# Contents

## Preface
- Who Should Use This Guide ................................................................. 8
- Summary of Contents ...................................................................... 9
- Appendices .................................................................................... 9
- Related Documentation ................................................................. 10
- More Information .......................................................................... 13
- Feedback ...................................................................................... 14

## Chapter 1
**Introduction**
- Overview .................................................................................. 16
- SecurePlatform Hardware Requirements ..................................... 17
- SecurePlatform Pro ................................................................. 18

## Chapter 2
**Preparing to Install SecurePlatform**
- Preparing the SecurePlatform Machine ....................................... 20
- Hardware Compatibility Testing Tool ......................................... 21
- Getting Started .......................................................................... 22
- Using the Hardware Compatibility Testing Tool ....................... 24
- BIOS Security Configuration Recommendations .................... 25

## Chapter 3
**Configuration**
- Using the Command Line ........................................................... 28
- First Time Setup Using the Command Line ................................. 28
- Using sysconfig .......................................................................... 29
- Check Point Products Configuration ........................................ 31
- Using the Web Interface ............................................................ 32
- First Time Setup Using the Web Interface ................................. 32
- Web Interface Layout ................................................................. 41
- First Time Reboot and Login .................................................... 56

## Chapter 4
**Administration**
- Managing Your SecurePlatform System .................................... 58
- Connecting to SecurePlatform by Using Secure Shell .............. 58
- User Management ................................................................. 59
- SecurePlatform Administrators ............................................. 60
- FIPS 140-2 Compliant Systems .............................................. 62
- Using TFTP ............................................................................. 63
- Backup and Restore ................................................................. 63
- SecurePlatform Shell .............................................................. 64
- Command Shell ...................................................................... 64
- Management Commands ......................................................... 66
- Documentation Commands ....................................................... 67
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and Time Commands</td>
<td>67</td>
</tr>
<tr>
<td>System Commands</td>
<td>70</td>
</tr>
<tr>
<td>Snapshot Image Management</td>
<td>78</td>
</tr>
<tr>
<td>System Diagnostic Commands</td>
<td>80</td>
</tr>
<tr>
<td>Check Point Commands</td>
<td>83</td>
</tr>
<tr>
<td>Network Diagnostics Commands</td>
<td>96</td>
</tr>
<tr>
<td>Network Configuration Commands</td>
<td>102</td>
</tr>
<tr>
<td>Dynamic Routing Commands</td>
<td>112</td>
</tr>
<tr>
<td>User and Administrator Commands</td>
<td>113</td>
</tr>
<tr>
<td>SNMP Support</td>
<td>115</td>
</tr>
<tr>
<td>Configuring the SNMP Agent</td>
<td>115</td>
</tr>
<tr>
<td>Configuring SNMP Traps</td>
<td>116</td>
</tr>
<tr>
<td>Check Point Dynamic Routing</td>
<td>120</td>
</tr>
<tr>
<td>Supported Features</td>
<td>120</td>
</tr>
<tr>
<td>Command Line Interface</td>
<td>123</td>
</tr>
<tr>
<td>SecurePlatform Boot Loader</td>
<td>125</td>
</tr>
<tr>
<td>Booting in Maintenance Mode</td>
<td>125</td>
</tr>
<tr>
<td>Customizing the Boot Process</td>
<td>126</td>
</tr>
<tr>
<td>Snapshot Image Management</td>
<td>126</td>
</tr>
</tbody>
</table>

**Chapter 5**

SecurePlatform Pro

Advanced Routing Suite

- Introduction .................................................. 128
- Check Point Advanced Routing Suite .................. 129
- Supported Features ........................................ 129
- Dynamic Routing ............................................ 129
- Command Line Interface .................................. 129

**Appendix A**

Installation on Computers without Floppy or CDROM Drives

- General Procedure ........................................ 136
- Client Setup ................................................ 136
- Server Setup ................................................ 137
- Required Packages ....................................... 137
- DHCP Daemon Setup ....................................... 138
- TFTP and FTP Daemon Setup .............................. 139
- Hosting Installation Files ............................... 140

**Index** ................................................................... 147
Preface

In This Chapter

Who Should Use This Guide  page 8
Summary of Contents  page 9
Related Documentation  page 10
More Information  page 13
Feedback  page 14
Who Should Use This Guide

This guide is intended for administrators responsible for maintaining network security within an enterprise, including policy management and user support.

This guide assumes a basic understanding of

- System administration.
- The underlying operating system.
- Internet protocols (IP, TCP, UDP etc.).
## Summary of Contents

This guide covers the following chapters:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chapter 1, “Introduction”</strong></td>
<td>This chapter covers the two “flavors” of SecurePlatform, and hardware requirements</td>
</tr>
<tr>
<td><strong>Chapter 2, “Preparing to Install SecurePlatform”</strong></td>
<td>This chapter covers everything you need to do before installing SecurePlatform</td>
</tr>
<tr>
<td><strong>Chapter 3, “Configuration”</strong></td>
<td>This chapter covers using the command line interface, the web interface, and what happens when you log in for the first time</td>
</tr>
<tr>
<td><strong>Chapter 4, “Administration”</strong></td>
<td>This chapter covers the various aspects of SecurePlatform administration</td>
</tr>
<tr>
<td><strong>Chapter 5, “SecurePlatform Pro Advanced Routing Suite”</strong></td>
<td>This chapter covers SecurePlatform’s support for dynamic routing protocols</td>
</tr>
</tbody>
</table>

## Appendices

This guide contains the following appendices:

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Appendix A, “Installation on Computers without Floppy or CDROM Drives”</strong></td>
<td>This chapter covers alternative means of installing SecurePlatform</td>
</tr>
</tbody>
</table>
**Related Documentation**

This release includes the following documentation

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Security Product Suite Getting Started Guide</td>
<td>Contains an overview of NGX R65 and step by step product installation and upgrade procedures. This document also provides information about What's New, Licenses, Minimum hardware and software requirements, etc.</td>
</tr>
<tr>
<td>Upgrade Guide</td>
<td>Explains all available upgrade paths for Check Point products from VPN-1/FireWall-1 NG forward. This guide is specifically geared towards upgrading to NGX R65.</td>
</tr>
<tr>
<td>SmartCenter Administration Guide</td>
<td>Explains SmartCenter Management solutions. This guide provides solutions for control over configuring, managing, and monitoring security deployments at the perimeter, inside the network, at all user endpoints.</td>
</tr>
<tr>
<td>Firewall and SmartDefense Administration Guide</td>
<td>Describes how to control and secure network access; establish network connectivity; use SmartDefense to protect against network and application level attacks; use Web Intelligence to protect web servers and applications; the integrated web security capabilities; use Content Vectoring Protocol (CVP) applications for anti-virus protection, and URL Filtering (UFP) applications for limiting access to web sites; secure VoIP traffic.</td>
</tr>
<tr>
<td>Virtual Private Networks Administration Guide</td>
<td>This guide describes the basic components of a VPN and provides the background for the technology that comprises the VPN infrastructure.</td>
</tr>
</tbody>
</table>
### TABLE P-1  VPN-1 Power documentation suite documentation (continued)

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eventia Reporter Administration Guide</td>
<td>Explains how to monitor and audit traffic, and generate detailed or summarized reports in the format of your choice (list, vertical bar, pie chart etc.) for all events logged by Check Point VPN-1 Power, SecureClient and SmartDefense.</td>
</tr>
<tr>
<td>SecurePlatform™/SecurePlatform Pro</td>
<td>Explains how to install and configure SecurePlatform. This guide will also teach you how to manage your SecurePlatform machine and explains Dynamic Routing (Unicast and Multicast) protocols.</td>
</tr>
<tr>
<td>Provider-1/SiteManager-1 Administration Guide</td>
<td>Explains the Provider-1/SiteManager-1 security management solution. This guide provides details about a three-tier, multi-policy management architecture and a host of Network Operating Center oriented features that automate time-consuming repetitive tasks common in Network Operating Center environments.</td>
</tr>
</tbody>
</table>

### TABLE P-2  Integrity Server documentation

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity Advanced Server Installation Guide</td>
<td>Explains how to install, configure, and maintain the Integrity Advanced Server.</td>
</tr>
<tr>
<td>Integrity Advanced Server Administrator Console Reference</td>
<td>Provides screen-by-screen descriptions of user interface elements, with cross-references to relevant chapters of the Administrator Guide. This document contains an overview of Administrator Console navigation, including use of the help system.</td>
</tr>
<tr>
<td>Integrity Advanced Server Administrator Guide</td>
<td>Explains how to managing administrators and endpoint security with Integrity Advanced Server.</td>
</tr>
<tr>
<td>Integrity Advanced Server Gateway Integration Guide</td>
<td>Provides information about how to integrating your Virtual Private Network gateway device with Integrity Advanced Server. This guide also contains information regarding deploying the unified SecureClient/Integrity client package.</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Integrity Advanced Server System</td>
<td>Provides information about client and server requirements.</td>
</tr>
<tr>
<td>Requirements</td>
<td></td>
</tr>
<tr>
<td>Integrity Agent for Linux Installation and</td>
<td>Explains how to install and configure Integrity Agent for Linux.</td>
</tr>
<tr>
<td>Configuration Guide</td>
<td></td>
</tr>
<tr>
<td>Integrity XML Policy Reference Guide</td>
<td>Provides the contents of Integrity client XML policy files.</td>
</tr>
<tr>
<td>Integrity Client Management Guide</td>
<td>Explains how to use of command line parameters to control Integrity client</td>
</tr>
<tr>
<td></td>
<td>installer behavior and post-installation behavior.</td>
</tr>
</tbody>
</table>
More Information

- For additional technical information about Check Point products, consult Check Point’s SecureKnowledge at https://secureknowledge.checkpoint.com/.

- See the latest version of this document in the User Center at http://www.checkpoint.com/support/technical/documents
Feedback

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

cp_techpub_feedback@checkpoint.com
Chapter 1

Introduction

In This Chapter

Overview  page 16
SecurePlatform Hardware Requirements  page 17
SecurePlatform Pro  page 18
Thank you for using SecurePlatform. This document describes how to install and configure SecurePlatform.

SecurePlatform is distributed on a bootable CD ROM which includes Check Point’s product suite comprising: VPN-1, Check Point QoS, SmartView Monitor, Policy Server, and UserAuthority Server.

The SecurePlatform CD ROM can be installed on any PC with an Intel Pentium III/IV, or AMD Athlon CPU. SecurePlatform includes a customized and hardened operating system, with no unnecessary components that could pose security risks. The system is pre-configured and optimized to perform its task as a network security device, requiring only minimal user configuration of basic elements, such as IP addresses, routes, etc.

On most systems, this installation process runs less than five minutes, resulting in a network security device ready to be deployed.

