcontent.checkpoint.com/solutions?id=sk67581](http://supportcontent.checkpoint.com/solutions?id=sk67581)).

**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 48) that includes the two peer Security Gateways.
4. Make Route Based VPN the default option ("Making Route Based VPN the Default Option" on page 48). Do this procedure one time for each Security Management server.
5. Define the VTI ("Configuring VPN Tunnel Interfaces" on page 48) 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 R75.40 VPN Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk67581).

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 Interface 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).
Configuring VPN Tunnel Interfaces - CLI (vpn tunnel)

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

Description
Add or delete a VPN Tunnel Interface (VTI)

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

delete vpn tunnel <Tunnel ID>
```

Parameters
- **type numbered**: Defines a numbered VTI that uses a specified, static IPv4 addresses for local and remote connections.
- **type unnumbered**: Defines an unnumbered VTI that uses the interface and the remote peer name to get addresses.
- **local**: Defines the local peer IPv4 address (numbered VTI only).
- **remote**: Defines the remote peer IPv4 address (numbered VTI only).
- **peer**: Remote peer name as defined in the VPN community. You must define the two peers in the VPN community before you can define the VTI. The Peer ID is an alpha-numeric character string.
- **dev**: Defines the interface (unnumbered VTI only).

Parameter Values
- **<Tunnel ID>**: Unique tunnel name (integer from 1 to 99). Gaia automatically adds the prefix 'vpnt' to the tunnel name.
  
  Example: vnpt10

- **<Local IP>**: Local peer IPv4 address (numbered VTI only) in dotted decimal format.

- **<remote IP>**: Remote peer IPv4 address (numbered VTI only) in dotted decimal format.

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

- **<IF>**: Local peer interface name (unnumbered VTI only).

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

Important
- After 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.
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</td>
<td>Any</td>
<td>accept</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MyIntranet &gt; Internal_Clear</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Internal_Clear &gt; MyIntranet</td>
<td></td>
<td></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 learn about configuring OSPF, see the R75.40 Gaia Advanced Routing Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk67581).

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.
6in4 Tunnel Interfaces

**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.

6in4 is a transparent mechanism that transmits IPv6 traffic on existing IPv4 networks. To do this, 6in4 does these functions:

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

The workflow for configuring 6in4 tunnels is:

1. Select the physical interface assigned to the tunnel.
2. Define the tunnel.
3. Select the remote host or router that connects to the tunnel.
4. Start the tunnel.
5. Optional: Assign an IPv6 address and mask length to the tunnel.

You must do this procedure for the <tp_gaia>gateway and the remote host.

**Configuring 6in4 Tunnel interfaces - WebUI**

**To add a 6in4 tunnel interface**

1. In the navigation tree, select **Interface Management > Network Interfaces**.
2. Click **Add 6in4 Tunnel**.
   - The **Add 6in4 Tunnel** window opens.
3. In the **6in4 Tunnel** tab, select the physical **Interface** which will forward the 6in4 tunnel frames.
   - The local address of the tunnel is the IPv4 address of the physical interface.
4. Set a **Tunnel ID**. The ID must be unique for all 6in4 tunnel that terminate on this Gaia system. Maximum value is 4096.
5. Set a the **TTL**. The Time To Live for tunnel data. The TTL field in packets through the tunnel is reduced by one on every router hop. Maximum value is 255.
6. Set the **Remote Address**. The IPv4 address at the remote end of the tunnel to which IPv6 packets are sent.
7. **Enable** the 6in4 tunnel interface.
8. **Optional**: Define an IPv6 address for the local end of the tunnel.
   - **Note** - IPv6 must be enabled. To enable IPv6, go to **System Management > System Configuration**.
     - a) In the **IPv6** tab, set the **IPv6 Address**.
     - b) Set a **Mask Length**. The number of bits in the subnet mask in CIDR notation.

The 6in4 interface name is **sit_6in4_<tunnel ID>**. For example, the name of a 6in4 interface with a tunnel ID of 5 is **sit_6in4_5**.

**To delete a 6in4 tunnel interface**

1. In the navigation tree, select **Interface Management > Network Interfaces**.
2. Select an interface of Type **6in4 Tunnel**.
3. Click **Delete**.

**Configuring 6in4 Tunnel Interfaces - CLI (interface)**

**Description**    Add, configure, monitor, and delete 6in4 tunnel interfaces.
Syntax

To add a 6in4 tunnel interface
add interface VALUE 6in4 VALUE remote VALUE ttl VALUE

For example
add interface eth0 6in4 2 remote 192.0.2.4 ttl 33

To monitor the 6in4 tunnel interface
show interface VALUE 6in4s

To configure an IPv6 address for a 6in4 tunnel interface
set interface VALUE ipv6-address VALUE mask-length VALUE

For example
set interface sit_6in4_3 ipv6-address 2001:DB8::333 mask-length 24

To delete a 6in4 tunnel interface
delete interface VALUE 6in4 VALUE

For example
delete interface eth0 6in4 3

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface VALUE</td>
<td>The physical interface which forwards the 6in4 tunnel frames, or the tunnel interface.</td>
</tr>
<tr>
<td>6in4 VALUE</td>
<td>The tunnel ID. The ID must be unique for all 6in4 tunnel that terminate on this Gaia system. Maximum value is 4096.</td>
</tr>
<tr>
<td>remote VALUE</td>
<td>The IPv4 address at the remote end of the tunnel to which IPv6 packets are sent.</td>
</tr>
<tr>
<td>ttl VALUE</td>
<td>The Time To Live for tunnel data. The TTL field in packets through the tunnel is reduced by one on every router hop. Maximum value is 255.</td>
</tr>
<tr>
<td>ipv6-address VALUE</td>
<td>Optional: Define an IPv6 address for the local end of the tunnel.</td>
</tr>
<tr>
<td>mask-length VALUE</td>
<td>The number of bits in the subnet mask in CIDR notation.</td>
</tr>
</tbody>
</table>

Example

show interface eth0 6in4s

Output

gw-940222> show interface eth0 6in4s
Tunnel ID sit_6in4_3
    local 192.0.2.201
    remote 192.168.0.32
    ttl 24

Comments

To save changes you must run save config

**PPPoE Interfaces**

**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.

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with DSL services where individual users connect to the DSL modem over Ethernet and in plain Metro Ethernet networks.
Configuring PPPoE Interfaces - WebUI

To add a PPPoE interface
1. In the navigation tree, select Interface Management > Network Interfaces.
2. Click Add and select PPPoE.
   The Add PPPoE page opens.
3. In the PPPoE tab, set the PPPoE ID. This ID must be unique for all PPPoE interfaces that terminate on this Gaia system. Maximum value is 999.
4. Select the the Interface. This is the physical Interface which will forward PPPoE frames.
5. Set the User Name and Password. The User name and password are needed to connect to the PPPoE server at the Internet Service Provider (ISP). Get them from the ISP.
6. Optional: Select Use Peer DNS. This allows the ISP to define the IPv4 DNS server for the Gaia system. The ISP supplies either one IPv4 DNS server (the Primary) or two (Primary and Secondary).

   Note - If you select Use Peer DNS, the IPv4 DNS servers configured in Network Management > Hosts and DNS are overwritten by the PPPoE Peer DNS servers.
7. Optional: Select Use Peer as Default Gateway. This makes the ISP server the Default Gateway for the Gaia system.

   Note - If you select Use Peer as Default Gateway the Default Gateway configured in Network Management > IPv4 Static Routes is not used.

To delete a PPPoE tunnel interface
1. In the navigation tree, select Interface Management > Network Interfaces.
2. Select an interface of Type PPPoE.
3. Click Delete.

Configuring PPPoE Interfaces - CLI (pppoe)

Description  Add, configure, monitor, and delete PPPoE interfaces.

Syntax

To add a PPPoE Interface
add pppoe client id VALUE interface VALUE user-name VALUE password VALUE use-peer-dns VALUE use-peer-as-default-gateway VALUE

For example:
add pppoe client id 2 interface eth0 user-name aaaa password aa use-peer-dns on use-peer-as-default-gateway on

To configure a PPPoE Interface
set pppoe client id VALUE
   interface VALUE
   password VALUE
   use-peer-as-default-gateway VALUE
   use-peer-dns VALUE
   user-name VALUE

To monitor a PPPoE Interface
show pppoe client id VALUE

For example
show pppoe client id 2

To delete a PPPoE Interface
delete pppoe client id VALUE
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client id VALUE</td>
<td>This ID must be unique for all PPPoE interfaces that terminate on this Gaia system. Maximum value is 999.</td>
</tr>
<tr>
<td>interface VALUE</td>
<td>This is the physical Interface which will forward PPPoE frames.</td>
</tr>
<tr>
<td>user-name VALUE</td>
<td>The User name and password are needed to connect to the PPPoE server at the Internet Service Provider (ISP). Get them from the ISP.</td>
</tr>
<tr>
<td>password VALUE</td>
<td></td>
</tr>
<tr>
<td>use-peer-dns VALUE</td>
<td>This allows the ISP to define the IPv4 DNS server for the Gaia system. The ISP supplies either one IPv4 DNS server (the Primary) or two (Primary and Secondary).</td>
</tr>
<tr>
<td>use-peer-as-default-gateway VALUE</td>
<td>This makes the ISP server the Default Gateway for the Gaia system.</td>
</tr>
</tbody>
</table>

**Note** - If you select Use Peer DNS, the IPv4 DNS servers configured in Network Management > Hosts and DNS are overwritten by the PPPoE Peer DNS servers.

**Note** - If you select Use Peer as Default Gateway the Default Gateway configured in Network Management > IPv4 Static Routes is not used.

#### Example

```
show pppoe client id 2
```

#### Output

```
Client ID:2
Client Name:pppoe2
Client User Name:aaaa
Client Password:**
Client Interface:eth0
Use Peer As Default Gateway:on
Use Peer DNS:on
Client Status:Connecting...
```

#### Comments

To save changes you must run `save config`

### 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 Interface Management > ARP page.
2. If you are in the Static Arp topic, click Related Topics: Dynamic ARP

**To show static ARP entries**

1. In the WebUI, go to the Interface Management > ARP page.
2. If you are in the Dynamic Arp topic, click Related Topics: Static ARP

**To change Static and dynamic ARP parameters**

1. In the WebUI, go to the Interface Management > ARP page.
2. If you are in the Dynamic Arp topic, click Related Topics: Static ARP
3. In the **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
   
   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 **Interface Management > ARP** page.
2. If you are in the **Dynamic Arp** topic, click Related Topics: Static ARP
3. Click **Add**.
4. Enter the **IP Address** of the static ARP entry and the **MAC Address** used when forwarding packets to
   the IP address.
5. Click **OK**.

**To delete a Static ARP entry**
1. In the WebUI, go to the **Interface Management > ARP** page.
2. If you are in the **Dynamic Arp** topic, click Related Topics: Static ARP
3. Select a Static ARP entry
4. Click **Remove**.

**To flush all dynamic ARP entries**
1. In the WebUI, go to the **Interface Management > ARP** page.
2. If you are in the **Static Arp** topic, click Related Topics: Dynamic ARP
3. 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></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>static</strong></td>
<td>Configured static arp entries</td>
</tr>
<tr>
<td><strong>dynamic</strong></td>
<td>Configured dynamic arp entries</td>
</tr>
<tr>
<td><strong>ipv4-address</strong></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><strong>macaddress</strong></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><strong>table validity-timeout</strong></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><strong>table cache-size</strong></td>
<td>This is the maximum number of entries in the arp cache. Default: 1024, Range: 1024-16384</td>
</tr>
</tbody>
</table>

**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.

### 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 **Interface 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
```
### Parameters

<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. 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.</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 (Domain Name Service) 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 Interface 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 To set the host name:
set hostname VALUE
To show the host name:
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 Interface 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 Interface 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 Interface Management > Hosts and DNS page.
2. In the Hosts section, select a host and click Delete.

**Configuring Hosts - CLI (host)**

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

**Syntax**
To add a host name and address:
add host name VALUE ipv4-address VALUE
add host name VALUE ipv6-address VALUE

To edit the name and IPv4 or IPv6 address of a host:
set host name VALUE ipv4-address VALUE
set host name VALUE ipv6-address VALUE

To delete a host name and address:
delete host name VALUE ipv4
delete host name VALUE ipv6

To show an IPv4 or IPv6 host address:
show host name VALUE ipv4
show host name VALUE ipv6

To show all IPv4 or IPv6 hosts:
show host names ipv4
show host names ipv6
### 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 Interface 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**. A search list for host-name lookup. The search is normally determined from the local domain name. By default, it contains only 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).

   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 of the Primary DNS Server**. The server to use when resolving hostnames. This should be a host running a DNS server

   c) (Optional) **IPv4 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 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>primary</td>
<td>The server to use when resolving hostnames. This should be a host running a DNS server.</td>
</tr>
<tr>
<td>secondary</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.</td>
</tr>
<tr>
<td>tertiary</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.</td>
</tr>
<tr>
<td>suffix</td>
<td>A search list for host-name lookup. The search is normally determined from the local domain name. By default, it contains only 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). 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>
<tr>
<td>VALUE</td>
<td>An IPv4 address</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 **Static Routes**.
2. In the **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. In the **Add** (or **Edit** **Interface Gateway** window, enter the IP address or interface name.
8. 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
**Network Management**

**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

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

**Parameter**

<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 <strong>gateway</strong>, <strong>blackhole</strong> or <strong>reject</strong>.</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 <strong>rank</strong> keyword in place of the <strong>nexthop</strong> keyword with no other parameters.</td>
</tr>
</tbody>
</table>
### Values

<table>
<thead>
<tr>
<th></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 default 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

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

### Comments

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

```
show route static
```

### CLI Procedures

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

#### To show static routes, run

```
show route static
```

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Connected</td>
</tr>
<tr>
<td>S</td>
<td>Static</td>
</tr>
<tr>
<td>R</td>
<td>RIP</td>
</tr>
<tr>
<td>B</td>
<td>BGP</td>
</tr>
<tr>
<td>O</td>
<td>OSPF IntraArea (IA), InterArea (E), External (N), NSSA</td>
</tr>
<tr>
<td>A</td>
<td>Aggregate</td>
</tr>
<tr>
<td>K</td>
<td>Kernel Remnant</td>
</tr>
<tr>
<td>H</td>
<td>Hidden</td>
</tr>
<tr>
<td>P</td>
<td>Suppressed</td>
</tr>
</tbody>
</table>

```
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 IP> 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
```

**Parameter**

<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<br>reject - Drops packets and sends an error message to the traffic source<br>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</td>
</tr>
<tr>
<td>S</td>
<td>Static</td>
</tr>
<tr>
<td>B</td>
<td>BGP</td>
</tr>
<tr>
<td>Rg</td>
<td>RIPng</td>
</tr>
<tr>
<td>A</td>
<td>Aggregate</td>
</tr>
<tr>
<td>O</td>
<td>OSPFv3 IntraArea (IA - InterArea, E - External)</td>
</tr>
<tr>
<td>K</td>
<td>Kernel Remnant</td>
</tr>
<tr>
<td>H</td>
<td>Hidden</td>
</tr>
<tr>
<td>P</td>
<td>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
```

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

- **Destination** - Destination IPv6 address.
- **GW IP** - Next hop gateway IPv6 address.
- **GW IF** - Next hop gateway interface name.

Example:

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

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

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

- **Destination** - Destination IP address.
- **GW IP** - Next hop gateway IP address.
- **P Value** - Integer between 1 and 8 (default =1)

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

Example:

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

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

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

- **Destination** - Destination IP address.
- **Reject** - Drops packets and sends an error message to the traffic source.
- **Blackhole** - Drops packets, but does not send an error message.

Examples:

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

```
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
```

## IPv6 Neighbor-Entry

The neighbor-entry feature adds and deletes IPv6 neighbor discovery entries (from where? the kernel tables??). Neighbor entries can be added or deleted only through the command line.

- **To Add a neighbor entry**
  
  **Description** Use this command to define the IPv6 address of a new static Neighbor Discovery entry.

  **Syntax**
  ```
  add neighbor-entry ipv6-address VALUE macaddress VALUE interface VALUE
  ```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-address</td>
<td>Enter the IPv6 address</td>
</tr>
<tr>
<td>macaddress</td>
<td>Enter the MAC address</td>
</tr>
<tr>
<td>interface</td>
<td>Enter the interface</td>
</tr>
</tbody>
</table>

- **To delete a neighbor entry**
  
  **Description** Use this command to delete the IPv6 address of a static Neighbor Discovery entry.

  **Syntax**
  ```
  delete neighbor-entry ipv6-address VALUE interface VALUE
  ```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-address</td>
<td>Enter the IPv6 address</td>
</tr>
<tr>
<td>interface</td>
<td>Enter the interface</td>
</tr>
</tbody>
</table>
Chapter 6

System Management

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 <strong>On</strong> or <strong>Off</strong>.</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**
To show the system date and time:
```
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**
To set the system date:
```
set date <date>
```

To show the 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**
To set the time:
```
set time <time of day>
```

To show the time:
```
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**

To set the time zone:

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

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

To show the time zone:

```
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, Etc, Europe, Indian, Pacific</td>
</tr>
<tr>
<td>&lt;Region&gt;</td>
<td>Region within the specified area.</td>
</tr>
</tbody>
</table>

**Example**

Set Time Zone America /Detroit

## 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 MIB (GaiaTrapsMIB)</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).
**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>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.</td>
</tr>
</tbody>
</table>

This trap works only if RAID is supported on the Gaia appliance or computer. To make sure that RAID monitoring is supported, run the command raid_diagnostics and confirm that it shows the RAID status.