SecurePlatform allows easy configuration of your computer and networking aspects, as well as the Check Point products installed. An easy-to-use shell provides a set of commands, required for easy configuration and routine administration of a security system, including: network settings, backup and restore utilities, upgrade utility, system log viewing, control, and much more. A Web GUI enables most of the administration configuration, as well as the first time installation setup, to be performed from an easy-to-use Web interface.
SecurePlatform Hardware Requirements

On SecurePlatform, the minimum hardware requirements for installing a VPN-1 SmartCenter server, Enforcement Module or SmartPortal are:

- Intel Pentium III 300+ MHz or equivalent processor
- 10 GB free disk space
- 256 MB (512 MB recommended)
- One or more supported network adapter cards
- CD-ROM Drive (bootable)
- 1024 x 768 video adapter card

For details regarding SecurePlatform on specific hardware platforms, see:

http://www.checkpoint.com/products/supported_platforms/recommended/ngx/index.html

**Note** - For information about the recommended configuration of high-performance systems running Check Point Performance Pack, see the CheckPoint R65 PerformancePack Administration Guide.
SecurePlatform Pro

SecurePlatform Pro is an enhanced version of SecurePlatform. SecurePlatform Pro adds advanced networking and management capabilities to SecurePlatform such as:

- Dynamic routing
- Radius authentication for SecurePlatform administrators

To install “SecurePlatform Pro” select the “SecurePlatform Pro” option during the installation.

To convert regular SecurePlatform to SecurePlatform Pro, from the expert mode command line run: “pro enable”.

Note - SecurePlatform Pro requires a separate license that must be installed on the SmartCenter server that manages the SecurePlatform Pro enforcement modules.

For information about RADIUS support, see: “How to Authenticate Administrators via RADIUS” on page 60

For information regarding advanced routing, see the SecurePlatform Pro & Advanced Routing Command Line Interface.

For all intents and purposes, wherever the name SecurePlatform is used, SecurePlatform Pro is implicitly included.
Chapter 2
Preparing to Install SecurePlatform

In This Chapter

  Preparing the SecurePlatform Machine  page 20
  Hardware Compatibility Testing Tool  page 21
  BIOS Security Configuration Recommendations  page 25
Preparing the SecurePlatform Machine

SecurePlatform installation can be done from a CD drive, from a diskette, or from a network server, using a special boot diskette.

Before you begin the SecurePlatform installation process, ensure that the following requirements are met:

• If the target computer has a CD drive, make sure that the system BIOS is set to reboot from this drive as the first boot option (this BIOS Setup Feature is usually named Boot Sequence).

• If your target computer cannot boot from a CD drive, or if you wish to install using a remote file server, refer to the instructions in the CheckPoint R65 Internet Security Products GettingStarted Guide.

**Warning** - The installation procedure erases all hard disks, so the former operating system cannot be recovered.

**Note** - SecurePlatform can be installed on a computer without a keyboard or VGA display by using a serial console attached to a serial port.
Hardware Compatibility Testing Tool

In This Section

Getting Started ..... page 22
Using the Hardware Compatibility Testing Tool ..... page 24

The Hardware Compatibility Testing Tool enables you to determine whether SecurePlatform is supported on a specific hardware platform.

The utility is available for download as a CD ISO image (hw.iso). The ISO image can be burned on the blank CD-R or on the CD-RW media, using a CD-burning tool.

Note - You must specify that you are burning “CD image” and not single file.

The Hardware Compatibility Testing Tool should be run in the same way that would be used to install SecurePlatform on the hardware platform (for example, boot from CD, boot from diskette and installation through network etc.).

The tool detects all hardware components on the platform, checks whether they are supported, and displays its conclusions: whether SecurePlatform can be installed on the machine (supported I/O devices found, support mass storage device was found), and the number of supported and unsupported Ethernet controllers detected.

The user can view detailed information on all the devices found on the machine.

The user can save the detailed information on a diskette, on TFTP server, or dump it via the serial port. This information can be submitted to Check Point Support in order to add support for unsupported devices.

SecurePlatform requires the following hardware:

• I/O Device (either Keyboard & Monitor, or Serial console).
• mass storage device
• at least one supported Ethernet Controller (If SecurePlatform is to be configured as a VPN-1 gateway, more than one controller is needed)

The tool makes no modifications to the tested hardware platform, so it is safe to use.
Getting Started

In This Section

- Booting from the CD page 22
- Booting from a Diskette and Accessing a Local CD page 22
- Booting from a Diskette and Accessing the CD over the Network page 23

The user can run the tool either by booting from the CD that contains it, booting from a disk and accessing a local CD, or booting from a diskette and accessing the CD through the network.

If no keyboard and monitor are connected to the hardware platform, the serial console can be used to perform the hardware detection.

**Booting from the CD**

To boot from the CD:

1. Configure the BIOS of the machine to boot from the CD drive.
2. Insert the CD into the drive.
3. Boot the machine.

**Booting from a Diskette and Accessing a Local CD**

This option should be used when the hardware platform cannot be configured to boot from the CD drive (but will boot from a diskette), and has a CD drive.

To boot from a diskette and access a local CD:

1. Insert the CD into the drive.
2. Insert a diskette into the drive.
3. Browse to your CDROM drive and select the SecurePlatform/images folder.
4. Drop the boot.img file on the cprawrite executable.
   
   Alternatively, using NT command shell (cmd), run the following command (where D: is the CD-ROM drive):

```cmd
D:\SecurePlatform\images\cprawrite.exe D:\SecurePlatform\images\boot.img
```

5. Boot the machine.
Booting from a Diskette and Accessing the CD over the Network

This option should be used when the machine to be tested has no CD drive. In this case, there will be two machines participating:

- the machine in which you will insert the CD
- the machine on which you will run the tool

To boot from a diskette and access a CD over the network:

On the Machine with the CD Drive

Proceed as follows:

1. Insert the CD into the drive of a (Microsoft Windows-based) machine.
2. Insert a diskette into its diskette drive.
3. Browse to the CD drive and select the SecurePlatform/images folder.
4. Drop the bootnet.img file on the cprawrite executable.
   Alternatively, using NT command shell (cmd), run the following command (where D: is the CD-ROM drive):

   ```
   D:\SecurePlatform\images\cprawrite.exe D:\SecurePlatform\images\bootnet.img
   ```

   This step writes files to the diskette, which you will transfer to the other machine (the machine on which the tool will be run).

5. Make the contents available on the network, either by allowing access to the CD drive, or by copying the CD to a hard disk and enabling access to that disk (for example, by FTP, HTTP, or NFS).

On the Machine You Are Testing

Proceed as follows:

1. Insert the diskette you created in step 4, above, into the diskette drive of the machine you are testing.
2. Boot the machine.
3. Configure the properties of the interface through which this machine is connected to the network, including its IP address, Netmask, default gateway and DNS.
   You can choose to configure this interface as a dynamic IP address interface.
4. Enable access to the files on the machine with the CD drive (see step 5).

5. Specify the following settings for the other machine:
   - IP address, or hostname
   - Package Directory
   - user/password (if necessary)

6. If you are installing using a serial console, instead of the keyboard and monitor, make sure that your terminal emulation software is configured as follows:
   - 9600 Baud rate
   - 8 data bits
   - no parity
   - no flow control

**Using the Hardware Compatibility Testing Tool**

The hardware tool automatically tests the hardware for compatibility.

*Note* - A simple, “ naïve” detection tool is included on the boot diskette. If for some reason, the complete detection tool is unavailable (e.g., the CDR drive is not supported), you can still use the simple tool to get some information on your hardware. The simple tool is available from the ‘Installation Method’ screen, by pressing the **Probe Hardware** button.

When it finishes, the tool displays a summary page with the following information:
- statement whether the Platform is suitable for installing SecurePlatform
- number of supported and unsupported mass storage devices found
- number of supported and unsupported Ethernet Controllers found

Additional information can be obtained by pressing the **Devices** button. The devices information window lists all the devices, found on the machine (grouped according to functionality).

Use the arrow keys to navigate through the list.

Pressing **Enter** on a specific device displays detailed information about that device.

The detailed information can be saved to a diskette, to a TFTP Server, or dumped through the Serial Console. This action can be required in cases where some of the devices are not supported.
BIOS Security Configuration Recommendations

The following are BIOS configuration recommendations:

• Disable the “boot from floppy” option in the system BIOS, to avoid unauthorized booting from a diskette and changing system configuration.

• Apply a BIOS password to avoid changing the BIOS configuration. Make sure you memorize the password, or keep it in a safe place.
Chapter 3

Configuration

In This Chapter

Using the Command Line page 28
Using the Web Interface page 32

SecurePlatform enables easy configuration of your computer and networking setup, and the Check Point products installed on them.
Using the Command Line

This section describes the `sysconfig` application, which provides an interactive menu system for all configuration aspects. Configuration can also be done using command line utilities provided by the SecurePlatform Shell. The SecurePlatform Shell is discussed in “SecurePlatform Shell” on page 64.

First Time Setup Using the Command Line

After the installation from the CD has been completed, and the computer has been rebooted, a first time setup is required in order to:

- configure the network settings
- apply the license
- select which products will be installed
- perform the SmartCenter initial setup, if selected

Perform the first time setup, as follows:

1. Run the `sysconfig` command from the console to configure SecurePlatform, using a text interface.

2. The command line setup wizard begins, and guides you through the first-time configuration.

3. Select “n” to proceed to the next menu, or “q” to exit the Wizard, and press Enter.

4. If you selected “n” and pressed Enter, the Network Configuration menu options are displayed. They are:
   - Host Name (Set/Show Host Name)
   - Domain Name (Set/Show Domain Name)
   - Domain Name Servers (Add/Remove/Show Domain Name Servers)
   - Network Connections (Add/Configure/Remove/Show Connection)
   - Routing (Set/Show Default Gateway)
5. You must configure the following:
   • the computer’s name
   • the domain name, and up to three DNS servers
   • the computer’s network interfaces
   • the default gateway

6. Enter the desired option number and press Enter.

   The Choose an action menu operation options are displayed.

7. Enter the desired operation option number and press Enter. (Select “e” and press Enter to return to the previous menu.)

8. When you have completed the Network Configuration, select “n” and press Enter to proceed to the next menu, Time and Date Configuration. (Select “p” and press Enter to return to the previous menu, or select “q” and press Enter to exit the Wizard.)

   In the Time and Date Configuration menu you can enter the current date and time, as well as setting the time zone.

   Note - This concludes the SecurePlatform operating system installation. For detailed installation instructions for a specific product, refer to the relevant documentation for that product.

Using sysconfig

Once you have performed the first time setup, via the command line setup wizard, you can use sysconfig to modify your configuration.

To run sysconfig, login to SecurePlatform and enter sysconfig at the prompt.

The sysconfig main menu lists various configuration items, (note that all configuration items must be defined). We recommend step by step configuration, by addressing each menu item in sequence, one after the other.

Select a menu item by typing the relevant number and pressing Enter. Selecting a main menu option displays an additional menu for setting or viewing various configuration items. To return to the main menu, select the menu item Done. To quit, select Exit from the main menu.

When selecting a set option, sysconfig prompts the user to enter all relevant configuration parameters. As soon as all the parameters are completed, the change is applied.
Using sysconfig

Note - Entering e at any point during sysconfig brings the user one menu level up.

Table 3-1  Sysconfig Configuration Options

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Inside Each Menu Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Host Name</td>
<td>Set or show host name.</td>
</tr>
<tr>
<td>2 Domain Name</td>
<td>Set or show domain name.</td>
</tr>
<tr>
<td>3 Domain Name Servers</td>
<td>Add or remove domain name servers, or show configured domain name servers.</td>
</tr>
<tr>
<td>4 Time &amp; Date</td>
<td>Set the time zone, date and local time, or show the date and time settings.</td>
</tr>
<tr>
<td>5 Network Connections</td>
<td>Add or remove connections, configure network connections, or show configuration of network connections.</td>
</tr>
<tr>
<td>6 Routing</td>
<td>Add network and route, add new host, set default gateway, delete route, or show routing configuration.</td>
</tr>
<tr>
<td>7 DHCP Server</td>
<td>Configure SecurePlatform DHCP Server.</td>
</tr>
<tr>
<td>8 DHCP Relay</td>
<td>Setup DHCP Relay.</td>
</tr>
<tr>
<td>9 Export Setup</td>
<td>Exports Check Point environment.</td>
</tr>
<tr>
<td>10 Products Installation</td>
<td>Installs Check Point products (cpconfig). For more information, see the product installation instructions.</td>
</tr>
<tr>
<td>11 Products</td>
<td>Configure Check Point products (cpconfig). For more information, see “Check Point Products Configuration”, below. Configuration</td>
</tr>
</tbody>
</table>
Check Point Products Configuration

To configure Check Point products, select this option in the \textit{sysconfig} application, or run the \texttt{cpconfig} application, available from the SecurePlatform Shell. For more information about configuring Check Point products, refer to the \textit{CheckPoint R65 Internet Security Products GettingStarted Guide}.

As soon as you finish the Check Point products configuration procedure, you will be asked to reboot your system. After reboot, your system will be available for use.

\textbf{Note} - You must run the Check Point Products Configuration procedure (\texttt{cpconfig}) in order to activate the products.

Proceed as follows:

- If you have installed an Enforcement Module, refer to the \textit{CheckPoint R65 Internet Security Products GettingStarted Guide} and the \textit{CheckPoint R65 SmartCenter Administration Guide} for information on how to set up a Security, VPN or QoS policy for your new gateway.

- If you have installed a SmartCenter server, refer to the \textit{CheckPoint R65 Internet Security Products GettingStarted Guide} and the \textit{CheckPoint R65 SmartCenter Administration Guide} for information on how to connect to your new SmartCenter server, using the Check Point SmartConsole.

- If you have installed VPN-1 Power, refer to the \textit{CheckPoint R65 VPN Administration Guide} for more information on how to connect, and set up your new product.
Using the Web Interface

This chapter describes SecurePlatform’s Web interface. Most of the common operations can be done by using the Web Interface. For information about other configuration options, see “Using the Command Line” on page 28.

Note - The Web interface is not accessible in the FIPS 140-2 compliant mode.

First Time Setup Using the Web Interface

After the installation from the CD has been completed, and the computer has been rebooted, a first time setup is required in order to:

- configure the network settings
- configure the time/date/time zone
- configure the allowed IPs of SSH and administration Web UI clients
- select which products will be installed
- set the initial configuration of installed products

Perform the first time setup as follows:

1. Set your browser to work with the IP address you have specified while setting up your network. (e.g. https://192.168.1.1). Since it is a first time installation, the End User’s License Agreement page will be displayed. If you accept the terms of the license agreement, the Login page is displayed.

   Alternatively, to configure SecurePlatform using a text interface, you can run the sysconfig command from the console.

2. In the Login page, login using admin as the user name, and admin as the password. Since this is an initial user name and password, the Change Password page is displayed.

3. In the Change Password page, proceed as follows:
   - It is recommended to utilize the available Onetime Login Key. In the Onetime Login Key section, click Download. The Login Key Challenge page is displayed. Enter a Question and Answer and click OK.
First Time Setup Using the Web Interface

• Change the User name and Password for the administrator. Click Save and Login when done.

Note - The defined user name and password are used for both the Web interface and the console.

The Welcome page is displayed. The setup wizard begins, and guides you through the first-time configuration. Click Next to proceed to the next page, or Back to return to the previous page.

4. Click Next to proceed to the Network Configuration page. You may configure the IP address and network mask of each interface. You can modify the MAC address of the Ethernet interfaces, add VLANs, and so forth.

Each interface can be associated with a primary IP and optionally with one or more secondary IPs.

Note - This page displays a list of all physical NICs that are on the appliance.

You may configure the Primary IP address to obtain the IP automatically, using DHCP. However, this option is not recommended for deployment in a production environment.

To configure the primary IP of an interface:

a. Click on a specific interface. The Connection Configuration page appears.

b. If you enable Use the following configuration, enter the IP address and Netmask.

c. If you enable Obtain IP address automatically (DHCP), the primary IPs are obtained automatically using DHCP.

d. Supply an MTU value.

e. Supply a Physical Address (MAC Address).

f. Select a Link Speed and Duplex value from the drop-down box.

g. Click Apply.

To add an additional IP to an interface:

On the Network Connections page, click New. The Add Network Connections drop-down box is displayed. The options are:

• Secondary IP
First Time Setup Using the Web Interface

- PPTP
- PPPoE
- ISDN
- VLAN
- Loopback

To add a secondary IP to an interface:

b. On the Add Secondary IP Connection page:
   i) Select an interface from the drop-down box
   ii) Supply an IP address
   iii) Supply a network mask
   Click Apply.

To add a PPTP connection to an interface:

a. Select PPTP. The Add PPTP Connection page appears.
b. On the Add PPTP Connection page:
   i) Supply a Remote Server IP address
   ii) Supply a Remote Server name
   iii) Supply a Username and Password
   iv) You can select to obtain the Default Gateway automatically
   v) You can select to obtain the DNS automatically
   vi) You can select to automatically connect on boot
c. Click Apply.

To add a PPPoE connection to an interface:

a. Select PPPoE. The Add PPPoE Connection page appears.
b. On the Add PPPoE Connection page:
   i) Select an interface from the drop-down box

Note - Make sure that the Remote Server is accessible from this computer
First Time Setup Using the Web Interface

ii) Supply a Username and Password
iii) You can select to obtain the Default Gateway automatically
iv) You can select to obtain the DNS automatically
v) You can select to automatically connect on boot

c. Click Apply.

To add an ISDN connection to an interface:
a. Select ISDN. The Add ISDN Connection page appears.
b. On the Add ISDN Connection page:
   i) Select a channel protocol from the drop-down box
   ii) Supply a Provider Name
   iii) Supply a country code
   iv) Supply an area code
   v) Supply a phone number
   vi) Supply a Username and Password
   vii) You can select to obtain the Default Gateway automatically
   viii) You can select to dial on demand
   ix) You can select to obtain the DNS automatically
   x) You can select to automatically connect on boot

3. Click Apply.

To add a VLAN connection to an interface:
a. Select VLAN. The Add VLAN Connection page appears.
b. On the Add VLAN Connection page:
   i) Select an interface from the drop-down box
   ii) Supply a VLAN Number
   iii) If you enable Use the following configuration, enter the IP address and Netmask.
   iv) If you enable Obtain IP address automatically (DHCP), the primary IPs are obtained automatically using DHCP.

c. Click Apply.

To add a Loopback connection to an interface:
First Time Setup Using the Web Interface

a. Select Loopback. The Add Loopback Connection page appears.
b. On the Add Loopback Connection page:
   i) Supply an IP Address
   ii) Supply a Netmask
c. Click Apply.

5. In the Routing Table page, you can add a static route or default route, or delete them.

Note - You cannot edit an existing route. To modify a specific route, delete it and create a new route in its place. Be careful not to delete a route that allows you to connect to the device.

   To delete a route:
   • Select the specific route checkbox and click Delete.

   To configure routing:
   • On the Routing Table page, click New. The Add Route drop-down box is displayed.
     The options are:
     • Route
     • Default Route

To add a new route:

a. Select Route. The Add New Route page appears.
b. On the Add New Route page, supply a:
   i) Destination IP Address
   ii) Destination Netmask
   iii) Interface (from the drop-down box)
   iv) Gateway
   v) Metric
c. Click Apply.

To add a default route:

a. Select Default Route. The Add Default Route page appears.
b. On the **Add Default Route** page, supply a:
   i) Gateway
   ii) Metric

c. Click **Apply**.

6. In the **DNS Servers** page, provide IP addresses for up to three DNS servers.

7. In the **Host and Domain Name** page:
   - Supply a Hostname.
   - Supply a Domain name.
   - Select an interface from the drop-down box. The Hostname will be associated with the IP of this interface.

8. In the **Date and Time Setup** page you can enter the current date and time, as well as setting the time zone. The date must be in the format: dd-Mon-yyyy (e.g. 31-Dec-2003). The time should be: HH:mm (e.g. 23:30).

   NTP is used to synchronize clocks of computers on the Internet.

   Click **Apply** to apply the date and time.

   **Warning** - If you change the date or time, and do not select **Apply**, the changes will not take effect.

9. In the **Web/SSH Clients** page, a list of configured client IPs is displayed. Only the configured client IPs are permitted to access SecurePlatform and SSH services. You can add or remove a Web/SSH client.

   To remove a Web/SSH client:
   - Select the specific Web/SSH client checkbox and click **Remove**.

   To add a Web/SSH client:
   a. In the **Web/SSH Clients** page, click **New**. The **Add Web/SSH Client** page is displayed.
   b. You can add the IP address, resolvable name, or Network of the Web client.

   **Note** - The Hostname can also contain a wildcard, or the word ‘any’, which enables a connection from any Web/SSH Client.

c. Click **Apply**.
10. In the **Installation options** page, select either Check Point Power (for headquarters and branch offices), or Check Point UTM (for medium-sized businesses). Your choices determine which other pages will be displayed by the wizard.

11. In the **Products Selection** page, select at least one of the following options and click **Next** (Your choices determine which other pages will be displayed by the wizard.):

- **VPN-1 Power**: Is the cornerstone of Check Point VPN-1 Power solutions, and the most comprehensive set of products and technologies for remote access, intranet, and extranet VPNs. VPN-1 Power protects the privacy of business communications over the Internet while securing critical network resources against unauthorized access.

- **Advanced Routing Suite**: Is a suite that adds Dynamic Routing and Multicast Protocols support as an integrated part of SecurePlatform and the Check Point products installed on it. Protocols supported include RIP v.1 and v.2; OSPF; BGP; IGMP; PIM-SM and PIM-DM.

- **SmartCenter**: Check Point's flagship management solution with an intuitive dashboard that enables administrators to centrally define the VPN, firewall and QoS policies.

- **Eventia Suite**: Is a complete reporting system, which delivers in-depth network security activity and event information from Check Point log data.

- **Integrity**: Centrally manages desktop firewall security, intrusion prevention, outbound threat protection, and access policy enforcement. It ensures that every PC meets antivirus, patch, and other requirements before it connects to the network.

- **SmartPortal**: A web application that allows you to manage your SmartCenter Server remotely using a web browser.

If you selected VPN-1 Power, select at least one of the following options:

- **Performance Pack**: A software-based acceleration module for VPN-1 Power gateways. By accelerating key security functions such as access control, encryption, NAT and accounting, it enables wire-speed firewall and VPN throughput for gigabit networks.