Configuring SNMP - WebUI

To enable SNMP:

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

5. In **SNMP Contact String**, enter a string that contains the contact information for the device. The maximum length for the string is 128 characters. That includes letters, numbers, spaces, special characters. For example: John Doe, Network Administrator, (111) 222-3333

6. Click **Apply**.

**To set an SNMP agent address:**

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.](image)

**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.](image)

**To add a USM user:**

1. In the tree view, click **System Management > SNMP**.
2. Below **V3 - User-Based Security Model (USM)**, click **Add**. The **Add New USM User** window opens.
3. In **User Name**, The range is 1 to 31 alphanumeric characters with no spaces, backslash, or colon characters. This can be the same as a user name for system access.
4. In **Security Level**, select from the drop down list:
   - **authPriv**—The user has authentication and privacy pass phrases and can connect with privacy encryption.
   - **authNoPriv**—The user has only an authentication pass phrase and can connect only without privacy encryption.
5. In **User Permissions**, select the privileges for the user:
   - **Read-only**
   - **Read-write**
6. In **Authentication 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** window opens.
3. The window shows this message: *Are you sure you want to delete "IPv4 address" entry? Click Yes.*

---

**Configuring SNMP - CLI (snmp)**

<table>
<thead>
<tr>
<th>Description</th>
<th>Use These commands to configure SNMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>Enable SNMP</td>
</tr>
<tr>
<td></td>
<td>Set Commands:</td>
</tr>
<tr>
<td></td>
<td><code>set snmp agent VALUE</code></td>
</tr>
<tr>
<td></td>
<td><code>set snmp agent-version VALUE</code></td>
</tr>
<tr>
<td></td>
<td><code>set snmp location VALUE</code></td>
</tr>
<tr>
<td></td>
<td><code>set snmp contact VALUE</code></td>
</tr>
<tr>
<td></td>
<td>Show Commands:</td>
</tr>
<tr>
<td></td>
<td><code>show snmp agent</code></td>
</tr>
<tr>
<td></td>
<td><code>show snmp agent-version</code></td>
</tr>
<tr>
<td></td>
<td><code>show snmp location</code></td>
</tr>
<tr>
<td></td>
<td><code>show snmp contact</code></td>
</tr>
<tr>
<td></td>
<td>Delete Commands:</td>
</tr>
<tr>
<td></td>
<td><code>delete snmp location</code></td>
</tr>
<tr>
<td></td>
<td><code>delete snmp contact</code></td>
</tr>
</tbody>
</table>
SNMP Agent Address

Add commands:
add snmp address VALUE

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.

⚠️ **Important** - We do not recommend the following command because passwords are stored as plain text in the command history:

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

⚠️ **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 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 password 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>An 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>community VALUE read-only</td>
<td>Set a string. This is a basic security precaution. The default is public.</td>
</tr>
<tr>
<td>community VALUE read-write</td>
<td>Set a string (optional).</td>
</tr>
</tbody>
</table>
usm user | The range is 1 to 31 alphanumeric characters with no spaces, backslash, or colon characters. This can be the same as a user name for system access.

authNoPriv | The user has only an authentication pass phrase and can connect only without privacy encryption. A user is always created with read-only privilege. This can be changed using the command `set snmp usm user <name> <usm-read-only / usm-read-write>`

authPriv | The user has authentication and privacy pass phrases and can connect with privacy encryption. A user is always created with read-only privilege. This can be changed using the command `set snmp usm user <name> <usm-read-only / usm-read-write>`

auth-pass-phrase | A password for the user that is between 8 and 128 characters in length.

auth-pass-phrasehashed | A hashed password which is the output of the command `show configuration snmp`

privacy-pass-phrase | A pass phrase that is between 8 and 128 characters in length. Used for protection against disclosure of SNMP message payloads.

privacy-pass-phrasehashed | A hashed password which is the output of the command `show configuration snmp`

usm users | All USM users

traps receiver | IP address selected to receive traps sent by the agent.

community | Set a string

traps trap | The trap name

polling-frequency | The polling frequency in seconds. Default is 20 seconds.

trap-user | The user which generates the traps.

Example

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

Output

```
authorizationError
```

Comments

- CLI only displays the enabled traps. For all trap types, see table in Configuring SNMP - WebUI (on page 77).
- 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 the following five: value, unSpecified, noSuchObject, noSuchInstance, and 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 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 OBJECT IDENTIFIER prefix that exactly</td>
</tr>
<tr>
<td></td>
<td>matches the prefix of any variable accessible by this request, its value</td>
</tr>
<tr>
<td></td>
<td>field is set to noSuchObject.</td>
</tr>
<tr>
<td>noSuchInstance</td>
<td>If the variable's name does not exactly match the name of a variable, its</td>
</tr>
<tr>
<td></td>
<td>value field is set to noSuchInstance.</td>
</tr>
<tr>
<td>genErr</td>
<td>If the processing of a variable fails for any other reason, the responding</td>
</tr>
<tr>
<td></td>
<td>entity returns genErr and a value in the error-index field that is the index</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>exceeds a local limitation or the maximum message size of the request's</td>
</tr>
<tr>
<td></td>
<td>source party, then the response PDU is discarded and a new response PDU</td>
</tr>
<tr>
<td></td>
<td>is constructed. The new response PDU has an error-status of tooBig, an</td>
</tr>
<tr>
<td></td>
<td>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 by letting an SNMPv2 manager request that the response be as large as possible given the constraints on the message size.

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 88).

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 job VALUE recurrence system-startup`
- `set cron mailto VALUE`

To monitor and troubleshoot the job scheduler configuration:
- `show cron job VALUE command`
- `show cron job VALUE recurrence`
- `show cron jobs`
- `show cron mailto`
### Parameters

<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>
<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>recurrence system-startup</td>
<td>Specify a job that will run at every system startup.</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. |
| time            | To specify the time, enter the time in the twenty four hour clock format. For example: 14:00. |
| mailto          | To specify a mail recipient, enter the email address. One email address per command. You must also configure a mail server ("Configuring Mail Notification - CLI (mail-notification)" on page 88). |

### Comments

Only Show commands provide an output.

---

### Mail Notification

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

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

Gaia supports these mail notification features:

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

Gaia does not support these mail notification features:

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

### Configuring Mail Notification - WebUI

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

### Configuring Mail Notification - CLI (mail-notification)

**Description**
Use this group of commands to configure mail notifications.

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

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

To view the mail server and user configurations:

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

<table>
<thead>
<tr>
<th>Parameter</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: <code>mail.company.com</code></td>
</tr>
<tr>
<td>username</td>
<td>The username on the mail server that receives the admin or monitor mail notifications. For example: <code>user@mail.company.com</code></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>Banner Message</th>
<th>Message of the Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Message: &quot;This system is for authorized use only&quot;</td>
<td>&quot;You have logged into the system&quot;</td>
</tr>
</tbody>
</table>

- **WebUI**
  - **When shown in WebUI**: Browser login page, before logging in
  - **When shown in clish**: When logging in, before entering the password

- **Default state**
  - **Enabled**: After logging in to the system

### 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>inactivity-timeout</td>
<td>The inactivity timeout (in minutes) for the command line.</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 product.
2. Install an IPv6 license on the Security Management server and enable it.
3. Create IPv6 objects in SmartDashboard.

Configuring the IPv6 Support - WebUI

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

Configuring the 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>syslog</td>
<td>Configures the system logging.</td>
</tr>
<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>
</tbody>
</table>
### Parameter Values

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;remote ip&gt;</td>
<td>IP address of remote computer.</td>
</tr>
</tbody>
</table>
| <severity> | syslog severity level. These are the legal values:  
  - emerg  
  - alert  
  - crit  
  - err  
  - warning  
  - notice  
  - info  
  - debug  
  - all |
| <file> | System log file name. |

**Example**

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

**Comments**

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

---

**Configuring Log Volume - CLI (volume)**

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

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

#### To show log partition usage, run:

**Syntax:**

```
show volume logs
```

**Output:**

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

#### To enlarge the log partition, run:

**Syntax:**

```
set volume VALUE size VALUE
```

**Example:**

```
set volume logs size 4
```

**Output:**

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

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

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

Y

This operation may take several minutes...
**Comments**

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

**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-certificate cert-file VALUE key-file VALUE passphrase VALUE`
- `set web ssl-certificate cert-file VALUE key-file VALUE prompt-passphrase`
- `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:
set web daemon-enable on | off

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>daemon-enable VALUE</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 VALUE</td>
<td>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</td>
</tr>
</tbody>
</table>

Setting a web SSL certificate

Use these command to set (define) a web SSL certificate, the certificate that authenticates the WebUI server to the browser.

Description

Use these commands to define the server certificate

Syntax

```
set web ssl-certificate cert-file VALUE key-file VALUE passphrase VALUE
set web ssl-certificate cert-file VALUE key-file VALUE prompt-passphrase
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cert-file VALUE</td>
<td>Enter the full path to the certificate file, for example: /usr/my_cert.crt</td>
</tr>
<tr>
<td>passphrase VALUE</td>
<td>Enter a password that lets you view the contents of the server certificate</td>
</tr>
<tr>
<td>key-file VALUE</td>
<td>Enter the full path to the key file, for example: /user/my_key.key</td>
</tr>
</tbody>
</table>

Comments

Obtain the certificate from the Internal Certificate Authority (ICA) of the Security Management server or an external certificate authority, such as VeriSign.

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
```

<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>
Description Specifies the port number on which the WebUI can be accessed when using SSL-secured connections

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 timeout

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 VALUE</td>
<td>The IPv4 address of the allowed host</td>
</tr>
<tr>
<td>mask-length VALUE</td>
<td>The mask-length of the allowed network</td>
</tr>
</tbody>
</table>

Example
- `add allowed-client host any-host`

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

gw-gaia> show allowed-client all

<table>
<thead>
<tr>
<th>Type</th>
<th>Address</th>
<th>Mask Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Any</td>
<td></td>
</tr>
</tbody>
</table>

gw-gaia>
```
Chapter 7

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)
  - Source-Specific Multicast (SSM)

IGMP

To learn about dynamic routing, see the R75.40 Gaia Advanced Routing Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk67581).
Chapter 8

User Management

In This Chapter

- Change My Password
- Users
- Roles
- Password Policy
- Authentication Servers
- System Groups
- GUI Clients

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 be 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.

Warning - A user with read and write permission to the Users feature can change the password of another user, or an admin user. Therefore, write permission to the Users feature should be assigned with caution.

Managing User Accounts - WebUI

To see a list of all users
Choose User Management > Users in the navigation tree.
You can also see your username in the toolbar of the WebUI.

To add a user
1. Open the User Management > Users page.
2. Click Add
3. In the Add User page, enter the following:
   • Login Name - (1–31 characters),
   • Home Directory - for the new user. Must be subdirectory of /home
   • Password.
   • Confirm Password
4. Click OK

To delete a user
1. Open the User Management > Users page.
2. Select the User
3. Click Delete.
### User Account Fields- WebUI

<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 (_). <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.  
  • `/sbin/nologin` - User is not allowed to log in.                                                                                                                                                                                                 |
| Reset Password     | Change the user password. **Important** - After resetting the password, tell the user to immediately change their password in User Management > Change My Password.                                                                                                                                                                      |
| Password           | Use this field to enter a new password if you are changing it. **Range:** 6-128 characters. All printable characters are allowed. **Note** - If you use an asterisk (*) in a password, users with that password are unable to log in.                                                                                                                                  |
| Confirm Password   | Re-enter the new password if you are changing it.                                                                                                                                                                                                                                                                                           |
| Access Mechanisms  | Choose whether the user is able to access Gaia from the command line, from the WebUI, both, or neither.                                                                                                                                                                                                                                                                                     |
| Roles              | Assign a role to the user. Define the roles in User Management > Roles.                                                                                                                                                                                                                                                                                                     |

**Managing User Accounts - CLI (user)**

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

To add user accounts:
add user <username> uid VALUE homedir

To modify user accounts:
set user <username>
gid VALUE
homedir VALUE
newpass VALUE
password
password-hash VALUE
realname VALUE
shell VALUE
uid VALUE

To delete an existing user:
delete user VALUE

To view configuration and conditions:
show users
show user <username>
gid
homedir
realname
shell
uid

Comments

You can use the add user command to add new users, but you must use the set user name passwd command to set the password and allow the user to log on to the system.

For information on removing access mechanism permissions from a user, see the delete rba user command.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user &lt;username&gt;</td>
<td>Specifies the new user name or an existing user name. The valid characters are alphanumeric characters, dash (-), and underscore (_). Range: 1-32 characters</td>
</tr>
<tr>
<td>gid VALUE</td>
<td>Specifies the ID (0-65535) for the primary group to which a user belongs. Use the group management commands to specify membership in other groups.</td>
</tr>
<tr>
<td>homedir VALUE</td>
<td>Specifies the user's home directory, where the user is placed on login. Enter the full Linux path name. If the directory does not already exist, it is created. The home directory for all users must be in a directory under /home/.</td>
</tr>
<tr>
<td>newpass VALUE</td>
<td>Specifies a new password for the user. If you use this keyword to change the password, you will not be asked to verify the new password and the password you enter is visible on the terminal and is stored as plain text in the command history.</td>
</tr>
<tr>
<td>password</td>
<td>Starts a password change dialog. You will be asked to enter a new password for the user and then asked to verify it by re-entering it. The password you enter will not be visible on terminal.</td>
</tr>
<tr>
<td>password-hash VALUE</td>
<td>An encrypted representation of the password. The password is not visible as text at the terminal 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 VALUE</td>
<td>User's real name or other informative label.</td>
</tr>
<tr>
<td>shell VALUE</td>
<td>Specifies the shell of the user, which is invoked when the user logs in. The default shell is /bin/csh. To change the shell, enter the new shell path name.</td>
</tr>
<tr>
<td></td>
<td>/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.</td>
</tr>
<tr>
<td></td>
<td>/bin/bash, /bin/csh, /bin/sh, /bin/tcsh - Standard Linux shells. To enter the clish shell, 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 VALUE</td>
<td>Unique user ID (Integer 0-65535). 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 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.

**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

```bash
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 &lt;List&gt;</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 &lt;List&gt;</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, revert,fcd
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 a role.

CLI Procedures

To define a new role or add features to an existing role:

Run:
```
add rba role <Name> domain-type System readonly-features <List> readwrite-features <List>
```
- `<role <Name>>` - Role name as a character string that contains letters, numbers or the underscore (_) character. The role name must with a letter.
- `<readonly-features <List>>` - Comma separated list of Gaia features that have read only permissions in the specified role.
- `<readwrite-features <List>>` - Comma separated list of Gaia features that have read/write permissions in the specified role.

To remove features from an existing role:

Run:
```
delete rba role <Name> readonly-features <List> readwrite-features <List>
```
- `<role <Name>>` - Role name as a character string that contains letters, numbers or the underscore (_) character. The role name must with a letter.
- `<readonly-features <List>>` - Comma separated list of Gaia features that have read only permissions in the specified role.
- `<readwrite-features <List>>` - Comma separated list of Gaia features that have read/write permissions in the specified role.

To assign or remove roles to a user:

Run:
```
add rba user <User Name> roles <List>
delete rba user <User Name> roles <List>
```
- `<user <User name>>` - User to which access mechanism permissions and roles are assigned.
- `<roles <List>>` - Comma separated list of role names that are assigned to or removed from the specified user.

To Assign or remove access mechanisms (WebUI or CLI) for a user:

Run:
```
add rba user <User name> access-mechanisms [Web/UI | CLI]
delete rba user <User name> access-mechanisms [Web/UI | CLI]
```
- `<user <User name>>` - Comma separated list of role names that are assigned to or removed from the specified user.
- `<Web/UI>` - Add or remove permissions to use the WebUI.
- `<CLI>` - Add or remove permissions to use the Gaia CLI.

Password Policy

This section explains how to configure your platform to:

- Enforce creation of strong passwords.
Monitor and prevent use of already used passwords.

Force users to change passwords at regular intervals.

One of the important elements of securing your Check Point network security platform is to set user passwords and create a good password policy. Strong, unique passwords that use a variety of character types and require password changes, are key factors in your overall network security.

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 (on page 98) and Change My Password (on page 98).

Password History Checks

The password history feature checks for the reuse of passwords and forces users to use a new password each time 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 from before, 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.