- **UserAuthority**: Provides a unified, secure communication layer for authenticating users to eBusiness applications. It enables applications to make intelligent authorization decisions based on VPN-1 Power authentication and security information.

12. If you select **VPN-1**, the **Gateway Type** page is displayed. Define the gateway type if needed, or skip this option, if it is not relevant.
a. If you select **Define the gateway type**, you can select:
   - **This gateway is a member of a Cluster**
   or
   - **This gateway uses dynamically assigned IP**.

b. Click **Next**.

**Member of a Cluster**

If the gateway is to be configured as a member of a Cluster, you must first select **This gateway is a member of a Cluster** and then perform the configuration using SmartDashboard.

**Uses Dynamically Assigned IP**

If the gateway uses DAIP, it must initiate a connection. However, if the **DNS Resolution** feature, in the **VPN Link Selection** tab, is enabled, the peer will also be able to initiate the connection.

13. The **Secure Internal Communication (SIC) Setup** page allows you to establish Secure Internal Communication (SIC) between this Gateway and the SmartCenter server. A certificate for this Gateway is then delivered across this connection. Once the certificate arrives at this Gateway, it can then communicate with other Check Point communicating components.

When running the Wizard, SIC is established by entering an Activation Key and clicking **Next**. At other times, SIC is established by entering an Activation Key and clicking **Initialize**. SIC must be initialized or re-initialized on the SmartCenter server, as well as on the Gateway. This can be done via SmartDashboard or SmartLSM by editing the Gateway object and entering the **same** Activation Key that you specified on this page.

Click **Next**.

14. If you select **SmartCenter**, the **SmartCenter** page is displayed. Select one of the following options and click **Next**:
   - **Primary SmartCenter**: The first SmartCenter server that is installed should always be defined as the Primary SmartCenter, whether or not you are using Check Point Management High Availability.
   - **Secondary SmartCenter**: In Check Point Management High Availability, the next SmartCenter server defined must be defined as the Secondary SmartCenter, which will take over from the Primary SmartCenter, if the Primary SmartCenter fails.
• **Log Server:** To reduce the SmartCenter server’s load, administrators can install Log Servers and then configure the modules to forward their logs to these Log Servers. In this case, the logs are viewed by logging with the SmartView Tracker into the Log Server machine (instead of the SmartCenter server machine). If you select Primary SmartCenter, or Secondary SmartCenter, Log Server is included.

15. Eventia Suite includes Eventia Reporter which generates reports based on the logs issued by Check Point products and Eventia Analyzer which correlates and manages real-time security events. If you select **Eventia Suite**, the **Eventia Suite Setup Type** page is displayed. You must select either **Eventia Reporter**, **Eventia Analyzer Server**, or **Eventia Correlation Unit**, and click Next.

16. The **SmartCenter GUI Clients** page specifies the remote computers from which administrators will be allowed to connect to the SmartCenter server. You can also add or remove additional GUI Clients. The type, hostname/IP address and netmask of the configured GUI Clients are provided. In order to add a new GUI client, click Add. To delete a GUI Client, select the specific GUI Client checkbox and click Remove.

17. In the **Add a SmartCenter GUI Client** page, you can enter either a hostname, or a network. The Hostname can also contain a Wildcard, an IP address range, or the word 'any', which enables a connection from any GUI Client. Click Apply and then Next.

18. The **SmartCenter Administrators** page lists the configured Administrators, and enables you to add additional SmartCenter Administrators. If no Administrator has been configured, it enables you to add a SmartCenter Administrator. This SmartCenter Administrator will have Read/Write Permissions to SmartCenter and will be allowed to manage the SmartCenter Administrator accounts. Click Add to add a new Administrator to the list. To delete a SmartCenter Administrator, select the specific SmartCenter Administrator checkbox and click Remove.

19. In the **Add a SmartCenter Administrator** page, enter an Administrator Name and a Password. Click Apply and then Next.

20. The **Summary** page is the last page in the wizard, and displays all the products you selected to install.

21. Click **Finish** to complete the installation.
Web Interface Layout

The initial configuration of SecurePlatform is performed using the First-Time Configuration Wizard. The SecurePlatform Web UI is then used to further configure SecurePlatform.

The Web UI layout is divided into three parts:

- The main navigation menu, on the left, provides navigation between the main categories.
- The Page Title pane, on the upper right, contains the Help and Logout links.
- The Page Contents pane, on the lower right, displays the page data.

**Status**

The Status category provides a concise summary of the system's functionality.

**Device Status**

This page provides a summary of the device status, and displays information, such as the machine host name, Version and Build, and Installation Type.

**Network**

This category provides the tools to specify the management parameters of your network settings, such as physical network interfaces, VLANs, Routing, DNS, and other devices.

**Network Connections**

This page enables you to edit the properties of existing network connections (for example, xDSL connections using PPPoE or PPTP) and to add VLANs to ethernet interface.

The **Network Connections** table displays all available network connections.

To use the table:

1. Click the specific interface link to edit the properties of a specific connection.
2. Select the specific interface checkbox and click **Delete** to delete a selected connection.

*Note* - You can disable an interface, by selecting the specific interface checkbox, and clicking the Down button. Loopback and Ethernet connection cannot be deleted.

3. To add a connection, Click **New** and select the connection type from the drop-down list. Click **Apply**

4. Click **Refresh** to refresh the table (in case the configuration was changed while you were on this page).

**Routing**

This page enables you to manage the routing table on your device. You can add a static or default route, or delete them.

*Note* - You cannot edit an existing route. To modify a specific route, delete it and create a new route in its place. Be careful not to delete a route that allows you connect to the device.

To delete a route:
- Select the specific route checkbox and click **Delete**.

To configure routing:
On the **Routing Table** page, click **New**. The **Add Route** drop-down box is displayed.

The options are:
- Route
- Default Route

To add a new route:
1. Select **Route**. The **Add New Route** page appears.
2. On the **Add New Route** page, supply a:
   a. Destination IP Address
      i. Destination Netmask
      ii. Interface (from the drop-down box)
      iii. Gateway
      iv. Metric
v. Click **Apply**.

To add a default route:
1. Select **Default Route**. The **Add Default Route** page appears.
2. On the **Add Default Route** page, supply a:
   a. Gateway
   b. Metric
   c. Click **Apply**.

### DNS

In the **DNS** page, you can define up to three DNS servers.

### Domain

In the **Host and Domain Name** page:
- Supply a Hostname.
- Supply a Domain name.
- Select a primary interface from the drop-down box. The Hostname will be associated with the IP of this interface.

### Hosts

This page enables you to configure the host's local resolving configuration. You can add a new host by clicking **New**, and delete an existing entry, by selecting the specific Hostname checkbox and clicking **Delete**.

To add a Host:
1. Click **New**. The **Add Host** page is displayed.
2. In the **Add Host** page:
   - Supply a Hostname.
   - Supply a Host IP Address
3. Click **Apply**.

### Device

The device category enables you to control the device itself. It contains the following topics:
Web Interface Layout

- Control
- Date and Time
- Backup
- Upgrade
- Administration Web Server
- Device Administrators
- Authentication Servers
- Web and SSH Clients
- Administrator Security
- SmartCenter Administrators
- SmartCenter GUI Clients
- Download SmartConsole Applications

**Control**

This page provides diagnostics information about all the processes that are running on the machine. For each Process, the User, PID, Parent PID, %CPU, % Memory and Command are displayed. You can use the Device Control drop-down list to Start, Restart, or Stop any of the Check Point products. In addition, you can Shutdown the device, or Reboot it, or download a diagnostic file (cpinfo output) useful for support.

You can refresh the information displayed in the page by clicking Refresh.

You can save the currently viewed diagnostics information in a file.

**Date and Time**

This page allows you to define the SecurePlatform’s date and time, optionally using NTP.

In the Date and Time Setup page you can enter the current date and time, as well as setting the time zone. The date must be in the format: dd-Mon-yyyy (e.g. 31-Dec-2003). The time should be: HH:mm (e.g. 23:30).

NTP is used to synchronize clocks of computers on the Internet.
Click **Apply** to set the date and time.

**Warning** - If you change the date or time, and do not select **Apply**, the changes will not take effect.

**Backup**

This page allows you to configure backup settings. You can choose to configure a scheduled backup, or you can choose to perform an instantaneous backup operation. The backup data can be stored on a TFTP Server, SCP Server, or locally. In addition, you can view a Backup Log.

**Note** - If you use a stock TFTP Server with Unix/Linux flavors, you must create a world writable file having the same name as the proposed backup file before executing the backup. Otherwise, the backup will not succeed. It is strongly recommended that you refer to your tftp server manual, or simply to the tftp protocol, and verify that the usage of the util is compliant with the environment that you are working in.

The SecurePlatform backup mechanism enables exporting snapshots of the entire dynamic configuration. Exported configurations can later be imported in order to restore a previous state in case of failure. The mechanism is also used for seamless upgrades of the software.

**Information Backed Up**

The information backed up includes:

- All settings performed by the Admin GUI
- Network configuration data
- Database of user settings (personal favorites, credentials, cookies etc.)

Two common use cases are:

- When the current configuration stops working, a previous exported configuration may be used in order to revert to a previous system state.
- Upgrading to a new SecurePlatform version. The procedure would include:
  - Backing up the configuration of the current version
  - Installing the new version
  - Importing the backed up configuration

Backup can be performed in configurable schedules.
The Backup page displays the **Current device date and time**. This field shows the user the current local time of the device, which may be different than the browser machine time.

**Viewing the Scheduling Status**

To view the Scheduling Status:

The **Scheduling Status** pane displays the following information:

- **Enabled**: backup currently enabled.
- **Backup to**: backup destination which can be one of the following: the current SecurePlatform, a TFTP Server, or an SCP Server,
- **Start at**: time to start the backup.
- **Recur every**: recurrence pattern.

**Restoring the Backup**

To restore the backup, run the restore shell command from the device.

The syntax is as follows:

```
restore [-h] [ -d ] [ [-tftp <ServerIP> <Filename>] | [-scp <ServerIP> <Username> <Password> <Filename>] | [-file <Filename>]]
```
Parameters

Table 3-2

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>obtain usage</td>
</tr>
<tr>
<td>-d</td>
<td>debug flag</td>
</tr>
<tr>
<td>--tftp &lt;ServerIP&gt;</td>
<td>IP address of TFTP server, from which the configuration is restored, and the filename.</td>
</tr>
<tr>
<td>[&lt;Filename&gt;]</td>
<td></td>
</tr>
<tr>
<td>--scp &lt;ServerIP&gt;</td>
<td>IP address of SCP server, from which the configuration is restored, the username and password used to access the SCP Server, and the filename.</td>
</tr>
<tr>
<td>&lt;Username&gt; &lt;Password&gt;</td>
<td></td>
</tr>
<tr>
<td>[&lt;Filename&gt;]</td>
<td></td>
</tr>
<tr>
<td>--file &lt;Filename&gt;</td>
<td>Specify a filename for restore operation, performed locally.</td>
</tr>
</tbody>
</table>

When the restore command is executed by itself, without any additional flags, a menu of options is displayed. The options in the menu provide the same functionality, as the command line flags, for the restore command.