Configuring Password Policy- WebUI

To Configure Password strength:

1. In the tree view, click User Management > Password policy.
2. In the Minimum Password Length field, enter the minimum number of characters to use in the password. The default is 6.
   
   Note - Does not apply to passwords that are already set.
3. You can Disallow Palindromes. A palindrome is a sequence of letters, numbers, or characters that are read the same in each direction. By default, it is selected.
4. In Password Complexity, select the required number of character types. The default is two character types.
5. Click Apply.
To configure password history check:
1. In the tree view, click User Management > Password policy.
2. Select Check for Password Reuse. By default, it is selected.
3. In History Length field, enter the number of former passwords to keep and examine against for each user. The range is 1-1000. The default is 10.
4. Click Apply.

To configure mandatory user password change
1. In the tree view, click User Management > Password policy.
2. For mandatory password change to work, you must enable Check for password Reuse.
3. Select one of:
   - Passwords never expire (the default)
   - Password expire after n days. Enter a number from 1-1827.
4. Click Apply.

**Configuring Password Policy- CLI (password-controls)**

**Description**
Use these commands to set a policy for managing user passwords. The features included in password and account management are a global and comprehensive way to manage password policy.

**Syntax**
To change password and account management configuration:

- `set password-controls complexity VALUE`
- `set password-controls history-checking VALUE`
- `set password-controls history-length VALUE`
- `set password-controls min-password-length VALUE`
- `set password-controls palindrome-check VALUE`
- `set password-controls password-expiration VALUE`

To view password and account management configuration:

- `show password-controls all`
- `show password-controls complexity`
- `show password-controls history-checking`
- `show password-controls history-length`
- `show password-controls min-password-length`
- `show password-controls palindrome-check`
- `show password-controls password-expiration`
User Management

Description
Use these commands to set a policy for managing user passwords. The features included in password and account management are a global and comprehensive way to manage password policy.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>complexity</td>
<td>The required number of character types. The range is 1-4. The default is 2.</td>
</tr>
<tr>
<td>history-checking</td>
<td>On or Off. On enables the history check.</td>
</tr>
<tr>
<td>history-length</td>
<td>The number of former passwords to keep and check against for each user. The range is 1-1000. The default is 10.</td>
</tr>
<tr>
<td>min-password-length</td>
<td>The minimum number of characters of a password. Does not apply to passwords that have already been set.</td>
</tr>
<tr>
<td>palindrome-check</td>
<td>A palindrome is a sequence of letters, numbers, or characters that are read the same in each direction. On or Off. On prevents passwords that are palindromes. The default is On.</td>
</tr>
<tr>
<td>password-expiration</td>
<td>The number of days after which a new password expires. The range is 1-1827. The default is never. When set to never, passwords do not expire. Does not apply to SNMP users.</td>
</tr>
</tbody>
</table>

Example

show password-controls all

Output

Password Strength
Minimum Password Length 6
Password Complexity 2
Password Palindrome Check on

Password History
Password History Checking on
Password History Length 10

Mandatory Password Change
Password Expiration Lifetime never

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

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.

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.

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.
3. In the Add New RADIUS Server window, enter or select a Priority value.
   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.
4. In the Host field, enter the RADIUS server host name or IP address.
   Note - IPv6 addresses are not supported for RADIUS servers.
5. In the UDP Port field, enter the RADIUS server UDP port. The default port is 1812 as specified by the RADIUS standard. The range of valid port numbers is 1 to 65535.
   Warning - Firewall software frequently blocks traffic on port 1812. Make sure that you define a firewall rule to allow port 1812 traffic between the RADIUS server and Gaia.
6. In the Shared secret field, enter 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. Some RADIUS servers have a maximum shared secret string length of 15 or 16 characters. See the documentation for your RADIUS server.
7. In Timeout in Seconds (optional), enter the timeout period in seconds. The default value is 3. If there is no response after the timeout period, Gaia tries to connect to a different server.
8. Click OK.

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, or the Timeout. You cannot change the Priority value.
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
add aaa radius-servers priority VALUE host VALUE [ port VALUE ] secret VALUE timeout VALUE
```

To delete a RADIUS configuration:

```
delete aaa radius-servers priority VALUE
```

To change the configuration of a RADIUS entry:

```
set aaa radius-servers priority VALUE host VALUE
set aaa radius-servers priority VALUE new-priority VALUE
set aaa radius-servers priority VALUE port VALUE
set aaa radius-servers priority VALUE prompt-secret
set aaa radius-servers priority VALUE secret VALUE
set aaa radius-servers priority VALUE timeout 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
show aaa radius-servers priority VALUE port
show aaa radius-servers priority VALUE timeout
```

**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>new-priority</td>
<td>The priority of the new RADIUS server</td>
</tr>
<tr>
<td>host</td>
<td>RADIUS server IP address in dot-delimited format.</td>
</tr>
<tr>
<td>port</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>prompt secret</td>
<td>Shared secret (password) text string. The system prompts you to enter the value.</td>
</tr>
<tr>
<td>timeout</td>
<td>The number of seconds to wait for the server to respond. The default value 3 seconds.</td>
</tr>
</tbody>
</table>
secret

The shared secret used to authenticate the RADIUS server and the local client. You must define this value on your RADIUS server.

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 103).

**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 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.

**Configuring TACACS+ Servers - WebUI**

**To configure a TACACS+ server:**

1. In the tree view, click User Management > Authentication Servers.
2. In the TACACS+ Server section:
   - **IPv4 Address:** The TACACS+ server IPv4 address.
   - **Password:** 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.
3. Click Apply.

**Configuring TACACS+ Servers - CLI (aaa)**

**Description**

Use the `aaa tacacs-servers` commands to configure one or more TACACS authentication servers.
Syntax

To change the configuration of a TACACS+ server entry:

```
set aaa tacacs-servers authentication server VALUE key VALUE
set aaa tacacs-servers authentication state On|off
```

To see a list of all TACACS+ servers

```
show aaa tacacs-servers
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server VALUE</td>
<td>The TACACS+ server IPv4 address.</td>
</tr>
<tr>
<td>key VALUE</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>
</tbody>
</table>
| state On|Off | On - Enable TACACS+ authentication  
Off - Disable TACACS+ authentication |

Example

```
set aaa tacacs-servers authentication server 10.10.10.99 key MySharedSecretKey
```

**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. You 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 temporarily grant administrators 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. For non-local Gaia users with different privilege, the admin can define roles with the name TACP-N, where N is a number from 1 to 15. Non-local Gaia users can changes their own privileges by moving to another TACP-N role. This requires a password.

**To configure Gaia as a TACACS+ Client:**

1. Define the role TACP-0
2. Define the features for the role.
   For instructions, see Roles (on page 103).
3. **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 privileges using the CLI:**

1. Connect to Gaia CLI as a TACACS+ user.
2. Enter the username and password of the user.
   After you are authenticated by the TACACs server, you will see the clish prompt. At this point you have the privileges of the TACP-0 role.
3. To raise the privileges to the \texttt{TACP-N} role (N is a number from 1 to 15), run:
   \texttt{tacacs_enable N}
4. Enter the password for the user.

**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 \texttt{TACP-N} role (N is a number from 1 to 15), click \texttt{Enable} at the top of the \texttt{Overview} page.
4. Enter the password for the user.

**Configuring TACACS+ Servers for Non-Local Users**

Non-local Gaia users can be defined on a TACACS server and not in Gaia. When a non-local user logs in to Gaia, the TACACS server authenticates the user and assigns the applicable permissions. You must configure the TACACS server to correctly authenticate and authorize non-local Gaia users.

\textbf{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 103).

All users are assigned by default to the \texttt{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 \texttt{users} group. The list of members of the \texttt{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
```

<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></td>
<td><strong>Note</strong> - 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.</td>
</tr>
<tr>
<td>member VALUE</td>
<td>Name of an existing user. For example, admin or monitor.</td>
</tr>
</tbody>
</table>

### 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.*
Chapter 9

High Availability

In This Chapter

- VRRP 117
- Advanced VRRP 126
- Troubleshooting VRRP 130

VRRP

VRRP (Virtual Routing Redundancy Protocol) is a cluster solution where two or more Gaia-based Security Gateways work together as one Security Gateway. You can configure your VRRP cluster for high availability and/or load sharing.

The Check Point VRRP implementation of includes additional functionality called Monitored Circuit VRRP. Monitored-Circuit VRRP prevents "black holes" caused by asymmetric routes created when only one interface on master router fails (as opposed to the master itself). Gaia releases priority over all interfaces on a virtual router to let failover occur.

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

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>(Virtual Router)</td>
<td>Cluster</td>
<td>A group of Security Gateways, with a unique group identifier, that gives redundancy and load sharing functionality. All members of a Virtual Router share a common IP address.</td>
</tr>
<tr>
<td>or VRRP Group</td>
<td></td>
<td></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 VRRP Groups.</td>
</tr>
<tr>
<td>Master</td>
<td>Primary (active) member</td>
<td>The VRRP router (Security Gateway) that handles traffic to and from a VRRP Group. The master is the VRRP router with the highest priority in a group. The master inspects traffic and enforces the security policy.</td>
</tr>
<tr>
<td>Backup</td>
<td>Backup (standby) member</td>
<td>A redundant VRRP router (Security Gateway) that is available to take over for the master in the event of a failure.</td>
</tr>
<tr>
<td>VRID</td>
<td></td>
<td>Unique VRRP Group (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>The IP address or addresses assigned to the VRRP Group (Virtual Router). These addresses are routable from internal and/or external network resources.</td>
</tr>
</tbody>
</table>
How VRRP Works

Each Virtual Router (VRRP Group) is identified by a unique virtual router ID (VRID) and one or more virtual router IP addresses. It is comprised of a master router and at least one backup router. If the master platform fails, VRRP specifies an election protocol that assigns a backup platform. The backup forwards IP traffic sent to the IP address of the virtual router.

The master sends periodic VRRP advertisements (also known as hello messages).

Gaia supports OSPF, BGP, RIP, and PIM (sparse and dense modes) to advertise the IP address of the VRRP virtual router. You must use monitored-circuit VRRP to configure virtual IP support for a Dynamic Routing protocol.

Note - Gaia also supports OSPF on VPN tunnels that stop at a VRRP group. Only active/passive VRRP environments are supported, active-active configurations are not.

The master is defined as the router with the highest Priority parameter. You define a priority for each platform when you create the VRID or add a platform to it. If two platforms have equivalent priorities, the platform that comes online and broadcasts VRRP advertisements first becomes the master.

Simple VRRP Configuration (platform A is the master, and platform B is the backup):

A VRRP router (a router that is running VRRP) might participate in more than one VRID. The VRID mappings and priorities are different for each VRID. You can create two VRIDs on the master and backup platforms. One VRID for connections with the external network, and one for connection with the internal network.
VRRP Configuration with Internal and External VRIDs:

In this example, Platform A acts as the master for VRID 1 and VRID 2, while Platform B acts as the backup for VRID 1 and VRID 2.

You can configure some platforms to be part of multiple VRIDs while they simultaneously back up each other. This is known as an active-active configuration.

VRRP Configuration with some Backups at the same time:

In this active-active configuration, two VRIDs are implemented on the internal network for load sharing. Platform A is the master for VRID 5, and is the default gateway for Host H1 and Host H2. Platform B is the master for VRID 7, and is the default gateway for Host H3 and Host H4. Platforms A and B are configured to back each other up. If one platform fails, the other takes its VRID and IP addresses. It supplies load balancing, full redundancy, and uninterrupted service to the default IP addresses.

**VRRP Methods**

You can configure VRRP using one of these procedures:

- **VRRP (Simple Monitored Circuit VRRP)**
  The simple Monitored Circuit VRRP configuration contains all of the basic parameters and is applicable for most environments.

- **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 it is necessary to monitor of each interface individually
  - You can change the VMAC assignment mode.
  For more information see Understanding Monitored-Circuit VRRP (on page 120).
You cannot use the easy and Advanced procedures to configure Monitored-Circuit VRRP on the same computer.

**Understanding Monitored-Circuit VRRP**

Monitored-circuit VRRP eliminates "black holes" caused by asymmetric routes that can be created if only one interface on the master fails (as opposed to the entire platform). Gaia does this by releasing priority over all of the interfaces in the virtual router to allow the backup to take over entirely.

To understand the advantage of monitored-circuit VRRP, consider the configuration pictured in . In this example, if you are using standard VRRPv2 and the external interface fails or becomes unreachable, the external virtual router fails over to the backup while the internal virtual router stays on the master. This can result in reachability failures, as the platform might accept packets from an internal end host but be unable to forward them to destinations that are reached through the failed interface to the external network.

Monitored-circuit VRRP monitors all of the VRRP-configured interfaces on the platform. If an interface fails, the master releases its priority over all of the VRRP-configured interfaces. This allows the backup platform to take over all of the interfaces and become master for both the internal and external VRID.

To release the priority, Gaia subtracts the priority delta, a Check Point-specific parameter that you configure when you set up the VRID, from the priority to calculate an effective priority. If you configure your system correctly, the effective priority is lower than that of the backup routers and, therefore, the VRRP election protocol is triggered to select a new master.

See Configuring Monitored-Circuit VRRP using the Simplified Method and Configuring Monitored-Circuit VRRP using the Full Method for configuration details.

**Before Configuring VRRP**

Do these steps before you define and create a VRRP Group.

1. Synchronize the system time on all of the VRRP Group members.
   - We recommend that you enable NTP (Network Time Protocol) on all members of a VRRP cluster.
   - You can also manually change the time and time zone on each member to match the other members.
   - You must synchronize member times to within a few seconds.

2. Add host names and IP address pairs to the host table on each VRRP member. This optional step lets you use host names as an alternative to IP addresses or DNS servers.

**Configuring Network Switches**

*Use PortFast with Spanning Tree Protocol*

If you use the Spanning Tree protocol on Cisco switches, in a network connected to Check Point systems that run VRRP, enable PortFast. PortFast sets interfaces to the Spanning-Tree forwarding state and not wait for the standard forward-time interval. If you use switches from a different vendor, use the equivalent feature supplied by that vendor.

If you use the Spanning Tree protocol without PortFast, or an equivalent feature, it can disrupt VRRP failovers.

*Do Not Cascade Switches*

Do not connect interfaces that are in the same VRRP virtual router to different cascaded switches. For example: do not use this configuration:

- Master node: Interface of virtual router 1 connected to switch A.
- Backup node: Interface of virtual router 1 connected to switch B.
- Switch A and switch B connected by an uplink connection.

This configuration can disrupt VRRP failovers.

**Configuring VRRP Rules for Check Point Security Gateway**

This section supplies information for firewall rules to work with VRRP.
Find this rule above the Stealth Rule:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls</td>
<td>mcast-224.0.0.18</td>
<td>vrrp</td>
<td></td>
</tr>
<tr>
<td>fwcluster-object</td>
<td></td>
<td>igmp</td>
<td>Accept</td>
</tr>
</tbody>
</table>

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

If your appliances run routing protocols such as OSPF and DVMRP, 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
- **Netmask:** 240.0.0.0

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

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster-all-ips</td>
<td>fwcluster-object</td>
<td>ospf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>vrrp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>igmp</td>
<td>Accept</td>
</tr>
<tr>
<td></td>
<td>MCAST.NET</td>
<td>dvmrp</td>
<td></td>
</tr>
</tbody>
</table>

**Enabling Virtual Routers**

When you log into Gaia for the first time after installation, you must use the First Time Wizard to 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 installation process and the restart the computer when prompted.

Do this procedure for each VRRP member.

When you complete this procedure for each VRRP member, do these steps in the WebUI:
1. Select **VRRP** from the navigation tree.
2. Clear the **Disable All Virtual Routers** option. This option is selected by default.

When you complete these procedures, define your Virtual Routers using the WebUI or the CLI.

**Configuring Global Settings for VRRP**

This section includes explanations and procedures for configuring the global settings, which apply to all defined Virtual Routers.
Configure these global settings:


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 disabled.

3. **Monitor Firewall State** - Select this option to let VRRP to 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**

When selected, Gaia starts to monitor the firewall after the cold start delay completes. This can cause some problems:

- If all the VRRP router (member) interfaces in a Virtual Router fail, all VRRP routers become backups. None of the VRRP routers can become the master and no traffic is allowed.

- If you change the time on any of the VRRP routers (member), a failover occurs automatically.

- In certain situations, installing a firewall policy causes a failover. This can happen if it takes a long time to install the policy.

**Configuring a Virtual Router - WebUI**

This section shows the basic procedure for configuring a Virtual Router.

**To add a new Virtual Router:**

1. In the navigation tree, select VRRP.
2. In the Virtual Routers section, click Add.
3. In the Add Virtual Router window, configure these parameters:

   - **Virtual Router ID** - Enter a unique ID number for this virtual router. The range of valid values is 1 to 255.

   - **Priority** - Enter the priority value, which selects the Security Gateway that takes over in the event of a failure. The Security Gateway with the highest available priority becomes the new master. The range of valid values 1 to 254. The default setting is 100.

   - **Hello Interval** - Select the number of seconds after which the master sends its VRRP advertisements. The range is 1-255 seconds (default = 1).

   All Security Gateways in a Virtual Router must have the same Hello Interval. If you do not do this, more than one Security Gateway can be in the master state.

   The Hello Interval also defines the failover interval (the time it takes a backup router to take over from a failed master).

   - **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 the format outlined in the VRRP protocol specification RFC 3768. It is automatically set to the same value on all VRRP routers a VRID. 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 dependant 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 a Virtual Router - CLI (mcvr)

### Description

Use the mcvr command to configure a basic (simplified) Virtual Router.

### Syntax

**Add and Delete commands**

```plaintext
add mcvr vrid VALUE backup-address VALUE vmac-mode VALUE [static-mac VALUE]
add mcvr vrid VALUE priority VALUE priority-delta VALUE
               [hello-interval VALUE authtype VALUE password VALUE]
delete mcvr vrid VALUE
```

**Set Commands**

```plaintext
set mcvr vrid VALUE authtype VALUE [password VALUE]
set mcvr vrid VALUE backup-address VALUE vmac-mode VALUE [static-mac VALUE]
set mcvr vrid VALUE hello-interval VALUE
set mcvr vrid VALUE priority VALUE
```

**Show commands**
show mcvr vrid VALUE all
show mcvr vrid VALUE authtype
show mcvr vrid VALUE backup-addresses
show mcvr vrid VALUE hello-interval
show mcvr vrid VALUE password
show mcvr vrid VALUE priority
show mcvr vrid VALUE priority-delta
show mcvr vrids

Parameters

<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 VRRP Group. You can define more that one address for a VRRP Group.  
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 VRRP Group. |
| 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 VRRP routers a VRID. 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 dependant 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. |
<p>| static-mac     | If the vmac-mode parameter is set to static, you enter the static VMAC address.                                                             |</p>
<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| hello-interval   | Select the number of seconds after which the master sends its VRRP advertisements. The range is 1-255 seconds (default = 1).  
All Security Gateways in a Virtual Router must have the same Hello Interval. If you do not do this, more than one Security Gateway can be in the master state.  
The **Hello Interval** also defines the failover interval (the time it takes a backup router to take over from a failed master). |
| password         | Authentication password.                                                        |
| priority         | Enter the priority value, which selects the Security Gateway that takes over in the event of a failure. The Security Gateway with the highest available priority becomes the new master. The range of valid values 1 to 254. |
| priority delta   | Enter the value to subtract from the **Priority** to create an effective priority when an interface fails. The range is 1-254.  
If an interface fails on the backup, the value of the priority delta is subtracted from its priority. This gives a higher effective priority to 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. |
| vrids            | Shows all VRIDs.                                                                |
Advanced VRRP

The advanced VRRP requires users to manually configure a virtual router for each monitored interface.

To change from Advanced VRRP to simple VRRP:
1. Delete all VRIDs, and recreate them in the regular VRRP section.

   **Note**: You cannot move a backup address between interfaces while a platform is in the master state. To modify a virtual IP address, first cause a failover to the backup. Reduce the priority or disconnect an interface, delete the VRID on the interface, and recreate it with the new IP address. Then configure it as before.

Configuring Advanced VRRP - WebUI

To configure VRRP Global Settings:
1. In the VRRP Global Settings section, in Cold Start Delay, select the number of seconds that the system waits after starting and before joining a Virtual Router. The value range is 1-3600. It is advised to configure a delay to let routing adjacencies form, or applications to synchronize before a system becomes the VRRP master.
2. In Disable All Virtual Routers, you can select to disable the routers, but it is advised to leave the clear default to keep the virtual routers enabled.
3. In Monitor Firewall State, you can select to clear (by default it is selected), but if you do, VRRP negotiation for master state might start before the firewall is fully started. This can result in two VRRP nodes assuming the master state while the firewall processes start.

   **Note**: When selected, the system begins to monitor the firewall after the cold start delay period elapses. That can cause these problems:
   - If all the VRRP interfaces in a Virtual Router fail, all the nodes become backup systems. None of the nodes is able to become the master, so no traffic is forwarded.
   - If you change the time on any of the nodes, a VRRP transition (failover) occurs.
   - Under certain circumstances, installing a firewall policy causes a VRRP transition to occur. This can happen if it takes a long time to install the policy.

Click **Apply Global Settings**. 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 VRID 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 VRRP routers 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 VRRP routers 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 VRID, a virtual MAC (VMAC) address is assigned to the backup address. 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 VRID.
- **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 VRID.

  **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 VRID.

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 or select with the arrows the number to subtract from Priority to create 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 the Check Point Security Gateway for VRRP

This section lists considerations for when you configure the Check Point Security Gateway for VRRP. For more details, refer to the Check Point documentation.

- Each cluster member (VRRP router) must have use the same.
- The Operating System and Gaia must run on the same firewall.
- Complete the VRRP configuration before you put the systems into service. Make sure each system is configured, and the firewall begins synchronization before it puts the VRRP group in service. This procedure ensures that all connections are synchronized correctly.

When you use the Check Point cpconfig program, follow these guidelines:

- Install the Check Point Security Gateway on each node. Do not install the Check Point Security Gateway and Security Management server together on the same node.

When you create and configure a gateway cluster object with the external VRRP IP address:

- Use the Check Point SmartDashboard application to create a gateway cluster object.
- Set the gateway cluster object address to the external VRRP IP address. That is, the VRRP IP (backup) address of the interface that faces the external network.
- Add a gateway object for each Check Point appliance to the gateway cluster object.
- In the gateway cluster object General Properties window, clear ClusterXL.
- Configure interfaces for each member of the VRRP cluster. In Topology, select each VRRP cluster member, and click Get > All Member's Interfaces with Topology.
- Configure interfaces for the VRRP cluster. In Topology, select the gateway cluster object, and click Get > All Member's Interfaces with Topology.

When you complete configuring the gateway cluster object, you must also specify settings in 3rd Party Configuration as described in this procedure.

To configure settings for 3rd party configuration:

1. In the Cluster Mode section, select High Availability.
2. From the Third-Party Solution drop down list, select Check Point VRRP.
3. Select Use State Synchronization, and configure interfaces for it in Topology.

   Note - The Firewall Synchronization network requires a bandwidth of 100 mbps or greater.

   The interfaces that you configure for State Synchronization cannot be part of VLAN. They also cannot have more than one IP address assigned to them.
4. Select all the available check boxes.
5. Click OK to save your configuration changes.

   Note - you can use different encryption accelerator cards in two appliances of one VRRP group 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 fail over incorrectly. If the encryption/authentication algorithm is supported on the master only, without NAT, tunnels are not accelerated after failover.

**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 VALUE
monitored-circuit vrid VALUE auto-deactivation VALUE
monitored-circuit vrid VALUE backup-address VALUE on|off
monitored-circuit vrid VALUE hello-interval VALUE
monitored-circuit vrid VALUE monitored-off
monitored-circuit vrid VALUE monitored-on
monitored-circuit vrid VALUE monitored-priority-delta VALUE
monitored-circuit vrid VALUE off
monitored-circuit vrid VALUE on
monitored-circuit vrid VALUE preempt-mode VALUE
monitored-circuit vrid VALUE priority VALUE
monitored-circuit vrid VALUE vmac-mode default-vmac
monitored-circuit vrid VALUE vmac-mode extended-vmac
monitored-circuit vrid VALUE vmac-mode interface-vmac
monitored-circuit vrid VALUE vmac-mode static-vmac VALUE off
virtual-router backup-vrid VALUE backup-address VALUE on|off
virtual-router backup-vrid VALUE hello-interval VALUE
virtual-router backup-vrid VALUE off
virtual-router backup-vrid VALUE preempt-mode VALUE
virtual-router backup-vrid VALUE priority VALUE
virtual-router backup-vrid VALUE vmac-mode default-vmac
virtual-router backup-vrid VALUE vmac-mode extended-vmac
virtual-router backup-vrid VALUE vmac-mode interface-vmac
virtual-router backup-vrid VALUE vmac-mode static-vmac VALUE
virtual-router vrid VALUE hello-interval VALUE
virtual-router vrid VALUE off
virtual-router vrid VALUE on
virtual-router vrid VALUE vmac-mode default-vmac
virtual-router vrid VALUE vmac-mode extended-vmac
virtual-router vrid VALUE vmac-mode interface-vmac
virtual-router vrid VALUE vmac-mode static-vmac VALUE

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

Parameters

<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>[on</td>
<td>off]</td>
</tr>
<tr>
<td>monitor-firewall</td>
<td></td>
</tr>
<tr>
<td>on</td>
<td>off</td>
</tr>
<tr>
<td>vrrp interface VALUE</td>
<td>The name of the specified Virtual Router interface</td>
</tr>
<tr>
<td>authtype simple VALUE</td>
<td>Enter a password to authenticate the Virtual Router.</td>
</tr>
<tr>
<td>monitored-circuit vrid</td>
<td>on or off for the interface to be monitored.</td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>auto-deactivation</td>
<td>on or off. On would create an effective priority 0. The virtual router with 0 priority cannot become master.</td>
</tr>
<tr>
<td>backup-address</td>
<td>The IPv4 address of the backup router.</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>
<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 VRRP group, a new master is selected. The range is 1-254</td>
</tr>
<tr>
<td>preempt-mode</td>
<td>on or off. If on, after a failover, the original master becomes master again when returns to service. If off, the backup system that becomes master, remains master.</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 backup-vrid</td>
<td>The backup virtual router ID number</td>
</tr>
<tr>
<td>virtual-router vrid</td>
<td>The virtual router ID number</td>
</tr>
</tbody>
</table>

**Troubleshooting VRRP**

This section shows known issues with VRRP configurations and fixes. Read this section before contacting Check Point Technical Support (www.checkpoint.com).

You can log information about errors and events for troubleshooting VRRP. Enable traces for VRRP.

**To enable traces for VRRP:**
1. In the WebUI tree, select Routing > Routing Options.
2. In the Trace Options section, in the Filter Visible Tables Below drop down list, select VRRP.
3. In the VRRP table, select an option, and click Activate.

The system restarts the routing subsystem and signals it to reread its configuration. The option you selected, its name and On/Off radio buttons show on the page.

**General Configuration Considerations**

If VRRP failover does not occur as expected, make sure that the configuration of these items.

- All routers of a VRRP group must have the same system times. The simplest method to synchronize times is to enable NTP on all nodes of the VRRP group. 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 VRRP group 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 VRRP group 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.

- V RIDs must be the same on all routers in a VRRP group. If you use Monitored-Circuit VRRP, make sure all platforms of one virtual IP address use the same VRID.

- 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

If your platforms run firewall software, you must configure the firewall policies to accept VRRP packets. 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 VRRP group 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 the change to a backup router occurs, the MAC address for virtual router shifts 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:

- Replace the switch with a hub.
- 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.
Chapter 10

Maintenance

In This Chapter

<table>
<thead>
<tr>
<th>License</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licenses</td>
<td>132</td>
</tr>
<tr>
<td>Image Management</td>
<td>140</td>
</tr>
<tr>
<td>System Configuration Backup</td>
<td>142</td>
</tr>
<tr>
<td>Download SmartConsole</td>
<td>147</td>
</tr>
<tr>
<td>Hardware Health Monitoring</td>
<td>147</td>
</tr>
<tr>
<td>Shutdown</td>
<td>148</td>
</tr>
</tbody>
</table>

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 134) or `cplic del` (on page 135).

**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](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** - The 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:

```plaintext
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:

```plaintext
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:

```plaintext
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**  
Check whether the license on the local machine will allow a given feature to be used.

**Usage**  

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-p &lt;product name&gt;</code></td>
<td>Product for which license information is requested. For example <code>fw1</code>, <code>netso</code></td>
</tr>
<tr>
<td><code>-v &lt;product version&gt;</code></td>
<td>Product version for which license information is requested</td>
</tr>
</tbody>
</table>
**Argument** | **Description**
---|---
-c *count* | Output the number of licenses connected to this feature
-t *<date>* | Check license status on future date. Use the format *ddmmmyyyy*. 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. The *feature* option is not needed
*<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, it can only be executed on the Security Management server.

**Usage** `cplic db_add < -l license-file | host expiration-date signature SKU/features >`

**Syntax**

---|---
- l *license-file* | Adds the license(s) from *license-file*. The following options are NOT needed:
  - Host Expiration-Date Signature SKU/feature

**Comments** Copy/paste the following parameters from the license received from the User Center. More than one license can be added.

- **host** - the target hostname or IP address.
- **expiration date** - The license expiration date.
- **signature** - The license signature string. For example:
  
  aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m (Case sensitive. The hyphens are optional.)
- **SKU/features** - The SKU of the license summarizes the features included in the license. For example: CPSUITE-EVAL-3DES-vNG

**Example** If the file `192.0.2.11.lic` contains one or more licenses, the command: `cplic db_add -l 192.0.2.11.lic` 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.

**Usage**

```
cplic db_print <object name | -all> [-n noheader] [-x print signatures] [-t type] [-a attached]
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</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 (or -type)</td>
<td>Print licenses with their type: Central or Local.</td>
</tr>
<tr>
<td>-a (or -attached)</td>
<td>Show which object the license is attached to. Useful if the -all option is specified.</td>
</tr>
</tbody>
</table>

**Comments** This command is a license repository command, it 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.

**Usage**

```
cplic db_rm <signature>
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</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, it 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.

**Usage**

```
cplic del [-F <output file>] <signature> <object name>
```

**Syntax**
### Argument | Description
---|---
-F <output file> | Send the output to <output file> instead of the screen.
<signature> | The signature string within the license.

### cplic del <object name>

**Description**   Detach a Central license from a Check Point 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.

**Usage** cplic del <Object name> [-F outputfile] [-ip dynamic ip] <Signature>

**Syntax**

<table>
<thead>
<tr>
<th>Argument</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>-F outputfile</td>
<td>Divert the output to outputfile rather than to the screen.</td>
</tr>
<tr>
<td>-ip dynamic ip</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>
</tbody>
</table>

**Signature**  The signature string within the license.

**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 Check Point Security Gateway (or from all Check Point gateways) into the license repository on the Security Management server. Do this to synchronize the repository with the Check Point gateway(s). When the command is run, all local changes will be updated.

**Usage** cplic get <ipaddr | hostname | -all> [-v41]

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddr</td>
<td>The IP address of the Check Point Security Gateway from which licenses are to be retrieved.</td>
</tr>
<tr>
<td>hostname</td>
<td>The name of the Check Point Security Gateway object (as defined in SmartDashboard) from which licenses are to be retrieved.</td>
</tr>
<tr>
<td>-all</td>
<td>Retrieve licenses from all Check Point gateways in the managed network.</td>
</tr>
<tr>
<td>-v41</td>
<td>Retrieve version 4.1 licenses from the NF Check Point gateway. Used to upgrade version 4.1 licenses.</td>
</tr>
</tbody>
</table>
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.

Usage  
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>

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-overwrite</td>
<td>On a Security Management server this will erase all existing licenses and replace them with the new license(s). On a Check Point Security Gateway this will erase only Local licenses but not Central licenses, that are installed remotely.</td>
</tr>
<tr>
<td>(or -o)</td>
<td></td>
</tr>
<tr>
<td>-check-only</td>
<td>Verify the license. Checks if the IP of the license matches the machine, and if the signature is valid</td>
</tr>
<tr>
<td>(or -c)</td>
<td></td>
</tr>
<tr>
<td>select</td>
<td>Select only the Local licenses whose IP address matches the IP address of the machine.</td>
</tr>
<tr>
<td>(or -s)</td>
<td></td>
</tr>
<tr>
<td>-F outputfile</td>
<td>Outputs the result of the command to the designated file rather than to the screen.</td>
</tr>
<tr>
<td>-Preboot</td>
<td>Use this option after upgrading and before rebooting the machine. Use of this option will prevent certain error messages.</td>
</tr>
<tr>
<td>(or -P)</td>
<td></td>
</tr>
<tr>
<td>-kernel-only</td>
<td>Push the current valid licenses to the kernel. For Support use only.</td>
</tr>
<tr>
<td>(or -k)</td>
<td></td>
</tr>
<tr>
<td>-l license-file</td>
<td>Installs the license(s) in license-file, which can be a multi-license file. The following options are NOT needed: host expiration-date signature SKU/feature</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  
Example: cplic put -l 215.153.142.130.lic produces output similar to the following:
**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.