Choose one of the following:

- [L] Restore local backup package
- [T] Restore backup package from TFTP server
- [S] Restore backup package from SCP server
- [R] Remove local backup package
- [Q] Quit

Select the operation of your choice.

Restoring Backups of Older Versions of SecurePlatform

When restoring backups of older versions of SecurePlatform, such as FP2, FP3 and NG AI, only system settings, such as routes, IP configuration, VLAN interfaces configuration, user accounts, hostname and domainname, and WebUI port will be restored.

You can not restore backups saved on newer SecurePlatform versions onto an older SecurePlatform version, for example you can not restore backups saved on R55 onto NG AI.
When restore detects that the currently installed version of Check Point products does not match the version that was stored in the backup file, the following information will be displayed:

When restoring from backups of SecurePlatform NG AI R55 and later:

The following information will be restored:

```
  system
```

The following information will NOT be restored:

```
  cp_products
```

Choose one of the following:

```
[C]     Continue.
[M]     Modify which information to restore.
[Q]     Quit.
```

Your choice:

If you choose to continue, only system settings will be restored

When restoring from backups of SecurePlatform NG AI and earlier, the following information will be shown:

Restoring...

Backup file was created MM-DD-YYYY-HH:MM.

The MD5 checksum of the backup file is: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.

Do you wish to restore this file (Y/N)?

If you choose "N", the restore operation will be aborted.

The restore operation will replace current configuration.
After restore you have to reboot your system.

Do you wish to proceed (Y/N)?

If you choose "N", the restore operation will be aborted.

Restore completed successfully.

You have to reboot your system now. Reboot now (Y/N)?

**Scheduling a Backup**

To schedule a backup:

1. On the **Backup** page, click **Scheduled backup**. The **Scheduled backup** page appears.

2. Select the **Enable backup recurrence** checkbox.

3. Set up the backup schedule.

4. Select a device to hold the backup. The options include the current SecurePlatform, a TFTP Server (Trivial File Transfer Protocol: A version of the TCP/IP FTP protocol that has no directory or password capability), or an SCP Server (SCP is a secure FTP protocol).

5. Click **Apply**.

To execute a backup:

- Click **Backup now**.

**Viewing the Backup Log**

To view the backup log:

- Click **View backup log**. The **Backup Log** page appears. You will see the Device Date and Time, Location (the device to which the backup has been sent), Location IP Address, Backup Status and Details.
Upgrade

To upgrade your device:

1. Select the upgrade package file.
2. Click **Upload package to device**.
3. Select either **Safe Upgrade**, or **Double-Safe Upgrade**.

   If you selected **Double-Safe Upgrade**, your browser will automatically try to perform the first login immediately after the upgrade, within the time interval that you set. To enable that, you should not close the **Upgrade** page, and not browse to any other page. Otherwise, you will have to login manually, before the above interval expires. If you do not login manually within the above interval, the system will interpret this as a loss of connectivity and reset to the saved state.

4. When you are done uploading the package, you can click on the "package information" link to see detailed information about the package, including version information and the MD5 checksum of the package. This checksum can be used to verify that the package is correct.

5. Click **Start Upgrade**.

   The **Upgrade Status** pane provides information such as **Action**, **Start Time**, **Status** and **Details**.

Administration Web Server

This page allows you to configure the Administration Web server listening IP and port.

1. Supply the port.

2. You can select an address from the drop-down list, instead of **All**. In that case, the Web server will only listen on that IP.

3. Click **Apply**.
Device Administrators

This page lists the Device Administrators, allows you to create a Device Administrator, and download a One Time Login Key.

To create a Device Administrator:
2. Provide a name and a password for the Device Administrator.
3. Select an Authentication Scheme from the drop-down list.
4. Click Apply.

To download a One Time Login Key:
1. Click Download.

Note - The One Time Login Key will be required in case you forget your password. Save this file in a safe place.

Authentication Servers

This page lists the configured RADIUS Authentication Servers and Authentication Server Groups. It also allows you to add a new RADIUS server and a new Authentication Server Group, or delete them.

Note - All Administrators must be authenticated by one of the supported authentication methods. As well as being authenticated through the internal database, Administrators may also be authenticated via RADIUS.

To add a new RADIUS server:
1. In the Authentication Servers section, click New. The New RADIUS Server page is displayed.
2. In the New RADIUS Server page:
   • Supply a Name
• Supply an IP address

Note - The Port and Timeout values are predefined.

• Supply a Shared Secret

3. Click Apply.

To add a new Authentication Server Group:
1. In the Authentication Server Group section, click New. The New Authentication Server Group page is displayed.
2. In the New Authentication Server Group page supply a Group name and click Apply.

Web/SSH Clients

In the Web/SSH Clients page, a list of configured client IPs is displayed. Only the configured client IPs are permitted to access SecurePlatform and SSH services. You can add or remove a Web/SSH client.

To remove a Web/SSH client:
• Select the specific Web/SSH client checkbox and click Remove.

To add a Web/SSH client:
1. In the Web/SSH Clients page, click Add. The Add Web/SSH Client page is displayed.
2. You can add the IP address, resolvable name, or Network of the Web client.

Note - The Hostname can also contain a wildcard, or the word ‘any’, which enables a connection from any Web/SSH Client.

3. Click Apply.

Administrator Security

In the Administrator Security window, you can configure the Administrator Security parameters.

To configure Administrator Security parameters:
1. Set the Administrator Session Timeout value.
2. In the **Administrator Login Restrictions** section, enable and set the **Lock Administrator's account after <x> login failures.**

3. Set the **Unlock Administrator's account after <y> minutes.**

4. Click **Apply.**

**SmartCenter Administrators**

The **SmartCenter Administrators** page lists the configured Administrators. If no Administrator has been configured, it enables you to add a SmartCenter Administrator. This SmartCenter Administrator will have Read/Write Permissions to SmartCenter and will be allowed to manage the SmartCenter Administrator accounts.

Only one administrator can be added to this list. In order to add more administrators the user must use SmartDashboard.

To delete a SmartCenter Administrator, select the specific SmartCenter Administrator checkbox and click **Remove.**

In the **Add a SmartCenter Administrator** page, enter an Administrator Name and a Password. Click **Apply.**

**SmartCenter GUI Clients**

The **SmartCenter GUI Clients** page lists the type, hostname/IP address and netmask of the configured GUI Clients, and enables you to add additional GUI Clients or remove them. To delete a GUI Client, select the specific GUI Client checkbox and click **Remove.** In order to add a new GUI client, click **Add.** In the **Add GUI Client** page, you can enter either a hostname, or a network. The Hostname can also contain a Wildcard, an IP address range, or the word 'any', which enables a connection from any GUI Client. Click **Apply.**

**Product Configuration**

The products category enables you to define which products are installed on the device (**Products** page) as well as to apply licenses to these products (**Licenses** page).
**Products Installed**

This page enables you to check (via the table), which products are already installed on the machine.

*Note* - VPN-1 Power should always be installed.

**Certificate Authority**

**Internal Certificate Authority**

The entity in charge of issuing certificates for management station, modules, users and other trusted entities such as OPSEC applications used in the system.

**Certificate Authority Page**

The **Certificate Authority** page lists key parameters of the SmartCenter Certificate Authority. These are:

- Certificate Authority Status
- SmartCenter DN
- Fingerprint

Clicking **Reset** retrieves the current parameter values.

**Licenses**

Use the **Licenses** page to apply a license for the products that you have installed.

To apply a license:

1. You can click the **Check Point User Center** link to obtain a license from the User Center.
2. Click **New**.
3. Enter the **IP Address**, **Expiration Date**, **SKU/Features**, and **Signature Key**.
4. You can also copy the license string into the clipboard, and click **Paste License** to copy all the information into the fields.
5. Click **Apply** when done.

   **Note** - License can also be applied by using SmartUpdate.

   **Logout**
   
   Click **Logout** to log out from the system. The **Logon** page is displayed.
First Time Reboot and Login

As soon as the system reboots, after installation, the SecurePlatform NGX Boot Loader screen will appear.

Note - The Boot Loader appears on the console, connected to the computer. The console can be a monitor and keyboard attached to the computer, or a serial console attached to the first serial port (com1).

The Boot Loader offers a selection of boot options. By default, if there is no user intervention, the first option will be selected after a few seconds. For now, allow this option to run. Detailed information about the Boot Loader can be found in “SecurePlatform Boot Loader” on page 125.

As soon as the reboot finishes, a login prompt is displayed.
Chapter 4
Administration

In This Chapter

Managing Your SecurePlatform System  page 58
SecurePlatform Shell  page 64
SNMP Support  page 115
Check Point Dynamic Routing  page 120
SecurePlatform Boot Loader  page 125

This chapter discusses how to manage the SecurePlatform system, how to use the SecurePlatform’s shell commands, and how to configure SNMP for use with SecurePlatform. In addition, the Dynamic Routing and Boot Loader features are discussed.
Managing Your SecurePlatform System

In This Section

Connecting to SecurePlatform by Using Secure Shell  page 58
User Management  page 59
SecurePlatform Administrators  page 60
FIPS 140-2 Compliant Systems  page 62
Using TFTP  page 63
Backup and Restore  page 63

This section provides information on how to manage your SecurePlatform NGX system, using the SecurePlatform Command Shell.

The Command Shell provides a set of commands required for configuration, administration and diagnostics of various system aspects. To manage security, VPN and QoS policies use either the:

• SmartConsole for Enterprise products or
• VPN-1 SmallOffice NG Web GUI for VPN-1 SmallOffice.

For more information about SmartConsole refer to the CheckPoint R65 SmartCenter Administration Guide and the relevant product Release Notes.

Connecting to SecurePlatform by Using Secure Shell

SecurePlatform NGX provides an SSH service, which allows secured, authenticated and encrypted access to the SecurePlatform system.

SSH (or Secure SHell) is a protocol for creating a secure connection between two systems. In the SSH protocol, the client machine initiates a connection with a server machine. The following safeguards are provided by SSH:

• After an initial connection, the client can verify that it is connecting to the same server during subsequent sessions.
• The client can transmit its authentication information to the server, such as a username and password, in an encrypted format.
• All data, sent and received, during the connection is transferred using strong encryption, making it extremely difficult to decrypt and read.
The SSH service runs, by default. In addition, access to the SSH service is limited to the same IPs that have been allowed access to the Web UI. Granular control of machines that are allowed access to the SecurePlatform system, using SSH, can be set, using the VPN-1 security policy.

SSH login is allowed using the Standard Mode account user name and password, only. SCP service and client files can be copied to and from SecurePlatform, using SCP client software. Access to SCP is controlled, by editing /etc/scpusers.

**User Management**

SecurePlatform Shell includes two permission levels (Modes): Standard and Expert.

**Standard Mode**

This is the default mode, when logging in to a SecurePlatform system. In Standard Mode, the SecurePlatform Shell provides a set of commands, required for easy configuration and routine administration of a SecurePlatform system. Most system commands are not supported in this Mode. Standard mode commands are listed in “SecurePlatform Shell” on page 64.

Standard Mode displays the following prompt: [hostname]#, where hostname is the host name of the machine.

**Expert Mode**

The Expert Mode provides the user with full system root permissions and a full system shell. Switching from Standard Mode to Expert Mode requires a password. The first time you switch to Expert mode you will be asked to select a password. Until then, the password is the same as the one that you set for Standard Mode.