**Usage**  
```
cplic put <object name> [-ip dynamic ip] [-F <output file>] < -l license-file | host expiration-date signature SKU/features >
```

<table>
<thead>
<tr>
<th><strong>Argument</strong></th>
<th><strong>Description</strong></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>
</tbody>
</table>
| -ip dynamic ip | 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.  
**NOTE:** If this parameter is used, then object name must be a DAIP Check Point gateway. |
| -F outputfile | Divert the output to `outputfile` rather than to the screen. |
| -l license-file | Installs the license(s) from `license-file`. The following options are **NOT** needed:  
Host Expiration-Date Signature SKU/features |

**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-zippoVWSm-n98N7ck3m  (Case sensitive. The hyphens are optional)
```
- **SKU/features** - A string listing the SKU and the Certificate Key of the license. The SKU of the license summarizes the features included in the license. For example: `CPMP-EVAL-1-3DES-NG CK0123456789ab`

**cplic print**

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

**Usage**  
```
cplic print [-n noheader] [-x prints signatures] [ -t type] [-F <outputfile>] [-p preatures]
```

**Syntax**

<table>
<thead>
<tr>
<th><strong>Argument</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>-noheader (or -n)</td>
<td>Print licenses with no header.</td>
</tr>
</tbody>
</table>
## Argument Description

- `-x`  
  Print licenses with their signature

- `type`  
  (or `-t`)  
  Prints licenses showing their type: Central or Local.

- `-F <outputfile>`  
  Divert the output to `outputfile`.

- `preatures`  
  (or `-p`)  
  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.

**Usage**  
`cplic upgrade <-l inputfile>`

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-l inputfile</code></td>
<td>Upgrades the licenses in the license repository and Check Point gateways to match the licenses in <code>&lt;inputfile&gt;</code></td>
</tr>
</tbody>
</table>

**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:
  
  ```bash
count:root(su) [~] # cplic get -all
golda:
Retrieved 1 licenses.
Detached 0 licenses.
Removed 0 licenses.
count:
Retrieved 1 licenses.
Detached 0 licenses.
Removed 0 licenses.
```

- To see all the licenses in the repository, run the command `cplic db_print -all -a`
count:root(su) [~] # cplic db_print -all -a

Retrieving license information from database ...

The following licenses appear in the database:

<table>
<thead>
<tr>
<th>Host</th>
<th>Expiration</th>
<th>Features</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.2.11</td>
<td>Never</td>
<td>CFW-FIG-25-53</td>
<td>golda</td>
</tr>
<tr>
<td>192.0.2.11</td>
<td>26Nov2012</td>
<td>CPSUITE-EVAL-3DES-NGX</td>
<td>count</td>
</tr>
</tbody>
</table>

- 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.**

See the **SmartUpdate** chapter of the **R75.40 Installation and Upgrade Guide** (http://supportcontent.checkpoint.com/solutions?id=sk67581).

### Image Management

You can:

- Make a **new image** (a snapshot) of the system. You can revert to the image at a later time.
- **Revert** to a locally stored image.
- **Delete** an image from the local system.
- **Export** an existing image. This creates a compressed version of the image. You can then download the exported image to another computer and delete the exported image from the Gaia computer, to save disk space.
- **Import** uploads an exported image and makes an image of it (a snapshot). You can revert to the image at a later time.
- View a list of images that are stored locally.

### Configuring Image Management - WebUI

**To create an image:**

1. In the tree view, click **Maintenance > Image Management**.
2. Below available images, click **New Image**. The **Create New Image window** opens.
3. In the **Name** field, enter a name for the image.
4. Optional: In the **Description** field, enter a description for the image.
5. Click **OK**.
Note - To create the snapshot requires free space on the Backup partition. The required free disk space is the actual size of the root partition, multiplied by 1.15.

To revert to an image:
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 an image:
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 an image:
1. In the tree view, click Maintenance > Image Management.
2. Select an image.
3. Click Export. The Export Image (name) window.
4. Click Start Export.
   
   Note -
   - The snapshot image exports to /var/log. The free space required in the export file storage location is the size of the snapshot multiplied by two.
   - The minimum size of a snapshot is 2.5G, so the minimum free space you need in the export file storage location is 5G.

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.

**Configuring Image 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 VALUE</td>
<td>The name of the image to export</td>
</tr>
<tr>
<td>snapshot import VALUE</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 free space required in the export file storage location is the size of the snapshot multiplied by two.

- The minimum size of a snapshot is 2.5G, so the minimum free space you need in the export file storage location is 5G.

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, or 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 do a scheduled backup.

- 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 and Restoring the System - CLI (Backup)**

**Backing up a Configuration**

**Description**  Use these commands to save the system's configuration

**Syntax**

- To save a backup locally:
  ```
  add backup local
  ```

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

- To 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
  ```

**Parameters**

<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/
Restoring a Configuration

**Description**  Use these commands to restore the system’s configuration from a backup file.

**Syntax**

To restore a backup from a locally held file:

```
set backup restore local <TAB>
```

To restore a backup from a remote server using ftp:

```
set backup restore ftp ip VALUE 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 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>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 feature.

Monitoring Backup Status

To monitor the creation of a backup:

```
show backups
```

To show the status of the last backup performed:

```
show backup status
```

**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
```
<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 <code>recurrence daily time</code>, 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 <code>recurrence monthly month</code>, 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 <code>recurrence weekly</code>, 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>

**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

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**. In the Security configuration widget, select Download
   - **Maintenance > Download SmartConsole**.
2. Click Download.

Hardware Health Monitoring

You can monitor these hardware elements:

- Fan sensors—Shows the fan number, status, and value.
- System Temperature sensor
- Voltage sensors
- Power Supply (on machines that support it)

**Showing Hardware Health Monitoring Information - WebUI**

In the navigation tree, click **Maintenance > Hardware Health**.

You can see the status of the machine fans, system temperature, the voltages, and (for supported hardware only) the power supply.
Note - The Hardware Health Monitoring page only appears for supported hardware.

For each component sensor, the table shows the value of its operation, and the status: **OK**, **Low**, or **High**.

- To see the health history of a component, select the component sensor. A graph shows the values over time.
- To change the time intervals that the graph shows, click the **Minute** arrows.
- To view different times, click the **Forward/Backward** arrows.
- To refresh, click **Refresh**.

### Showing Hardware Monitoring Information - CLI (sysenv)

**Description**
These commands display the status for various system components. Components for which the status can be displayed include temperature, voltage, power supplies, and fans. The command returns status only for installed components.

**Syntax**
To display all system status information:

```
show sysenv all
```

To display all system component information:

```
show sysenv fans
show sysenv ps
show sysenv temp
show sysenv volt
```

**Parameters**

<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**

```
gw-3002f0> show sysenv all
```

**Output**

```
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>
```

### 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.
Chapter 11

Software Updates

In This Chapter
- Configuring a Software Deployment Policy - WebUI: 150
- Configuring Software Update Notifications - WebUI: 151
- Configuring Software Deployment - WebUI: 151
- Configuring Software Deployment – cli.sh (installation): 152

Gaia automatically locates and shows the available software update packages for Check Point products and the Gaia OS. Only packages that are applicable to the Gaia computer are shown. The packages can be downloaded from the Check Point Support center and installed. You can configure downloads and installations to be manual, scheduled, or automatic.

You can add a private package to the list of available packages. A private package is a hotfix that you get from Check Point Support. Private packages are not available on the Check Point Support Center.

The general workflow for updating software is:
1. Define the software deployment policy for downloads and installation.
   - Downloads and installations can be manual, automatic, or scheduled (daily, weekly, monthly, or once only).
2. Define mail notifications for new packages and for automatic package updates.
3. Do the software download and installation.

Configuring a Software Deployment Policy - WebUI

To define the software deployment policy:
1. In the WebUI, go to the Software Updates > Policy page.
2. Configure how to download updates. Select one of Manually, Scheduled, or Automatic.
   - If you choose to make a schedule for the download of updates. You can define the schedule to be Daily, Weekly, Monthly, or Once.
3. Configure how to install updates. Select one of Manually, Scheduled, or Automatic.
4. Check Point would like to collects statistics about downloaded and installed packages. This information is used only to make a better software update service. To let Check Point collect statistics, select Allow sending statistics information.
5. Select which sanity tests to perform after installing the software updates:
   - Processes - Make sure that Check Point processes are running
   - Policy installation - Make sure that it is possible to install a policy
   - Network Access - Make sure that all the network interfaces on the Gaia computer are Up.
6. Select Auto-rollback upon failure to do this if the installed package fails one of the sanity tests:
   - Automatically restore the installation you had before the package was installed.
   - Send a notification that the installation failed.
   - If the installed package fails one of the sanity tests, and this option is not selected, only the notification is sent.
7. Click Apply.
Configuring Software Update 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 on the Gaia computer that have been downloaded.
- Package installation success or failure.

To configure software update notifications:
1. In the WebUI, go to the Software Updates > Software Update Notifications page.
2. Click Add.
3. Enter the email addresses of persons who will receive notification, and select the types of notification they will receive.
4. Go to the System Management > Mail Notifications page.
5. Enter the email address of the sender of the software update notifications.
6. Configure a mail server address.

Note - If you do not configure an email address in the System Management > Mail Notifications page, no notifications are sent.

Configuring Software Deployment - WebUI

Before doing a software update:
1. Configure the software updates policy to:
   - Download packages manually, automatically or according to a schedule.
   - Install packages manually, automatically or according to a schedule.
2. Configure mail notifications for packages.

To manually download a software package:
You will receive an email when a package is available for download from the Check Point Support Center.
1. In the Software Updates > Status and Actions page, select a package with the status Available for Download.
2. Click Download.

When the package is downloaded, the package status changes to Available for Install. If you configured mail notifications for downloads, you will get an email notification.

To manually install a software package:
If you configured mail notifications for downloads, you will receive an email when a package is available for installation.
1. In the Software Updates > Status and Actions page, select a package with the status Available for install.
2. Click Install.

When the package is installed on the Gaia computer, the package status changes to Installed. If you configured mail notifications for packages, you will receive an email when a package is Installed.

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 that you get from Check Point Support. Private packages are not available on the Check Point Support Center.
1. In the Software Updates > Status and Actions page, insert the URL that you received from Support.
2. Click Add.

The package is added to the list of packages.
Configuring Software Deployment – clish (installation)

**Description**
Using the `installer` tool you can:

- Define the software deployment policy for downloads and installation. Either manual or automatic.
- Define mail notifications for packages.
- Do the software download and installation.
- See the software package status

**Syntax**
To see the names of the packages that are available for download, install and uninstallation:

```
installer
download <TAB>
install <TAB>
uninstall <TAB>
```

To download, install and uninstall updates:

```
installer
download <package name>
install <package name>
uninstall <package name>
```

To restore the default deployment policy:

```
installer restore_policy
```

To download updates automatically or manually:

```
set installer download_mode
  automatic
  manual
```

To install updates automatically or manually:

```
set installer install_mode
  automatic
  manual
```

To configure mail notifications

```
set installer deployment-mail-notification <email address>
  available_packages false
  available_packages true
  download_status false
  download_status true
  install_status false
  install_status true
```

To show a list of packages and the package status:

```
show installer
  available_packages
  available_local_packages
  installed_packages
  package_status
```
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>download</td>
<td>Download a selected package</td>
</tr>
<tr>
<td>install</td>
<td>Install a selected package</td>
</tr>
<tr>
<td>restore_policy</td>
<td>Restore the default update policy</td>
</tr>
<tr>
<td>uninstall</td>
<td>Uninstall a selected package</td>
</tr>
<tr>
<td>download_mode</td>
<td>Configure how packages are downloaded. Either automatic or manual.</td>
</tr>
<tr>
<td>install_mode</td>
<td>Configure how packages are installed. Either automatic or manual.</td>
</tr>
<tr>
<td>deployment-mail-notification &lt;email address&gt;</td>
<td>The email address to receive (or not receive) notifications</td>
</tr>
<tr>
<td>available_packages</td>
<td>Packages that are available to download.</td>
</tr>
<tr>
<td>download_status</td>
<td>The status of newly downloaded packages</td>
</tr>
<tr>
<td>install_status</td>
<td>The status of newly installed packages</td>
</tr>
<tr>
<td>available_local_packages</td>
<td>The packages that are available to install.</td>
</tr>
<tr>
<td>installed_packages</td>
<td>The installed packages</td>
</tr>
<tr>
<td>package_status</td>
<td>The packages and their current status</td>
</tr>
</tbody>
</table>

### CLI Procedures - Software Updates

This section includes some basic procedures for configuring software updates using the CLI.
Show Commands
To show the packages that are available for download:
show installer available_packages

To show the packages that are available for installation:
show installer available_local_packages

To show the installed packages:
show installer installed_packages

To show the packages and their status:
show installer package_status

Configuring the Software Deployment Policy
To download a package:
installer download <package name or number>

To install a local package:
installer install <package name or number>

To uninstall a package:
installer uninstall <package name or number>

To restore the default deployment policy:
installer restore_policy

Configuring Package Notifications
To configure notifications for available packages:
You can add or remove email addresses from the list to which emails about available packages are sent.

clear installer deployment-mail-notification <email address> available packages
set installer deployment-mail-notification <email address> available packages true

To configure notifications for downloaded packages:
You can add or remove email addresses from the list to which emails about newly downloaded (or failed) packages are sent.

clear installer deployment-mail-notification <email address> download_status
set installer deployment-mail-notification <email address> download_status true

To configure notifications for installed packages:
You can add or remove email addresses from the list to which emails about newly installed (or failed) packages are sent.

clear installer deployment-mail-notification <email address> installed_packages
set installer deployment-mail-notification <email address> installed_packages true
set installer deployment-mail-notification <email address> install_status true
set installer deployment-mail-notification <email address> install_status false

Configuring the Software Deployment Policy

To sets downloads to be automatic or manual:
set installer download_mode manual
set installer download_mode automatic

To sets installation to be automatic or manual:
set installer install_mode manual
set installer install_mode automatic
Chapter 12

Security Management Server and Firewall Commands

In This Chapter

- cpca_client  
- cp_conf  
- cpconfig  
- cpinfo  
- cpstart  
- cpstat  
- cpstop  
- fw  
- fwm

**cpca_client**

**Description**  This command and all its derivatives are used to execute operations on the ICA.

**Usage**  cpca_client

**cpca_client create_cert**

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

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

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Debug flag</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</td>
</tr>
<tr>
<td>-f &lt;PKCS12 filename&gt;</td>
<td>Specifies the file name where the certificate and keys are saved.</td>
</tr>
</tbody>
</table>

**cpca_client revoke_cert**

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

**Usage**  cpca_client [-d] revoke_cert [-p <ca_port>] -n "CN=<common name>"
<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Debug flag</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</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>Debug flag</td>
</tr>
<tr>
<td>-dn substring</td>
<td>Filters results to those with a DN that matches this substring</td>
</tr>
<tr>
<td>-stat</td>
<td>Filters results to this status</td>
</tr>
<tr>
<td>-kind</td>
<td>Filters results for specified kind: SIC, IKE, User, or LDAP</td>
</tr>
<tr>
<td>-ser number</td>
<td>Filters results for this serial number</td>
</tr>
<tr>
<td>-dp number</td>
<td>Filters results from this CDP</td>
</tr>
</tbody>
</table>

**cpca_client set_mgmt_tools**

Description: Invoke or terminate the ICA Management Tool.

Usage: `cpca_client [-d] set_mgmt_tools on|off [-p <ca_port>] [-no_ssl] [-a|-u "administrator|user DN" -a|-u "administrator|user DN" ... ]`

Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Debug flag</td>
</tr>
<tr>
<td>set_mgmt_tools on</td>
<td>off</td>
</tr>
<tr>
<td></td>
<td>off - Stop ICA Management tool</td>
</tr>
<tr>
<td>-p &lt;ca_port&gt;</td>
<td>Specifies the port which is used to connect to the CA (if the appropriate service was not run from the default port 18265)</td>
</tr>
<tr>
<td>-no_ssl</td>
<td>Configures the server to use clear http rather than https</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>-a</td>
<td>-u&quot;administrator</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.

**Usage**
cp_conf

**cp_conf sic**

**Description** Enables the user to manage SIC.

**Usage**
cp_conf sic state # Get the current Trust state
cp_conf sic init <Activation Key> [norestart] # Initialize SIC
cp_conf sic cert_pull <Security Management server name/IP> <module object name> # Pull certificate (DAIP only)

**cp_conf admin**

**Description** Manage Check Point Administrators.

**Usage**
cp_conf admin get # Get the list of administrators.
cp_conf admin add <user> <passw> <permissions> # Add administrator
where permissions:
w - read/write
r - read only
cp_conf admin del <admin1> <admin2>... # Delete administrators.

**cp_conf ca**

**Description** Initialize the Certificate Authority

**Usage**
cp_conf ca init # Initializes Internal CA.
cp_conf ca fqdn <name> # Sets the name of the Internal CA.

**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

**Usage**
cp_conf finger get # Get Certificate's Fingerprint.

**cp_conf lic**

**Description** Enables the administrator to add a license manually and to view the license installed.

**Usage**
cp_conf lic get # Get licenses installed.
cp_conf lic add -f <file name> # Add license from file.
Security Management
Server and Firewall Commands

Gaia Administration Guide R75.40 | 159

\texttt{cp\_conf lic add -m <Host> <Date> <Signature Key> <SKU/Features>} # Add license manually.
\texttt{cp\_conf lic del <Signature Key>} # Delete license.

\textbf{\texttt{cp\_conf client}}
\textbf{Description} Manage the GUI Clients that are allowed to connect to the Security Management server.
\textbf{Usage} \texttt{cp\_conf client get} # Get the GUI Clients list
\texttt{cp\_conf client add < GUI Client >} # Add one GUI Client
\texttt{cp\_conf client del < GUI Client 1> < GUI Client 2>...} # Delete GUI Clients
\texttt{cp\_conf client createlist < GUI Client 1> < GUI Client 2>...} # Create new list.

\textbf{\texttt{cp\_conf ha}}
\textbf{Description} Enable or disable High Availability.
\textbf{Usage} \texttt{cp\_conf ha enable/disable [norestart]} # Enable/Disable HA

\textbf{\texttt{cp\_conf snmp}}
\textbf{Description} Activate or deactivate SNMP.
\textbf{Usage} \texttt{cp\_conf snmp get} # Get SNMP Extension status.
\texttt{cp\_conf snmp activate/deactivate [norestart]} # Deactivate SNMP Extension.

\textbf{\texttt{cp\_conf auto}}
\textbf{Description} Determine whether or not the Security Gateway/Security Management server starts automatically after the machine restarts.
\textbf{Usage} \texttt{cp\_conf auto get [fw1] [fg1] [rm] [all]} # Get the auto state of products.
\texttt{cp\_conf auto <enable|disable> <product1> <product2>...} # Enable/Disable auto start.

\textbf{\texttt{cp\_conf sxl}}
\textbf{Description} Enable or disable SecureXL acceleration.
\textbf{Usage} \texttt{cp\_conf sxl <enable|disable>} # Enable/Disable SecureXL.

\textbf{\texttt{cpconfig}}
\textbf{Description} Run a command line version of the Check Point Configuration Tool. This tool is used to configure an installed Check Point product. The options shown depend on the installed configuration and products. Amongst others, these options include:
\begin{itemize}
  \item \textbf{Licenses and contracts} - Modify the necessary Check Point licenses and contracts.
  \item \textbf{Administrator} - Modify the administrator authorized to connect to the Security Management server.
  \item \textbf{GUI Clients} - Modify the list of SmartConsole Client machines from which the administrators are authorized to connect to a Security Management server.
  \item \textbf{SNMP Extension} - Configure the SNMP daemon. The SNMP daemon enables SecurePlatform to export its status to external network management tools.
  \item \textbf{PKCS #11 Token} - Register a cryptographic token, for use by SecurePlatform; see details of the token, and test its functionality.
  \item \textbf{Random Pool} - Configure the RSA keys, to be used by SecurePlatform.
  \item \textbf{Certificate Authority} - Install the Certificate Authority on the Security Management server in a first-time installation.
\end{itemize}
- **Secure Internal Communication** - Set up trust between the gateway on which this command is being run and the Security Management server.

- **Certificate's Fingerprint** - Display 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.

- **Automatic Start of Check Point Products** - Specify whether Check Point Security Gateways will start automatically at boot time.

**Usage** `cpconfig`

**Further Info.** See the R75.40 Installation and Upgrade Guide ([http://supportcontent.checkpoint.com/solutions?id=sk67581](http://supportcontent.checkpoint.com/solutions?id=sk67581)).

### cpinfo

**Description** - CPinfo is a utility that collects data on a machine at the time of execution. The CPinfo output file enables Check Point's support engineers to analyze setups from a remote location. Engineers can open the CPinfo file in demo mode, while viewing real Security Policies and objects. This allows for in-depth analysis of all configuration options and environment settings.

**Usage** - `cpinfo [-v] [-l] [-n] [-o] [-r | -t [tablename]] [-c Domain Management Server ... | -x vs]`

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-z</td>
<td>Output gzipped (effective with -o option)</td>
</tr>
<tr>
<td>-r</td>
<td>Includes the registry (Windows - very large output)</td>
</tr>
<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>-t</td>
<td>Output consists of tables only (SR only)</td>
</tr>
<tr>
<td>-c</td>
<td>Get information about the specified Domain Management Server (Multi-Domain Security Management)</td>
</tr>
<tr>
<td>-x</td>
<td>Get information about the specified VS (VSX)</td>
</tr>
</tbody>
</table>

**Further Info.** SecureKnowledge solution sk30567 ([http://supportcontent.checkpoint.com/solutions?id=sk30567](http://supportcontent.checkpoint.com/solutions?id=sk30567))

### cpstart

**Description** - Start all Check Point processes and applications running on a machine.

**Usage** `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 machine or on another machine, in various formats.

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

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-h host</code></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><code>-p port</code></td>
<td>Port number of the AMON server. The default is the standard AMON port (18192).</td>
</tr>
<tr>
<td><code>-s</code></td>
<td>Secure Internal Communication (SIC) name of the AMON server.</td>
</tr>
<tr>
<td><code>-f flavor</code></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><code>-o</code></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><code>-c</code></td>
<td>Specifies how many times the results are shown. The default is 0, meaning the results are repeatedly shown.</td>
</tr>
<tr>
<td><code>-e</code></td>
<td>Specifies the interval (seconds) over which 'statistical' olds are computed. Ignored for regular olds.</td>
</tr>
<tr>
<td><code>-d</code></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  
- `polsrv`  
- `uas`  
- `svr`  
- `cpsemd`  
- `cpsead`  
- `asm`  
- `ls`  
- `ca`

The following flavors can be added to the application flags:
Security Management  Server and Firewall Commands

- **vpn** — "default", "product", "IKE", "ipsec", "traffic", "compression", "accelerator", "nic", "statistics", "watermarks", "all"
- **fg** — "all"
- **ha** — "default", "all"
- **mg** — "default"
- **persistency** — "product", "Tableconfig", "SourceConfig"
- **polsrv** — "default", "all"
- **uas** — "default"
- **svr** — "default"
- **cpsemd** — "default"
- **cpsead** — "default"
- **asm** — "default", "WS"
- **ls** — "default"
- **ca** — "default", "crl", "cert", "user", "all"

**Example**

```
> 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**|
```

**cpstop**

**Description**  Terminate all Check Point processes and applications, running on a machine.

**Usage**  cpstop

```
  cpstop -fwflag [-proc | -default]
```

**Syntax**

<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>
</tbody>
</table>
### fwflag -default

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 machine 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.

**Usage**

```
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.

**Usage**

```
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.

**Usage**

```
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>
<tbody>
<tr>
<td>&lt;Install</td>
<td>Uninstall&gt;</td>
</tr>
<tr>
<td>• Uninstall — tells the operating system to stop passing packets to the Security Gateway, and unloads the Security Policy. The networks behind it become unprotected.</td>
<td></td>
</tr>
<tr>
<td>• Install — tells the operating system to start passing packets to the Security Gateway. The command <code>fw ctl install</code> runs automatically when <code>cpstart</code> is performed.</td>
<td></td>
</tr>
<tr>
<td>Note - If you run <code>fw ctl uninstall</code> followed by <code>fw ctl install</code>, the Security Policy is not restored.</td>
<td></td>
</tr>
<tr>
<td>debug</td>
<td>Generate debug messages to a buffer. See <code>fw ctl debug</code> (on page 164).</td>
</tr>
<tr>
<td>kdebug</td>
<td>Reads the debug buffer and obtains the debug messages. If there is no debug buffer, the command will fail.</td>
</tr>
<tr>
<td>• [-f] read the buffer every second and print the messages, until <code>Ctrl-C</code> is pressed. Otherwise, read the current buffer contents and end.</td>
<td></td>
</tr>
<tr>
<td>• [-t/T] print the time field (seconds/microseconds)</td>
<td></td>
</tr>
<tr>
<td>• [-p] to print specific fields</td>
<td></td>
</tr>
<tr>
<td>all</td>
<td>proc</td>
</tr>
<tr>
<td>• [-m] - number of cyclic files, [-s] - size of each</td>
<td></td>
</tr>
<tr>
<td>pstat [-h][-k][-s][-n][-l]</td>
<td></td>
</tr>
<tr>
<td>Displays Security Gateway internal statistics:</td>
<td></td>
</tr>
<tr>
<td>-h — Generates additional hmem details.</td>
<td></td>
</tr>
<tr>
<td>-k — Generates additional kmem details.</td>
<td></td>
</tr>
<tr>
<td>-s — Generates additional smem details.</td>
<td></td>
</tr>
<tr>
<td>-n — Generates NDIS information (Windows only).</td>
<td></td>
</tr>
<tr>
<td>-l — Generates general Security Gateway statistics.</td>
<td></td>
</tr>
<tr>
<td>iflist</td>
<td>Displays the IP interfaces known to the kernel, by name and internal number.</td>
</tr>
<tr>
<td>arp [-n]</td>
<td>Displays ARP proxy table.</td>
</tr>
<tr>
<td>-n — Do not perform name resolution.</td>
<td></td>
</tr>
<tr>
<td>block &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>on — Blocks all traffic.</td>
<td></td>
</tr>
<tr>
<td>off — Restores traffic and the Security Policy.</td>
<td></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.
Usage A number of debug options are available:
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 [-d <comma separated list of ^strings>]
fw ctl debug [-s <string>]
fw ctl debug -h
fw ctl debug -x

Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-buf [buffersize]</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: fw ctl debug -m VPN all</td>
</tr>
</tbody>
</table>
| [+ | -] <options| all|0>          | Sets or resets debug flags for the requested gateway.  
|                |   • If + is used, the specified flags are set, and the rest remain as they were.  
|                |   • If - is used, the specified flags are reset, and the rest remain as they were.  
|                |   • If neither + nor - are used, the specified flags are set and the rest are reset.                                                        |
| -h              | Print a list of debug modules and flags.                                                                                                     |
| 0               | Returns all flags in all gateways to their default values, releases the debug buffer (if there was one).                                         |
| -d <comma separated list of strings> | Only lines containing these strings are included in the output. (Available in R70 or higher)                                              |
| -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 R75.40 Firewall Administration Guide [http://supportcontent.checkpoint.com/solutions?id=sk67581].

*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) for details, see the R75.40 Performance Pack Administration Guide [http://supportcontent.checkpoint.com/solutions?id=sk67581].

- Or edit the **fwaffinity.conf** configuration file for details, see the R75.40 Firewall Administration Guide [http://supportcontent.checkpoint.com/solutions?id=sk67581].

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*.

**Usage**  
```
fw ctl affinity -s <proc_selection> <cpuid>
```

**Syntax**  
*<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 <em>&lt;pid&gt;</em> is the process ID#.</td>
</tr>
<tr>
<td>-n &lt;cpdname&gt;</td>
<td>Sets affinity for a Check Point daemon, where <em>&lt;cpdname&gt;</em> 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 <em>&lt;instance&gt;</em> is the instance's number.</td>
</tr>
<tr>
<td>-i &lt;interfacename&gt;</td>
<td>Sets affinity for an interface, where <em>&lt;interfacename&gt;</em> 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 R75.40 Firewall Administration Guide [http://supportcontent.checkpoint.com/solutions?id=sk67581].

**Usage**  
```
fw ctl affinity -l [<proc_selection>] [<listtype>]
```

**Syntax**  
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:
**Parameter** | **Description**  
--- | ---  
-p <pid> | Displays the affinity of a particular process, where *<pid>* is the process ID#.

-n <cpdname> | Displays the affinity of a Check Point daemon, where *<cpdname>* is the Check Point daemon name (for example: fwd).

-k <instance> | Displays the affinity of a kernel instance, where *<instance>* is the instance’s number.

-i <interfacename> | Displays the affinity of an interface, where *<interfacename>* is the interface name (for example: eth0).

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:

**Parameter** | **Description**  
--- | ---  
-a | All: includes items without specific affinities.

-r | Reverse: lists each processing core and the items that have it as their affinity.

-v | Verbose: list includes additional information.

**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.

**Usage**  
```
fw ctl engine {on | off | stat | setdefault}
```

**Syntax**

<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*.

| off | Deactivates the engine if active. Subsequent policy installation on the gateway does NOT auto-activate the engine unless the command is used again.

| stat | Print the status of the engine. For example: "During compilation", "Before auto-activation", "Deactivated". |
### setdefault

**Description**

Restore control to database settings. Security Management server settings are ignored.

At the next policy installation, return the control of the engine to the values of the following gateway database attributes:

- **inspect2c_compile** *(true/false)* - 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.
- **inspect2c_activate** *(true/false)* - controls whether the engine is automatically activated after it is compiled. When set to true, the engine is compiled regardless of the value of **inspect2c_compile**.

Use GuiDBEdit to change the values of the attributes.

### 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.

**Usage**

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

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>fw ctl zdebug &gt;&amp; outputfile</code></td>
<td>Turn on debug mode and specify an output file.</td>
</tr>
<tr>
<td><code>fw ctl sdstat start</code></td>
<td>Activate the IPS counters</td>
</tr>
<tr>
<td><code>fw ctl sdstat stop</code></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><code>sdstat_get_stats_all_instances : Smart Defense report objects are not initialized, hence no report can be done.</code></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><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**

Fetched the Inspection Code from the specified host and installs it to the kernel.

**Usage**

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

**Syntax**

<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 <code>state</code> 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 <code>filename</code> is not specified, the list in <code>conf/masters</code> is used.</td>
</tr>
<tr>
<td><code>-c</code></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><code>-i</code></td>
<td>Ignore SIC information (for example, SIC name) in the database and use the information in <code>conf/masters</code>. 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>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</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 <strong>targets</strong> is not specified, or if <strong>targets</strong> is inaccessible, the Policy is fetched from <strong>localhost</strong>.</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.

**Usage**  
*fw fetchlogs* [[-\* file name] ...] *module*

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-* filename</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 <em>.log</em>. Related pointer files will automatically be fetched.</td>
</tr>
<tr>
<td>module</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 -\* 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
```

**Further Info.**  
See the [R75.40 Security Management Administration Guide](http://supportcontent.checkpoint.com/solutions?id=sk67581).
**fw hastat**

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

**Usage**  `fw hastat [<target>]`

**Syntax**

<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.

**Usage**  `fw isp_link [target] link-name {up|down}`

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>The name of the Check Point 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 `snmpd` daemon is: `$FWDIR/tmp/snmpd.pid`.

**Usage**  `fw kill [-t sig_no] proc-name`

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-t sig_no</td>
<td>This Unix only command specifies that if the file <code>$FWDIR/tmp/proc-name.pid</code> exists, send signal <code>sig_no</code> to the pid given in the file. If no signal is specified, signal 15 (<code>sigterm</code> or the <code>terminate</code> command) is sent.</td>
</tr>
<tr>
<td>proc-name</td>
<td>Prompt the kernel to shut down specified firewall daemon processes.</td>
</tr>
</tbody>
</table>

**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.

**Usage**  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

**Usage**  fw lichosts [-x] [-l]

**Syntax**

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

fw log

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

**Usage**  fw log [-f [-t]] [-n] [-l] [-o] [-c action] [-h host] [-s starttime] [-e endtime] [-b starttime endtime] [-u unification_scheme_file] [-m unification_mode(initial|semi|raw)] [-a] [-k (alert_name|all)] [-g] [logfile]

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f [-t]</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.</td>
</tr>
</tbody>
</table>

The -t 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.

-t must come with a -f flag. These flags are relevant only for active files.

- n  Do not perform DNS resolution of the IP addresses in the Log file (the default behavior). This option significantly speeds up the processing.

- l  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).

- o  Show detailed log chains (all the log segments a log record consists of).
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-c action</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 host</code></td>
<td>Display only log whose origin is the specified IP address or name.</td>
</tr>
<tr>
<td><code>-s starttime</code></td>
<td>Display only events that were logged after the specified time (see time format below). starttime may be a date, a time, or both. If date is omitted, then today's date is assumed.</td>
</tr>
<tr>
<td><code>-e endtime</code></td>
<td>Display only events that were logged before the specified time (see time format below). endtime may be a date, a time, or both.</td>
</tr>
<tr>
<td><code>-b starttime endtime</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 unification_scheme_file</code></td>
<td>Unification scheme file name.</td>
</tr>
<tr>
<td><code>-m unification_mode</code></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 <code>-f</code>, 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><code>-a</code></td>
<td>Output account log records only.</td>
</tr>
<tr>
<td><code>-k alert_name</code></td>
<td>Display only events that match a specific alert type. The default is all, for any alert type.</td>
</tr>
<tr>
<td><code>-g</code></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>
<tr>
<td><code>logfile</code></td>
<td>Use logfile instead of the default Log file. The default Log File is $FWDIR/log/fw.log.</td>
</tr>
</tbody>
</table>

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
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

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;

14:57:49 keyinst jam.checkpoint.com >daemon src:
veredr.checkpoint.com; peer gateway: veredr.checkpoint.com; scheme:
IKE; IKE: Main Mode completion.; CookieI: 32f09ca38aeaf4a3; 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 an 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 179) and fw fetchlogs (on page 170).