You need to enter the first replacement password that you used when logging in as the admin user. Any sequential admin password change will not update the expert password that you must enter at the first-time expert user password change. To exit Expert Mode, run the command exit.

Expert Mode displays the following prompt: [Expert@hostname]#, where hostname is the host name of the machine.

**Warning** - Expert Mode should be used with caution. The flexibility of an open shell, with a root permission, exposes the system to the possibility of administrative errors.
SecurePlatform Administrators

SecurePlatform NGX supports multiple administrator access to the regular shell. This can be used to audit configuration changes performed by administrators. Every such change is logged to the system's syslog mechanism, with the username of the administrator, as a tag.

To configure another administrator from the cpshell, use the following command:

```bash
adduser [-x EXTERNAL_AUTH] <user name>
```

**Note** - An Expert user must first login as a Standard user, and only then enter the `expert` command to access Expert Mode. Until you change passwords, the Expert password is the same password that you set for Standard Mode, i.e. you need to enter the first replacement password that you used when logging in as the admin user. Any sequential admin password change will not update the expert password that you must enter at the first-time expert user password change.

**How to Authenticate Administrators via RADIUS**

All Administrators must be authenticated by one of the supported authentication methods. As well as being authenticated through the internal database, Administrators may also be authenticated via RADIUS. SecurePlatform administrators can be authenticated using the RADIUS server in two ways:

You will be asked to enter and confirm a password for the administrator. The password must conform to the following complexity requirements:

- at least 6 characters, in length
- a mixture of alphabetic and numeric characters
- at least four different characters
- does not use simple dictionary words, or common strings such as “qwerty”

To delete an administrator from the cpshell, use the following command:

```bash
deluser <name>
```

You can also define additional administrators through the Web GUI.
By configuring the local user authentication via the RADIUS server. In this case it is necessary to define all users that will be authenticated by the RADIUS server on every SecurePlatform machine, and it is NOT required to define any RADIUS groups.

By defining the list of RADIUS groups. All users that belong to the RADIUS groups defined on SecurePlatform will be able to authenticate and perform login.

The option utilizing RADIUS groups allows more flexibility, by eliminating the need to define all RADIUS users on each SecurePlatform machine.

There is a special RADIUS group called any. When this group is present in the group list, ALL users defined on the RADIUS server will be able to log into the SecurePlatform machine.

To authenticate an Administrator via RADIUS, you must:

1. Verify that a RADIUS server is configured. If a RADIUS server is not configured, add one by using the following command:

   ```
   radius servers add <server[:port]> <secret> <timeout> <label>
   ```

2. Verify that at least one of the following is correct:

   A. The user that you want to authenticate via the RADIUS server is configured on SecurePlatform, as using the RADIUS authentication method. You can define local users that authenticate via RADIUS by using the following command:

   ```
   radius users add <username>
   ```

   B. At least one RADIUS group is configured, and the user defined on the RADIUS server belongs to that group. You can define RADIUS groups by using the following command line:

   ```
   radius groups add <groupname>
   ```

3. Define the Administrator as a RADIUS user, by using the following command:

   ```
   radius users add <username>
   ```

You can use the following commands to monitor and modify your RADIUS configuration.

To control RADIUS servers:

- `radius servers show`
- `radius servers add <server[:port]> <secret> <timeout>`
• radius servers del <server[:port]>

To control RADIUS user groups:
• radius groups show
• radius groups add <groupname>
• radius groups del <groupname>

To control local RADIUS users:
• radius users show
• radius users add <username>
• radius users del <username>

**FIPS 140-2 Compliant Systems**

The Federal Information Processing Standard (FIPS) 140-2 imposes certain restrictions on the operation of SecurePlatform. Administrators whose systems are FIPS 140-2 compliant, must configure their systems as follows:

Run the following command from cpshell:

```
fips on
```

This command does the following:

1. Adds an integrity check that verifies the integrity of all executables, scripts and configuration files, before connecting the system to the network.

2. Enforces the policy of locking accounts of administrators who have exceeded the threshold of unsuccessful login attempts (see “Lockout of Administrator Accounts”, below).

3. Removes the Web GUI daemon, thus disabling the Web GUI.

4. Removes the Check Point Remote Installation daemon, thus disabling SmartUpdate.

5. Configures VPN-1’s default filter to “drop all incoming”.

**Lockout of Administrator Accounts**

The account of an administrator, who attempts to logon unsuccessfully, three times in one minute, is locked for 60 minutes. This feature is configurable using the lockout command.
Using TFTP

Trivial File Transfer Protocol (TFTP) provides an easy way for transferring files, such as installation files, to and from the SecurePlatform system. SecurePlatform mechanisms that can utilize TFTP include:

- **Backup / Restore Utilities**
- **Patch Utility**—used for software updates
- **Diag Utility**—used for obtaining various diagnostics information

**Note** - Freeware and Shareware TFTP servers are available from the Internet.

Follow the vendor instructions on how to setup the TFTP server, and make sure that you configure the server to allow both reception and transmission of files.

**Warning** - TFTP is not an encrypted, or authenticated protocol. Make sure that you run the TFTP server on your internal network only.

Backup and Restore

SecurePlatform NGX provides a command line, or Web GUI, capability for conducting backups of your system settings and products configuration.

The **backup** utility can store backups either locally on the SecurePlatform machine hard drive, or remotely to a TFTP server or SCP server. The backup can be performed on request, or it can be scheduled to take place at set intervals.

The backup files are kept in tar gzipped format (.tgz). Backup files, saved locally, are kept in /var/CPbackup/backups.

The **restore** command line utility is used for restoring SecurePlatform settings, and/or Product configuration from backup files.

**Note** - Only administrators with Expert permission can directly access directories of a SecurePlatform NGX system. You will need the Expert password to execute the restore command.

For more information about the **backup** and **restore** utilities, see “backup” on page 71, and “restore” on page 74.
SecurePlatform Shell

In This Section

Command Shell .................................................. page 64
Management Commands ........................................... page 66
Documentation Commands ......................................... page 67
Date and Time Commands .......................................... page 67
System Commands ................................................. page 70
Snapshot Image Management ..................................... page 78
System Diagnostic Commands .................................... page 80
Check Point Commands ............................................ page 83
Network Diagnostics Commands ................................. page 96
Network Configuration Commands ............................... page 102
Dynamic Routing Commands ..................................... page 112
User and Administrator Commands ............................... page 113

This section includes a complete listing of SecurePlatform’s shell commands. These commands are required for configuration, administration and diagnostics of various system aspects.

Note - All commands are case sensitive.

Command Shell

Command Set

To display a list of available commands, enter ? or help at the command prompt. Many commands provide short usage instructions by running the command with the parameter ‘--help’, or with no parameters.
**Command Line Editing**

SecurePlatform Command Shell uses command line editing conventions. You can scroll through previously entered commands with the **up** or **down** arrow keys. When you reach a command you wish to use, you can edit it or click the **Enter** key to start it. The **audit** command is used to display history of commands entered at the command prompt (see “audit” on page 70):

**Table 4-1 Command Line Editing Keys**

<table>
<thead>
<tr>
<th>Key</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right Arrow/^f</td>
<td>Move cursor right</td>
</tr>
<tr>
<td>Left Arrow/^b</td>
<td>Move cursor left</td>
</tr>
<tr>
<td>Home/^a</td>
<td>Move cursor to beginning of line</td>
</tr>
<tr>
<td>End/^e</td>
<td>Move cursor to end of line</td>
</tr>
<tr>
<td>Backspace/^h</td>
<td>Delete last char</td>
</tr>
<tr>
<td>^d</td>
<td>Delete char on cursor</td>
</tr>
<tr>
<td>^u</td>
<td>Delete line</td>
</tr>
<tr>
<td>^w</td>
<td>Delete word to the left</td>
</tr>
<tr>
<td>^k</td>
<td>Delete from cursor to end of line</td>
</tr>
<tr>
<td>Up arrow/^p</td>
<td>View previous command</td>
</tr>
<tr>
<td>Down arrow/^n</td>
<td>View next command</td>
</tr>
</tbody>
</table>

**Command Output**

Some command output may be displayed on more than one screen. By default, the Command Shell will display one screen, and prompt: **-More-**. Click any key to continue to display the rest of the command output.

The **More** functionality can be turned on or off, using the **scroll** command.
Management Commands

In This Section

exit  page 66
Expert Mode  page 66
passwd  page 66

**exit**

Exit the current Mode:

- In Standard Mode, exit the shell (logout of the SecurePlatform system)
- In Expert Mode, exit to Standard Mode

**Syntax**

```plaintext
exit
```

**Expert Mode**

Switch from Standard Mode to Expert Mode.

**Syntax**

```plaintext
expert
```

**Description**

After entering the `expert`, command supply the expert password. After password verification, you will be transferred into expert mode.

**passwd**

Changing the password can be performed in both modes. Changing the password in Standard Mode changes the login password. Changing the password in Expert Mode changes the Expert Mode and Boot Loader password. During the first transfer to Expert Mode, you will be required to enter your Standard Mode password, i.e. you need to enter the first replacement password that you used when logging in as the admin user. Any sequential admin password change will not update the expert password that you must enter at the first-time expert user password change. Change the Expert Mode password. After the Expert Mode password is changed, the new password must be used to obtain Expert Mode access.
Documentation Commands

In This Section

help  page 67

help
List the available commands and their respective descriptions.

Syntax

help
or
?

Date and Time Commands

In This Section

date  page 67
time  page 68
timezone  page 68
ntp  page 69
ntpstop  page 69
ntpstart  page 70

date
Show or set the system’s date. Changing the date or time affects the hardware clock.
Date and Time Commands

Syntax

```
date [MM-DD-YYYY]
```

Parameters

Table 4-2  Date Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>MM-DD-YYYY</td>
<td>The date to be set, first two digits (MM) are the month [01..12], next two digits (DD) are the day of month [01..31], and last four digits (YYYY) are the year</td>
</tr>
</tbody>
</table>

**time**

Show or set the system's time. Changing the date or time affects the hardware clock.

Syntax

```
time [HH:MM]
```

Parameters

Table 4-3  Time Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>HH:MM</td>
<td>The time to be set, first two digits (HH) are the hour [00..23], last two digits (MM) are the minute [00..59]</td>
</tr>
</tbody>
</table>

**timezone**

Set the system's time zone.
Syntax

```
timezone [-show | --help]
```

Parameters

Table 4-4  Time Zone Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>if no parameters are entered, an interactive mode of time zone selection is displayed</td>
</tr>
<tr>
<td>-show</td>
<td>show currently selected time zone</td>
</tr>
<tr>
<td>--help</td>
<td>show usage message</td>
</tr>
</tbody>
</table>

**ntp**

Configure and start the Network Time Protocol polling client.