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

Usage  fw logswitch [-audit] [filename]

fw logswitch -h hostage [+-]filename

Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-audit</td>
<td>Does logswitch for the Security Management server audit file. This is relevant for local activation.</td>
</tr>
<tr>
<td>filename</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>
</tbody>
</table>
### fw logswitch

**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.

**Usage**
```
fw mergefiles [-s] [-t time_conversion_file] log_file_name_1 [... log_file_name_n] output_file
```

**Syntax**
### Gaia Administration Guide R75.40

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td>Sort merged file by log records time field.</td>
</tr>
<tr>
<td>-t time_conversion_file</td>
<td>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</td>
</tr>
<tr>
<td>log_file_name_n</td>
<td>Full pathnames of the Log File(s).</td>
</tr>
<tr>
<td>output_file</td>
<td>Full pathname of the output Log File.</td>
</tr>
</tbody>
</table>

**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.

**Usage**

```
```

**Syntax**
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`-u</td>
<td>s`</td>
</tr>
<tr>
<td><code>-i</code></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 <code>fw</code> monitor process and want to be sure that all data is written to a file.</td>
</tr>
<tr>
<td><code>[-d] [-D]</code></td>
<td><strong>Debugging fw monitor:</strong> The <code>-d</code> option is used to start fw monitor in debug mode. This will give you an insight into <code>fw</code> monitor's inner workings. This option is only rarely used outside Check Point. It is also possible to use <code>-D</code> 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>| <code>-l len</code> | <strong>Limiting the packet length:</strong> <code>fw</code> monitor allow you to limit the packet data which will be read from the kernel with <code>-l</code>. This is especially useful if you have to debug high sensitive communication. It allows 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. <code>fw</code> 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. |
| <code>-m mask</code> | <strong>Setting capture masks:</strong> By default <code>fw</code> 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. |
| <code>-x offset[,len]</code> | <strong>Printing packet/payload data:</strong> In addition to the IP and Transport header <code>fw</code> monitor can also print the packets' raw data using the <code>-x</code> 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>
<tbody>
<tr>
<td>-o &lt;file&gt;</td>
<td><strong>Write output to file:</strong> 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. <strong>Note</strong> - The snoop file format is normally used to store Layer 2 frames. For &quot;normal&quot; capture files this means that the frame includes data like a source and a destination MAC address. <code>fw</code> monitor operates in the firewall kernel and therefore has no access to Layer 2 information like MAC addresses. Instead of writing random MAC addresses, <code>fw</code> monitor includes information like interface name, direction and chain position as &quot;MAC addresses&quot;.</td>
</tr>
<tr>
<td>-T</td>
<td>Print time stamp in microseconds. <code>-T</code> is needed only when <code>-o</code> is not used. When <code>-o</code> is used the exact time is written to the snoop file by default as of Corsica.</td>
</tr>
<tr>
<td>[&lt;pi pos] [-pI pos] [-po pos] [-p0 pos] [-p all]</td>
<td><strong>Insert <code>fw</code> monitor chain module at a specific position:</strong> In addition to capture masks (which give the ability to look at packets in a specific position) <code>fw</code> monitor has the ability to define where exactly in the firewall chain the packets should be captured. This can be defined using these options.</td>
</tr>
<tr>
<td>-a</td>
<td><strong>Use absolute chain positions:</strong> If you use <code>fw</code> monitor to output the capture into a file (option <code>-o</code>), one of the fields written down to the capture file is the chain position of the <code>fw</code> monitor chain module. Together with a simultaneous execution of <code>fw ctl chain</code> you can determine where the packet was captured. Especially when using <code>-p all</code> you will find the same packet captured multiple times at different chain positions. The option <code>-a</code> changes the chain id from a relative value (which only makes sense with the matching <code>fw ctl chain</code> output) to an absolute value. These absolute values are known to CPEthereal and can be displayed by it.</td>
</tr>
<tr>
<td>[-ci count] [-co count]</td>
<td><strong>Capture a specific number of packets:</strong> <code>fw</code> 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 <code>fw</code> 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.</td>
</tr>
<tr>
<td>-h</td>
<td>Displays the usage.</td>
</tr>
</tbody>
</table>

**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 gateway. Please note that the same packet is appearing several times (two times in the example below). This is caused by `fw` monitor capturing the packets at different capture points.

**Output**
### Security Management

Server and Firewall Commands

<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>

#### cpmodule]

```bash
# 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

```bash
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

```bash
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.


### fw lslogs

**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.

**Usage** `fw lslogs [ -f <filename> ] ... [ -e ] [ -s name | size | stime | etime ] [ -r ] [ <machine> ]`

**Syntax**

<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>
### Parameter 
**Description**
- **-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
<table>
<thead>
<tr>
<th>Size</th>
<th>Creation Time</th>
<th>Closing Time</th>
<th>Log file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>16KB</td>
<td>10Jan2002 18:36:05</td>
<td>--</td>
<td>fw.log</td>
</tr>
</tbody>
</table>
```

### 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.

**Usage**
```
fw putkey [-opsec] [-no_opsec] [-ssl] [-no_ssl] [-k num] [-n <myname>] [-p <pswd>] [host...]
```

**Syntax**

<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>-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>
</tbody>
</table>
### 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.

**Usage** fw repairlog [-u] logfile

**Syntax**

<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>logfile</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.

**Usage** Add/Cancel SAM rule according to criteria:

```
fw sam [-v][-s <sam server>][-S <server sic name>][-f <fw host>][-t timeout][-l 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:
Monitor SAM rules according to criteria:

\[
\text{fw sam } [-v][-s \text{ <sam server>}] [-S \text{ <server sic name>}] [-f \text{ <fw host>}] \text{ -M -ijn all}
\]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</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 \text{ sam_server})</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 \text{ server_sic_name})</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>
<tr>
<td>(-f \text{ &lt;fw host&gt;})</td>
<td>Specify the host, the Security Gateway machine on which to enforce the action.</td>
</tr>
<tr>
<td>(-D)</td>
<td>Cancel all inhibit ((-i, -j, -I, -J)) and notify ((-n)) commands. To &quot;uninhibit&quot; inhibited connections, execute \text{fw sam} with the (-C) or (-D) parameters. It is also possible to use this command for active SAM requests.</td>
</tr>
<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 (-t) (timeout) parameter.</td>
</tr>
<tr>
<td>(-t \text{ timeout})</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 \text{ log})</td>
<td>The type of the log for enforced actions can be one of the following: nolog, long_noalert, long_alert. The default is long_alert.</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>Parameter</td>
<td>Meaning</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</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:

\[
<\text{source ip}><\text{source netmask}><\text{destination ip}><\text{destination netmask}><\text{service}><\text{protocol}>
\]

Possible combinations are:

- \text{src <ip>}
- \text{dst <ip>}
- \text{any <ip>}
- \text{subsrc <ip><netmask>}
- \text{subdst <ip><netmask>}
- \text{subany <ip><netmask>}
- \text{srv <src ip><dest ip><service><protocol>}
- \text{subsrv <src ip><src netmask><dest ip><dest netmask><service><protocol>}
- \text{subsrvd <src ip><src netmask><dest ip><dest netmask><service><protocol>}
- \text{dstsrv <dest ip><service><protocol>}
- \text{subdstsrv <dest ip><dest netmask><service><protocol>}
- \text{srcpr <ip><protocol>}
- \text{dstpr <ip><protocol>}
- \text{subsrcpr <ip><netmask><protocol>}
- \text{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>Criteria Parameters</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>subany &lt;ip&gt; &lt;netmask&gt;</strong></td>
<td>Match either the source IP address or destination IP address of connections according to the netmask.</td>
</tr>
<tr>
<td><strong>srv &lt;src ip&gt; &lt;dst ip&gt; &lt;service&gt; &lt;protocol&gt;</strong></td>
<td>Match the specific source IP address, destination IP address, service and protocol.</td>
</tr>
<tr>
<td><strong>subsrv &lt;src ip&gt; &lt;netmask&gt; &lt;dst ip&gt; &lt;netmask&gt; &lt;service&gt; &lt;protocol&gt;</strong></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><strong>subsrvs &lt;src ip&gt; &lt;src netmask&gt; &lt;dest ip&gt; &lt;netmask&gt; &lt;service&gt; &lt;protocol&gt;</strong></td>
<td>Match the specific source IP address, source netmask, destination netmask, service and protocol.</td>
</tr>
<tr>
<td><strong>subsrvd &lt;src ip&gt; &lt;dest ip&gt; &lt;dest netmask&gt; &lt;service&gt; &lt;protocol&gt;</strong></td>
<td>Match specific source IP address, destination IP, destination netmask, service and protocol.</td>
</tr>
<tr>
<td><strong>dstsrv &lt;dst ip&gt; &lt;service&gt; &lt;protocol&gt;</strong></td>
<td>Match specific destination IP address, service and protocol.</td>
</tr>
<tr>
<td><strong>subdstsrv &lt;dst ip&gt; &lt;netmask&gt; &lt;service&gt; &lt;protocol&gt;</strong></td>
<td>Match specific destination IP address, service and protocol. Destination IP address is assigned according to the netmask.</td>
</tr>
<tr>
<td><strong>srcpr &lt;ip&gt; &lt;protocol&gt;</strong></td>
<td>Match the source IP address and protocol.</td>
</tr>
<tr>
<td><strong>dstpr &lt;ip&gt; &lt;protocol&gt;</strong></td>
<td>Match the destination IP address and protocol.</td>
</tr>
<tr>
<td><strong>subsrcpr &lt;ip&gt; &lt;netmask&gt; &lt;protocol&gt;</strong></td>
<td>Match the source IP address and protocol of connections. Source IP address is assigned according to the netmask.</td>
</tr>
<tr>
<td><strong>subdstpr &lt;ip&gt; &lt;netmask&gt; &lt;protocol&gt;</strong></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:

```bash
dfw 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:

```bash
dfw 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:

```bash
dfw 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 louvre is the source or destination address:

```bash
dfw sam -M -nij any louvre
```

This command cancels the command in the first example:

```bash
dfw 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`

**Usage**

```
fw stat -l
fw stat -s
```

**Syntax**

<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**

```
>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:

```
>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 enables you to view the contents of kernel tables, and change the content of dynamic kernel tables. Static kernel tables cannot be changed.

Kernel tables (also known as State tables) are used to keep state information which the firewall virtual machine, and other components of the Security Gateway need to correctly inspect the packet. The tables are actually the 'memory' of the virtual machine in the kernel, and are the key component of Check Point Stateful Inspection technology. State tables are implemented as dynamic hash tables in kernel memory. All field values are in hexadecimal, apart from the time-out value at the end of the entry, when present.

**Usage**

```
```

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-t &lt;table&gt;</td>
<td>Specifies a table for the command.</td>
</tr>
<tr>
<td>-s</td>
<td>Displays a short summary of the table(s) information.</td>
</tr>
<tr>
<td>-y</td>
<td>Specifies to not prompt a user before executing any commands.</td>
</tr>
<tr>
<td>-f</td>
<td>Displays a formatted version of the table content. Every table may have its own specific format style.</td>
</tr>
</tbody>
</table>
### Security Management

#### Server and Firewall Commands

**Gaia Administration Guide R75.40**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-o &lt;filename&gt;</td>
<td>Dumps CL formatted output to filename, which can later be read by fw log or any other entity that can read FW log formats.</td>
</tr>
<tr>
<td>-c</td>
<td>Displays formatted table information in common format.</td>
</tr>
<tr>
<td>-r</td>
<td>Resolves IP addresses in formatted output.</td>
</tr>
<tr>
<td>-x, -a, -e</td>
<td>It is possible to add or remove an entry from an existing dynamic table by using the -a or the -x flags, respectively. These flags must be followed by the -e flag and an entry description (&lt;entry&gt;).</td>
</tr>
</tbody>
</table>

**Caution** - Improper use of the -a and -x flags may cause system instability.

| [hostname] | A list of one or more targets. When not used, the local machine is used as the default target. |

**Example**

```
fw tab -t <table-name> -a -e "1,2;3,4,5" or
fw tab -t <table-name> -a -e "<1,2;3,4,5>"
```

Adds an entry: `<00000001,00000002,00000003,00000004,00000005,>` to <table-name>.

```
fw tab -t <table-name> -a -e "1,2," or
fw tab -t <table-name> -a -e "<1,2>"
```

Adds an entry with only a key field: `<00000001,00000002>`

If <table><table-name> contains the following entry:

```
<00000000,00000001,00000002>
```

```
fw tab -t <table-name> -x -e "0,1" or
fw tab -t <table-name> -x -e "0,1;2"
```

Removes the entry from the specified table.

**Comments**

If table has the 'expire' attribute, entries added using the -a flag will receive the default table timeout.

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.

**Usage**

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

**Syntax**

<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 &lt;filename&gt;</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.

**Usage**  
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*.

**Usage**  
fwm dbimport [-m] [-s] [-v] [-r] [-k errors] [-f file] [-d delim]

**Syntax**

<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><em>fwm dbimport</em> will delete all existing users in the database.</td>
</tr>
<tr>
<td>-k errors</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 file</td>
<td>The name of the import file. The default import file is <code>$FWDIR/conf/user_def_file</code>. Also see the requirements listed under “File Format” on page 72.</td>
</tr>
<tr>
<td>-d delim</td>
<td>Specifies a delimeter 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:
    
    ```text
    {name; groups; destinations; sources; auth_method; fromhour; tohour; expiration_date; color; days; internal_password; SKEY_seed; SKEY_passwd; SKEY_gateway; template; comments; userc}
    ```
  - The attributes must be separated by a delimeter 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.

**Usage**  fw expdate dd-mmm-1976

**Comments**  The date can be modified using a filter.

**Example**  fw expdate 02-mar-2003 -f 01-mar-2003

**fwm dbexport**

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

• the same Usage as the import file for fwm dbimport

• LDIF format, which can be imported into an LDAP server using ldapmodify

**Usage**  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:
**Syntax**

```
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**

- 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:

<table>
<thead>
<tr>
<th>DN</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn=ben,o=WidgetCorp,c=us</td>
</tr>
<tr>
<td>cn=maryj,o=WidgetCorp,c=us</td>
</tr>
</tbody>
</table>

### 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.

**Usage**  
fwm dbload [-all | -conf <conffile>] [<targets>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>-conf &lt;conffile&gt;</td>
<td>Only OPSEC control connections 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.

**Usage**  
fwm ikecrypt shared-secret user-password

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

### fw getcap

**Description**  
fwm getcap command line fetches the packet capture.

**Usage**  
fwm getcap -g <gw> -u "{CAP_ID}" [-p <path>] [-c <domain>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-g</td>
<td>Host name of the gateway</td>
</tr>
<tr>
<td>-u</td>
<td>Capture UID</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>-p</td>
<td>Output pathname</td>
</tr>
<tr>
<td>-c</td>
<td>Host name of the Domain Management Server</td>
</tr>
</tbody>
</table>

**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.

**Usage**  
fwm load [\-p <plug-in product name>] [-S] <rulebase version name> <targets>

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-S</td>
<td>The targets are UTM-1 Edge gateways.</td>
</tr>
<tr>
<td>-p</td>
<td>Specifies the product name if applicable.</td>
</tr>
<tr>
<td>rulebase</td>
<td>A Rule Base created by the GUI. Specify the name of the rulebase, such as Standard (case sensitive).</td>
</tr>
<tr>
<td>-v version number</td>
<td>Retrieve the Security Policy from the version repository. The version number represents the number of the Security Policy as it is saved in the version repository.</td>
</tr>
<tr>
<td>targets</td>
<td>Execute command on the designated target.</td>
</tr>
</tbody>
</table>

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

```
fwm load -v18 Standard johnny
```

**fwm lock_admin**

**Description**  View and unlock locked administrators.

**Usage**  
fwm lock_admin [-v][-u administrator][-ua]

**Syntax**

<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 administrator</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 delimiter</td>
<td>Set the output delimiter. The default is a semicolon (;).</td>
</tr>
<tr>
<td>-i filename</td>
<td>The name of the input Log file. The default is the active Log file, fw.log</td>
</tr>
<tr>
<td>-o outputfile</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>
<tr>
<td>-m</td>
<td>This flag specifies the unification mode.</td>
</tr>
<tr>
<td>-a</td>
<td>Show account records only (the default is to show all records).</td>
</tr>
</tbody>
</table>

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 records 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;;
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).

**Usage**  
fwm sic_reset

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sic_reset</td>
<td>Resets the internal CA SIC certificates and deletes the Internal CA.</td>
</tr>
</tbody>
</table>

**fwm unload <targets>**

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

**Usage**  
fwm unload <targets>[-all | -conf conffile]

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targets</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>conf conffile</td>
<td>Execute command on targets specified in the conffile.</td>
</tr>
</tbody>
</table>

**fwm ver**

**Description**  
fwm ver displays the build number.

**Usage**  
fwm ver [-f <filename>]

**fwm verify <policy-name>**

**Description**  
The fwm verify <policy-name> command verifies the specified policy package without installing it.
**Usage**

`fwm verify <policy-name>`

**Syntax**

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

Usage  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 <object name> -cert <certificate name>`: 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 goes to the specified directory, 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.

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

    vpn crlview -f <filename>
    vpn crlview -view

Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-obj</td>
<td>-obj refers to the name of the CA network object</td>
</tr>
<tr>
<td>-cert</td>
<td>-cert refers to the name of the certificate</td>
</tr>
<tr>
<td>-f</td>
<td>Refers to the filename of the certificate</td>
</tr>
</tbody>
</table>
VPN Commands

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-view</td>
<td>Views the CRL</td>
</tr>
<tr>
<td>-d</td>
<td>Debug option</td>
</tr>
</tbody>
</table>

**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

**Usage**

Usage: 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

**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 associated with this topic at the specified level (or higher) are sent to $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 (changes the current vpnd.elg file to vpnd0.elg and creates a new vpnd.elg), enables vpnd and ike debugging and adds a timestamp to the vpnd.elg file.</td>
</tr>
</tbody>
</table>

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

**Example**

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.

**Usage**  
- `vpn drv on|off`
- `vpn drv stat`

**Syntax**

<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 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.

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

**Syntax**

<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**  
```
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.

**Usage**  
```
vpn macutil <username>
```

**Example**  
```
vpn macutil John
```

**Output**  
```
20-0C-EB-26-80-7D, "John"
```
**vpn nssm_topology**

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

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

**Syntax**

<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>
<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 XLM format. This flag writes that topology to a file in XLM 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

**Usage**  
```bash  
vpn overlap_encdom [communities | traditional]  
```

**Syntax**

<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**  
```bash  
vpn overlap_encdom communities  
```
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.

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

**Syntax**

<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.

**Usage**  
```shell
tunnelutil
```

**Example**  
```shell
tunnelutil
```

**Output**
VPN Commands

********** 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.

Usage: `vpn ver [\-k] -f <filename>`

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ver</td>
<td>Displays the version name and version build number</td>
</tr>
<tr>
<td>-k</td>
<td>Displays the version name and build number and the kernel build number</td>
</tr>
<tr>
<td>-f</td>
<td>Prints the version number and build number to a text file.</td>
</tr>
</tbody>
</table>
Chapter 14

SmartView Monitor Commands

In This Chapter

Overview

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>

Syntax

<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 `<module_name>{<interface_name>|-filter "<complex filter>"}`

**Description**  
Starts the monitoring process and specify parameters for monitoring an interface.

**Usage**  
rtm monitor `<module_name>{<interface_name>}[options]-g<grouping> [entity-1...entity-n]`

or

rtm monitor `<module_name>-filter["complex filter"][options]-g<grouping> [entity-1...entity-n]`

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>`&lt;aggregate</td>
</tr>
<tr>
<td>-w</td>
<td>`&lt;bandwidth</td>
</tr>
<tr>
<td>-t</td>
<td>`&lt;wire</td>
</tr>
<tr>
<td>-i</td>
<td><code>&lt;number of seconds&gt;</code></td>
</tr>
<tr>
<td>@@</td>
<td>specifies subrule (for example, ‘rule@@subrule’)</td>
</tr>
<tr>
<td>default values</td>
<td><code>-y bytes -a aggregate -w bandwidth -i2</code></td>
</tr>
<tr>
<td>grouping types</td>
<td>`svc</td>
</tr>
<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>-d</td>
<td>Specifies one of the following monitor directions:</td>
</tr>
<tr>
<td></td>
<td>- inbound</td>
</tr>
<tr>
<td></td>
<td>- outbound</td>
</tr>
<tr>
<td></td>
<td>- eitherbound</td>
</tr>
<tr>
<td>inbound</td>
<td>Monitors the inbound direction.</td>
</tr>
<tr>
<td>outbound</td>
<td>Monitors the outbound direction.</td>
</tr>
<tr>
<td>eitherbound</td>
<td>Monitors both directions.</td>
</tr>
<tr>
<td>-y</td>
<td>Specifies one of the following measurement units:</td>
</tr>
<tr>
<td></td>
<td>- bytes</td>
</tr>
<tr>
<td></td>
<td>- pkts</td>
</tr>
<tr>
<td></td>
<td>- line</td>
</tr>
<tr>
<td>c</td>
<td>Indicates the number of new connections opened per second.</td>
</tr>
<tr>
<td>C</td>
<td>Average concurrent connections</td>
</tr>
<tr>
<td>-a</td>
<td>Aggregate - displays a specific type of connections as an aggregate.</td>
</tr>
<tr>
<td></td>
<td>Individual - displays a specific type of connections as an individual. The default is eitherbound.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| -g        | Specifies one of the following grouping options for monitored traffic:  
|           | - svc  
|           | - src  
|           | - dst  
|           | - ip   
|           | - fgrule  
|           | - topsvc  
|           | - topsrc  
|           | - topdst  
|           | - topfdst  
|           | - topfwm  
|           | - topfgrule  
| svc       | Monitors according to a service.  
| src       | Monitors according to a network object (source only).  
| dst       | Monitors according to a network object (destination only).  
| ip        | Monitors according to a network object (source and destination).  
| fgrule    | Monitors according to a QoS Policy rule.  
| topsvc    | Monitors the traffic of the top 50 services.  
| topsrc    | Monitors the traffic of the top 50 sources.  
| topdst    | Monitors the traffic of the top 50 destinations.  
| topfdst   | Monitors traffic to and from the top 50 IP addresses (source of destination).  
| topfwm    | Monitors according to the top 50 Firewall rules.  
| topfgrule | Monitors according to the top 50 QoS Policy rules.  
| -p        | Specifies whether or not thousands will be separated by commas.  
| -filter   | ["<complex filter>"] Only monitors traffic that matches the complex -filter Boolean expression.  

**Example**  
The following command line displays monitoring data in bytes-per-sec for the top 50 services passed on any interface in both directions:
```
rtm monitor localhost -filter -g topsvc
```

The following command will display monitoring data in Conncurrent-Connections for the top 50 sources passed on interface eth0, inbound (that is, not telnet of http).
rtm monitor localhost -filter "[and[[interface 0 [[eth0in]]][svc 1 [telnet http]]]]" -y C -g topsrc

The default monitors all traffic on any interface in both directions.

**Comments** The specified entities should correspond to the specified grouping option. For example, if the monitoring process works according to a service (svc), all of the monitored services should be listed and separated by single spaces.

When monitoring occurs according to the QoS Policy rule (fgrule), "rule@@subrule" should be used to specify a subrule entity.

There is no need to specify the top grouping options since they automatically monitor the top 50 entities according to the specified group.

**Example** The following command displays monitoring data in bytes-per-sec for the top 50 services passed on interface hme1.

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

**rtm monitor <module_name>-v<virtual_link_name>**

**Description** Start the monitoring process and specifies parameters for monitoring a Virtual Link.

**Usage** `rtm monitor <module_name>-v<virtual_link_name>[options]entity-1... entity-n`

**Syntax**

<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>virtual-link-name</td>
<td>The name of the monitored Virtual Link.</td>
</tr>
<tr>
<td>-d</td>
<td>Specifies one of the following monitoring directions:</td>
</tr>
<tr>
<td></td>
<td>- a2b</td>
</tr>
<tr>
<td></td>
<td>- b2a</td>
</tr>
<tr>
<td></td>
<td>- a2b_b2a</td>
</tr>
<tr>
<td>a2b</td>
<td>Monitors End Point A to End Point B.</td>
</tr>
<tr>
<td>b2a</td>
<td>Monitors End Point B to End Point A.</td>
</tr>
<tr>
<td>a2b_b2a</td>
<td>Monitors both directions.</td>
</tr>
<tr>
<td>-y</td>
<td>Specifies one of the following measurement units. It is only required when the -w value is bandwidth.</td>
</tr>
<tr>
<td></td>
<td>- bytes</td>
</tr>
<tr>
<td></td>
<td>- pkts</td>
</tr>
<tr>
<td>-w</td>
<td>Specifies the displayed data type.</td>
</tr>
<tr>
<td>bandwidth</td>
<td>Displays the effective bandwidth.</td>
</tr>
<tr>
<td>loss</td>
<td>Displays the difference between the transmission rate and the receiving rate.</td>
</tr>
<tr>
<td>rtt</td>
<td>Displays the time required to make the round trip between the two End Points.</td>
</tr>
</tbody>
</table>
### SmartView Monitor Commands

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-t</td>
<td>Specifies the data type. It is only required when the -w value is bandwidth.</td>
</tr>
<tr>
<td>wire</td>
<td>Shows the data on the wire after compression or encryption.</td>
</tr>
<tr>
<td>application</td>
<td>Shows the data as the application sees it (that is, not compressed and not encrypted).</td>
</tr>
</tbody>
</table>

### 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
Chapter 15

ClusterXL Commands

In This Chapter

- cphaconf 207
- cphaprob 208
- cphastart 208
- cphastop 208

**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 <machine id>] [-p <policy id>] [-b <db_id>] [-n <cluster num>] [-c <cluster 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>
<tbody>
<tr>
<td>set_ccp &lt;broadcast/multicast&gt;</td>
<td>Sets whether Cluster 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 cluster members.</td>
</tr>
</tbody>
</table>

| stop_all_vs | Stops the cluster 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.
Index

3
32 and 64-bit Gaia Editions • 20

6
6in4 Tunnel Interfaces • 52

A
Advanced Routing • 97
Advanced VRRP • 126
Aliases • 35
ARP • 55
Authentication Servers • 109

B
Backrestoring the System - CLI (Backup) • 143
Backing Up and Restoring the System - WebUI • 143
Before Configuring VRRP • 120
Bond Interfaces (Link Aggregation) • 39
Bridge Interfaces • 45

C
Change My Password • 98
Change My Password - CLI (selfpasswd) • 98
Changing System Edition • 28
CLI Configuration Procedures for VPN Tunnel Interfaces • 50
CLI Procedures • 38, 67, 106
CLI Procedures - IPv6 Static Routes • 70
CLI Procedures- Software Updates • 153
CLI Reference (interface) • 30
Client Environment Output Format • 23
ClusterXL Commands • 206
Command Completion • 17
Command History • 18
Command Line Movement and Editing • 19
Command Reuse • 18
Commands and Features • 15
Completing the VTI Configuration • 51
Configuration Tab • 13
Configuration using the CLI • 46
Configuration Using the CLI • 37
Configuration using the WebUI • 35
Configuring 6in4 Tunnel Interfaces - CLI (interface) • 52
Configuring 6in4 Tunnel Interfaces - WebUI • 52
Configuring a DHCP Server - CLI (dhcp) • 58
Configuring a DHCP Server - WebUI • 58
Configuring a Software Deployment Policy - WebUI • 150
Configuring a Virtual Router - CLI (mcrv) • 123
Configuring a Virtual Router - WebUI • 122
Configuring Advanced VRRP - CLI (vrp) • 128
Configuring Advanced VRRP - WebUI • 126
Configuring Aliases - CLI (interface) • 36

Configuring Allowed Gaia Clients - CLI (allowed-client) • 96
Configuring Allowed Gaia Clients - WebUI • 95
Configuring ARP - CLI (arp) • 56
Configuring ARP- WebUI • 55
Configuring Bond Interfaces - CLI • 40
Configuring Bond Interfaces - WebUI • 39
Configuring Bridge Interfaces - CLI (bridging) • 45
Configuring Bridge Interfaces - WebUI • 45
Configuring DNS - CLI (dns) • 63
Configuring DNS - WebUI • 63
Configuring Gaia as a RADIUS Client • 112
Configuring Gaia as a TACACS+ Client • 113
Configuring Global Settings for VRRP • 121
Configuring Host Name - CLI (hostname) • 61
Configuring Host Name - WebUI • 61
Configuring Hosts - CLI (host) • 62
Configuring Hosts- WebUI • 62

Configuring Image Management - CLI (snapshot) • 141
Configuring Image Management - WebUI • 140
Configuring IPv4 Static Routes - WebUI • 65
Configuring IPv6 Static Routes - CLI (ipv6 static-route) • 69
Configuring IPv6 Static Routes - WebUI • 68
Configuring Job Scheduler - CLI (cron) • 86
Configuring Job Scheduler - WebUI • 85
Configuring Licenses - CLI (cplic) • 133
Configuring Licenses - WebUI • 132
Configuring Log Volume - CLI (volume) • 92
Configuring Loopback Interfaces - CLI (interface) • 47
Configuring Loopback Interfaces - WebUI • 46
Configuring Mail Notification - CLI (mail-notification) • 88
Configuring Mail Notification - WebUI • 88
Configuring Many Static Routes at Once • 65
Configuring Messages - CLI (message) • 89
Configuring Messages - WebUI • 88
Configuring Network Switches • 120
Configuring NTP - CLI (ntp) • 73
Configuring Password Policy - CLI (password-controls) • 108
Configuring Password Policy- WebUI • 107
Configuring Physical Interfaces - CLI (interface) • 34
Configuring Physical Interfaces - WebUI • 33
Configuring PPPoE Interfaces - CLI (pppoe) • 54
Configuring PPPoE Interfaces- WebUI • 54
Configuring RADIUS Servers - CLI (aaa) • 111
Configuring RADIUS Servers - WebUI • 110
Configuring RADIUS Servers for Non-Local Users • 112
Configuring Roles - CLI (rba) • 105
Configuring Roles - WebUI • 103
Configuring Scheduled Backups - CLI (backup-scheduled) • 145
Configuring Scheduled Backups - WebUI • 144
Configuring SNMP - CLI (snmp) • 79
Configuring SNMP - WebUI • 77
Configuring Software Deployment – clish (installation) • 152
Configuring Software Deployment - WebUI • 151
Configuring Software Update Notifications - WebUI • 151
Configuring Static Routes - CLI (static-route) • 66
Configuring System Groups - CLI (group) • 115
Configuring System Groups - WebUI • 114
Configuring System Logging - CLI (syslog) • 91
Configuring System Logging - WebUI • 91
Configuring TACACS+ Servers - CLI (aaa) • 112
Configuring TACACS+ Servers - WebUI • 112
Configuring TACACS+ Servers for Non-Local Users • 114
Configuring Telnet Access - CLI (netaccess) • 93
Configuring Telnet Access - WebUI • 93
Configuring the Check Point Security Gateway for VRRP • 128
Configuring the IPv6 Support - CLI • 90
Configuring the IPv6 Support - WebUI • 90
Configuring the Session - CLI (inactivity-timeout) • 90
Configuring the Session - WebUI • 90
Configuring the WebUI Web server • 93
Configuring VLAN Interfaces - WebUI • 36
Configuring VPN Tunnel Interfaces • 48
Configuring VPN Tunnel Interfaces - CLI (vpn tunnel) • 49
Configuring VPN Tunnel Interfaces - WebUI • 48
Configuring VRRP Rules for Check Point Security Gateway • 120
cpcl • 157
cpcl admin • 157
cpcl auto • 158
cpcl ca • 157
cpcl client • 158
cpcl finger • 157
cpcl ha • 158
cpcl lic • 157
cpcl sic • 157
cpcl snmp • 158
cpcl sxl • 158
cpca_client • 155
cpca_client create_cert • 155
cpca_client lscert • 156
cpca_client revoke_cert • 155
cpca_client set_mgmt_tools • 156
cpcconfig • 158
cphaconf • 206
cphaprof • 207
cphastart • 207
cphastop • 207
cpinfo • 159
cplic check • 133
cplic db_add • 134
cplic db_print • 135
cplic db_rm • 135
cplic del • 135
cplic del <object name> • 136
cplic get • 136
cplic print • 138
cplic put • 137
fclic put <object name> ... • 138
cfclic upgrade • 139
cpstart • 159
cpstat • 160
cpstop • 161
Creating or Deleting a Bond Interface • 42
D
Defining Directional Matching VPN Rules • 50
Defining Load Sharing Parameters • 44
Defining Rules to Allow OSPF Traffic • 51
Defining Slave Interfaces • 42
Defining the ARP monitoring interval • 43
Defining the Bond Operating Mode • 42
Defining the Media Monitoring Interval • 43
Defining the Primary Slave Interface • 43
Defining the UP and Down Delay Times • 44
Defining the VPN Community • 48
Defining VPN Rules • 50
DHCP Server • 57
Do Not Cascade Switches • 120
Domain Name Service (DNS) • 63
Download SmartConsole • 147
Download SmartConsole - WebUI • 147
E
Enabling Virtual Routers • 121
Environment Commands • 21
Expert Mode • 23
F
Firewall Policies • 131
fw • 162
fw ct • 162
fw ct aff • 165
fw ct aff -i • 165
fw ct aff -s • 165
fw ct debug • 163
fw ct engine • 166
fw ct multik stat • 167
fw ct sdstat • 167
fw fetch • 168
fw fetchlogs • 169
fw getcap • 189
fw hastat • 170
fw -i • 162
fw isp_link • 170
fw kill • 170
fw lea_notify • 171
fw lichost • 171
fw log • 171
fw logsw • 173
fw lslogs • 178
fw mergefiles • 174
fw monitor • 175
fw putkey • 179
fw repairlog • 180
fw sam • 180
fw stat • 184
fw tab • 184
fw ver • 185
fwm • 186
fwm dbexport • 187
fwm dbimport • 186