Syntax

```
ntp <MD5_secret> <interval> <server1> [<server2>[<server3>]]
nntp -n <interval> <server1> [<server2>[<server3>]]
```

Parameters

Table 4-5  ntp Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5_secret</td>
<td>pre-shared secret used to authenticate against the NTP server; use “-n” when authentication is not required.</td>
</tr>
<tr>
<td>interval</td>
<td>polling interval, in seconds</td>
</tr>
<tr>
<td>server[1,2,3]</td>
<td>IP address or resolvable name of NTP server</td>
</tr>
</tbody>
</table>

**ntpstop**

Stop polling the NTP server.
System Commands

Syntax

ntpstart

ntpstart
Start polling the NTP server.

Syntax

System Commands

In This Section

audit page 70
backup page 71
Examples page 72
patch page 73
restore page 74
shutdown page 77
ver page 77

audit
Display or edit commands, entered in the shell for a specific session. The audit is not kept between sessions.
**Syntax**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>audit setlines &lt;number_of_lines&gt;</code></td>
<td>restrict the length of the command history to <code>&lt;number_of_lines&gt;</code></td>
</tr>
<tr>
<td><code>audit show &lt;number_of_lines&gt;</code></td>
<td>show the last <code>&lt;number_of_lines&gt;</code> recent commands</td>
</tr>
<tr>
<td><code>audit clear &lt;number_of_lines&gt;</code></td>
<td>clear the command history</td>
</tr>
</tbody>
</table>

### Table 4-6 Audit Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>lines</code></td>
<td>restrict the length of the command history to <code>&lt;number_of_lines&gt;</code></td>
</tr>
<tr>
<td><code>show</code></td>
<td>show the last <code>&lt;number_of_lines&gt;</code> recent commands</td>
</tr>
<tr>
<td><code>clear</code></td>
<td>clear the command history</td>
</tr>
</tbody>
</table>

**backup**

Backup the system configuration. You can also copy backup files to a number of scp and tftp servers for improved robustness of backup. The backup command, run by itself, without any additional flags, will use default backup settings and will perform a local backup.

**Syntax**

```plaintext
backup [-h] [-d] [-l] [--purge DAYS] [--sched [on hh:mm <-m DayOfMonth> | <-w DaysOfWeek> | off] [--tftp <ServerIP> [-path <Path> [<Filename>]] | [--scp <ServerIP> <Username> <Password> [-path <Path>][<Filename>]] | [--file [-path <Path>][<Filename>]]]
```
Parameters

Table 4-7  Backup Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>obtain usage</td>
</tr>
<tr>
<td>-d</td>
<td>debug flag</td>
</tr>
<tr>
<td>-l</td>
<td>flag enables VPN-1 log backup (By default, VPN-1 logs are not backed up.)</td>
</tr>
<tr>
<td>--purge DAYS</td>
<td>delete old backups from previous backup attempts</td>
</tr>
<tr>
<td>[--sched [on hh:mm &lt;-m DayOfMonth&gt;</td>
<td>&lt;-w DaysOfWeek&gt;]</td>
</tr>
<tr>
<td>-tftp &lt;ServerIP&gt; [-path &lt;Path&gt;][&lt;Filename&gt;]</td>
<td>List of IP addresses of TFTP servers, on which the configuration will be backed up, and optionally the filename.</td>
</tr>
<tr>
<td>--scp &lt;ServerIP&gt; &lt;Username&gt; &lt;Password&gt;[&lt;-path &lt;Path&gt;][&lt;Filename&gt;]</td>
<td>List of IP addresses of SCP servers, on which the configuration will be backed up, the username and password used to access the SCP Server, and optionally the filename.</td>
</tr>
<tr>
<td>--file [-path &lt;Path&gt;]&lt;Filename&gt;</td>
<td>When the backup is performed locally, specify an optional filename</td>
</tr>
</tbody>
</table>

Note - If a Filename is not specified, a default name will be provided with the following format: backup_hostname.domain-name_day of month_month_year_hour_minutes.tgz for example: backup_gateway1.mydomain.com_13_11_2003_12_47.tgz

Examples

backup -file -path /tmp filename (will put the backup file in (local) /tmp and name it filename)

backup

-tftp <ip1> -path tmp

-tftp <ip2> -path var file1
-scp <ip3> username1 password1 -path /bin file2
-file file3
--scp <ip4> username2 password2 file4
--scp <ip5> username3 password3 -path mybackup

The backup file be saved on:
1. tftp server with ip1, the backup file will be saved in the tmp directory (under the tftp server default directory – usually /tftproot) with the default file name – backup_SystemName_TimaStamp.tgz
2. tftp server with ip2 , the backup file will be saved on var (under the tftp server default directory – usually /tftproot) as file1
3. scp server with ip3 , the backup file will be saved on /bin as file2
4. locally on the default directory (/var/CPbackup/backups) as file3
5. scp server with ip4 on the username2 home directory as file4
6. scp server with ip5 on ~username3/mybackup/ with the default backup file name

**reboot**

Restart the system.

**Syntax**

```
reboot
```

**patch**

Apply an upgrade or hotfix file.

**Note** - See the Release Notes for information about when to replace the patch utility with a more recent version.
System Commands

Syntax

```bash
patch add scp <ip_address> <patch_name> [password (in expert mode)]
patch add tftp <ip_address> <patch_name>
patch add cd <patch_name>
patch add <full_patch_path>
patch log
```

Parameters

Table 4-8  Patch Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>install a new patch</td>
</tr>
<tr>
<td>log</td>
<td>list all patches installed</td>
</tr>
<tr>
<td>scp</td>
<td>install from SCP</td>
</tr>
<tr>
<td>cd</td>
<td>install from CD</td>
</tr>
<tr>
<td>tftp</td>
<td>install from TFTP server</td>
</tr>
<tr>
<td>ip</td>
<td>IP address of the tftp server containing the patch</td>
</tr>
<tr>
<td>patch_name</td>
<td>the name of the patch to be installed</td>
</tr>
<tr>
<td>password</td>
<td>password, in expert mode</td>
</tr>
<tr>
<td>full_patch_path</td>
<td>the full path for the patch file (for example, /var/tmp/mypatch.tgz)</td>
</tr>
</tbody>
</table>

**restore**

Restore the system configuration.
When the restore command is executed by itself, without any additional flags, a menu of options is displayed. The options in the menu provide the same functionality, as the command line flags, for the restore command

```
Choose one of the following:
------------------------------------------
-- 
[L] Restore local backup package
[T] Restore backup package from TFTP server
[S] Restore backup package from SCP server
[R] Remove local backup package
[Q] Quit
------------------------------------------
```

Select the operation of your choice.
**Restoring Backups of Older Versions of SecurePlatform**

When restoring backups of older versions of SecurePlatform, such as FP2, FP3 and NG AI, only system settings, such as routes, IP configuration, VLAN interfaces configuration, user accounts, hostname and domainname, and WebUI port will be restored.

You can not restore backups saved on newer SecurePlatform versions onto an older SecurePlatform version, for example you can not restore backups saved on R55 onto NG AI.

When *restore* detects that the currently installed version of Check Point products does not match the version that was stored in the backup file, the following information will be displayed:

When restoring from backups of SecurePlatform NG AI R55 and later:

The following information will be restored:

```
  system
```

The following information will NOT be restored:

```
  cp_products
```

Choose one of the following:

```
[C] Continue.
[M] Modify which information to restore.
[Q] Quit.
```

Your choice:

If you choose to continue, only system settings will be restored

When restoring from backups of SecurePlatform NG AI and earlier, the following information will be shown:
Restoring...

Backup file was created MM-DD-YYYY-HH:MM.
The MD5 checksum of the backup file is: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.
Do you wish to restore this file (Y/N)?
If you choose "N", the restore operation will be aborted.
The restore operation will replace current configuration.
After restore you have to reboot your system.
Do you wish to proceed (Y/N)?
If you choose "N", the restore operation will be aborted.
Restore completed successfully.
You have to reboot your system now. Reboot now (Y/N)?

**shutdown**

Shut down the system.

**Syntax**

```
shutdown
```

**ver**

Display the SecurePlatform system's version.

**Syntax**

```
ver
```
Snapshot Image Management

In This Section

Revert  page 78
Snapshot  page 79

Commands to take a snapshot of the entire system and to restore the system, from the snapshot, are available. The system can be restored at any time, and at boot time the user is given the option of booting from any of the available snapshots. This feature greatly reduces the risks of configuration changes.

The snapshot and revert commands can use an TFTP server or a SCP Server to store snapshots. Alternatively, snapshots can be stored locally.

**Note** - The amount of time it takes to perform a snapshot or revert depends on the amount of data (for example, logs) that is stored or restored. For example, it may take between 90 to 120 minutes to perform a snapshot or revert for SmartCenter, Log Server, Provider-1, etc.

**Revert**

Reboot the system from a snapshot file. The revert command, run by itself, without any additional flags, will use default backup settings, and will reboot the system from a local snapshot.

```
```
Parameters

Table 4-10  Revert Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>obtain usage</td>
</tr>
<tr>
<td>-d</td>
<td>debug flag</td>
</tr>
<tr>
<td>--tftp &lt;ServerIP&gt; &lt;Filename&gt;</td>
<td>IP address of the TFTP server, from which the snapshot is rebooted, as well as the filename of the snapshot.</td>
</tr>
<tr>
<td>--scp &lt;ServerIP&gt; &lt;Username&gt; &lt;Password&gt; &lt;Filename&gt;</td>
<td>IP address of the SCP server, from which the snapshot is rebooted, the username and password used to access the SCP Server, and the filename of the snapshot.</td>
</tr>
<tr>
<td>--file &lt;Filename&gt;</td>
<td>When the snapshot is made locally, specify a filename</td>
</tr>
</tbody>
</table>

The revert command functionality can also be accessed from the snapshot image management boot option.

**Snapshot**

This command creates a snapshot file. The snapshot command, run by itself, without any additional flags, will use default backup settings and will create a local snapshot.

**Syntax**

```
snapshot [-h] [-d] [(-tftp <ServerIP> <Filename>) | (-scp <ServerIP> <Username> <Password> <Filename>) | (-file <Filename>)]
```
Parameters

Table 4-11  Snapshot Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>obtain usage</td>
</tr>
<tr>
<td>-d</td>
<td>debug flag</td>
</tr>
<tr>
<td>--tftp &lt;ServerIP&gt;</td>
<td>IP address of the TFTP server, from which the snapshot is made, as well as the filename of the snapshot.</td>
</tr>
<tr>
<td>&lt;Filename&gt;</td>
<td></td>
</tr>
<tr>
<td>--scp &lt;ServerIP&gt;</td>
<td>IP address of the SCP server, from which the snapshot is made, the username and password used to access the SCP Server, and the filename of the snapshot.</td>
</tr>
<tr>
<td>&lt;Username&gt; &lt;Password&gt; &lt;Filename&gt;</td>
<td></td>
</tr>
<tr>
<td>--file &lt;Filename&gt;</td>
<td>When the snapshot is made locally, specify a filename</td>
</tr>
</tbody>
</table>

System Diagnostic Commands

In This Section

- diag  page 80
- log  page 81
- top  page 82

**diag**

Display or send the system's diagnostic information (diag files).
System Diagnostic Commands

Syntax

```
diag <log_file_name> tftp <tftp_host_ip_address>
```

Parameters

Table 4-12  Diag Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>log_file_name</td>
<td>name of the logfile to be sent</td>
</tr>
<tr>
<td>tftp</td>
<td>use tftp to upload the diagnostic information (other upload methods can be added in the future)</td>
</tr>
<tr>
<td>tftp_host_ip_address</td>
<td>IP address of the host, that is to receive the diagnostic information</td>
</tr>
</tbody>
</table>

**log**

Shows the list of available log files, applies log rotation parameters, shows the index of the log file in the list, and selects the number of lines of the log to display.
System Diagnostic Commands

**Syntax**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>log --help</code></td>
<td>Display help information for log command</td>
</tr>
<tr>
<td><code>log list</code></td>
<td>Display list of available log files</td>
</tr>
<tr>
<td><code>log limit &lt;log-index&gt; &lt;max-size&gt; &lt;backlog-copies&gt;</code></td>
<td>Apply log rotation parameters</td>
</tr>
<tr>
<td><code>log unlimit &lt;log-index&gt;</code></td>
<td>Remove log size limitations</td>
</tr>
<tr>
<td><code>log show &lt;log-index&gt; [lines]</code></td>
<td>Show log file details</td>
</tr>
</tbody>
</table>

**Parameters**

Table 4-13  Log Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>show the list of available log files</td>
</tr>
<tr>
<td>limit</td>
<td>apply log rotation parameters</td>
</tr>
<tr>
<td>unlimit</td>
<td>remove log size limitations</td>
</tr>
<tr>
<td>log-index</td>
<td>show the index of the log file, in the list</td>
</tr>
<tr>
<td>max-size</td>
<td>show the size of the log file, in bytes</td>
</tr>
<tr>
<td>backlog-copies</td>
<td>list the number of backlog copies of the log file</td>
</tr>
<tr>
<td>lines</td>
<td>select the number of lines of the log to display</td>
</tr>
</tbody>
</table>

**top**

Display the top 15 processes on the system and periodically updates this information. Raw CPU percentage is used to rank the processes.

**Syntax**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>top</td>
<td>Display top processes on the system</td>
</tr>
</tbody>
</table>
Check Point Commands

In This Section

- cpconfig
- cpstart
- cpstop
- fw
- cpinfo
- cpstat
- cplic
- cpshared_ver
- cphastart
- cphastop
- cphaprob
- fwm
- vpn
- LSMcli
- LSMcli
- LSMenabler

**cpconfig**

cpconfig displays a screen with the configuration options. The tabs that appear depend on the installed configuration and product(s). The tabs and their fields are briefly described in Table 4-14.

**Syntax**

```
cpconfig
```

**Note** - Some of the following options (Table 4-14) are available only on Modules and some are available only on the Management Server. All are shown here for convenience,
Table 4-14 Configuration Options

Welcome to VPN-1 Power Configuration Program.
============================================
This program will let you re-configure your VPN-1 Power configuration.
----------------------
(1) Licenses
(2) Administrators
(3) GUI clients
(4) SNMP Extension
(5) Groups
(6) PKCS#11 Token
(7) Random Pool
(8) Certificate Authority
(9) Secure Internal communication
(10) CA Keys
(11) Fingerprint
(12) Enable ClusterXL (High Availability)
(13) Automatic Start of Check Point Modules
(14) Exit
Enter your choice (1-14) :
Thank You...

Table 4-15 cpconfig Configuration Options

<table>
<thead>
<tr>
<th>option</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licenses</td>
<td>Updates SecurePlatform licenses.</td>
</tr>
<tr>
<td>Administrators</td>
<td>Updates the list of administrators (users who are authorized to connect to a Check Point SmartCenter server, via the Check Point SmartConsole).</td>
</tr>
<tr>
<td>GUI clients</td>
<td>Updates the list of GUI Clients and machines, where administrators are authorized to connect to a Check Point SmartCenter server, via the Check Point SmartConsole.</td>
</tr>
<tr>
<td>SNMP Extension</td>
<td>Configures the SNMP daemon. The SNMP daemon enables SecurePlatform to export its status to external network management tools.</td>
</tr>
<tr>
<td>Groups</td>
<td>Updates the list of Unix groups, authorized to run SecurePlatform.</td>
</tr>
<tr>
<td>PKCS #11 Token</td>
<td>Registers a cryptographic token, for use by SecurePlatform; see details of the token, and test its functionality.</td>
</tr>
<tr>
<td>Random Pool</td>
<td>Configures the RSA keys, to be used by SecurePlatform.</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>Configures Certificate Authority keys, to be used by SecurePlatform.</td>
</tr>
</tbody>
</table>
Check Point Commands

**Table 4-15  cpconfig Configuration Options**

<table>
<thead>
<tr>
<th>option</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Internal communication</td>
<td>Used to set up trust between this machine and the Check Point SmartCenter server. Once trust is established, this machine can communicate with other Check Point communicating components.</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Shows the Check Point SmartCenter server's fingerprint, a text string derived from the certificate of the Check Point SmartCenter server. It is used to verify the identity of the Check Point SmartCenter server, being accessed via the GUI Client.</td>
</tr>
<tr>
<td>ClusterXL (High Availability)</td>
<td>Specifies whether this gateway is a member of a ClusterXL (High Availability) Gateway Cluster.</td>
</tr>
<tr>
<td>Automatic Start of Check Point Modules</td>
<td>Check Point Modules specify whether SecurePlatform will start automatically at boot time.</td>
</tr>
</tbody>
</table>

**cpstart**

cpstart starts all the Check Point applications running on a machine (other than cprid, which is invoked upon boot, and keeps on running independently). cpstart implicitly invokes fwstart (or any other installed Check Point product, such as etmstart, uagstart, etc.).

**Syntax**

```
cpstart
```  

**cpstop**

cpstop stops all the Check Point applications running on a machine (other than cprid, which is invoked upon boot and keeps on running independently). cpstop implicitly invokes fwstop (or any other installed Check Point product, such as etmstop, uagstop, etc.).

**Syntax**

```
cpstop
```  

**fw**

Executes SecurePlatform commands.
Syntex

Table 4-16  fw Syntax

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>fw ver [-k]</td>
</tr>
<tr>
<td>fw kill [-t sig_no] procname</td>
</tr>
<tr>
<td>fw putkey</td>
</tr>
<tr>
<td>fw sam</td>
</tr>
<tr>
<td>fw fetch targets</td>
</tr>
<tr>
<td>fw tab [-h]</td>
</tr>
<tr>
<td>fw monitor [-h]</td>
</tr>
<tr>
<td>fw ctl [args]</td>
</tr>
<tr>
<td>fw lichosts</td>
</tr>
<tr>
<td>fw log [-h]</td>
</tr>
<tr>
<td>fw logswitch [-h target] [+-] [oldlog]</td>
</tr>
<tr>
<td>fw repairlog ...</td>
</tr>
<tr>
<td>fw mergefiles</td>
</tr>
<tr>
<td>fw lslogs</td>
</tr>
<tr>
<td>fw fetchlogs</td>
</tr>
</tbody>
</table>
**Parameters**

**Table 4-17  fw Syntax Options**

<table>
<thead>
<tr>
<th>syntax</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>fw ver [-k]</td>
<td>display version</td>
</tr>
<tr>
<td>fw kill [-t sig_no]</td>
<td>send signal to a daemon proclename</td>
</tr>
<tr>
<td>fw putkey</td>
<td>client server keys</td>
</tr>
<tr>
<td>fw sam</td>
<td>control sam server</td>
</tr>
<tr>
<td>fw fetch targets</td>
<td>fetch last policy</td>
</tr>
<tr>
<td>fw tab [-h]</td>
<td>kernel tables content</td>
</tr>
<tr>
<td>fw monitor [-h]</td>
<td>monitor SecurePlatform traffic</td>
</tr>
<tr>
<td>fw ctl [args]</td>
<td>control kernel</td>
</tr>
<tr>
<td>fw lichosts</td>
<td>display protected hosts</td>
</tr>
<tr>
<td>fw log [-h]</td>
<td>display logs</td>
</tr>
<tr>
<td>fw logswitch [-h target] [+</td>
<td>-][oldlog]</td>
</tr>
<tr>
<td>fw repairlog ...</td>
<td>log index recreation</td>
</tr>
<tr>
<td>fw mergefiles</td>
<td>log files merger</td>
</tr>
<tr>
<td>fw lslogs</td>
<td>Remote machine log files list</td>
</tr>
<tr>
<td>fw fetchlogs</td>
<td>Fetch logs from a remote host</td>
</tr>
</tbody>
</table>

**cpinfo**

Show Check Point diagnostics information.
Check Point Commands

Syntax

```
cpinfo [-v] [-o filename]
```

Parameters

Table 4-18  cpinfo Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>v</td>
<td>Show cpinfo version (expert mode only)</td>
</tr>
<tr>
<td>-o filename</td>
<td>Store output in filename (expert mode only)</td>
</tr>
</tbody>
</table>

**cpstat**

cpstat displays, in various formats, the status of Check Point applications on a local or non-local machine.
Syntax

```bash
cpstat [-h host][-p port][-f flavour][-d] application_flag
```

Parameters

Table 4-19  
<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-h host</code></td>
<td>A resolvable hostname, or a dot-notation address (for example, 192.168.33.23). 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>-f flavor</code></td>
<td>The flavor of the output (as appears in the configuration file). The default is to use the first flavor found in the configuration file.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>entity</th>
<th>One of:</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>fw</code></td>
<td>FireWall-1</td>
</tr>
<tr>
<td><code>vpn</code></td>
<td>VPN-1</td>
</tr>
<tr>
<td><code>fg</code></td>
<td>FloodGate-1</td>
</tr>
<tr>
<td><code>ha</code></td>
<td>Cluster XL (High Availability)</td>
</tr>
<tr>
<td><code>os</code></td>
<td>for SVN Foundation and OS Status</td>
</tr>
<tr>
<td><code>mg</code></td>
<td>for Management Status</td>
</tr>
</tbody>
</table>

**cplic**

Show, add or remove Check Point licenses.
**Syntax**

```
cplic [put | del | print | check ]
```

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>put</td>
<td>The CPlic put command (located in <code>$CPDIR/bin</code>) is used to install one or more local licenses. This command installs a license on a local machine and it cannot be performed remotely.</td>
</tr>
<tr>
<td>del</td>
<td>The CPlic del command (located in <code>$CPDIR/bin</code>) deletes a single Check Point license on a host. Use it to delete unwanted evaluation, expired, and other licenses.</td>
</tr>
<tr>
<td>print</td>
<td>The CPlic print command (located in <code>$CPDIR/bin</code>) prints details of Check Point licenses on the local machine.</td>
</tr>
<tr>
<td>check</td>
<td>The CPlic check command (located in <code>$CPDIR/bin</code>) checks whether the license on the machine will allow a given feature to be used.</td>
</tr>
</tbody>
</table>

**cpshared_ver**

Show the SVN Foundation’s version.

**Syntax**

```
cpshared_ver
```

**cphastart**

`cphastart` enables the Cluster XL feature on the machine.

**Syntax**

```
cphastart start
```

**cphastop**

`cphastop` disables the Cluster XL feature on the machine.
Syntax

Cphastop

cphaprob
cphaprob defines "critical" processes. When a critical process fails, the machine is considered to have failed.
### Syntax

```bash
  cphaprob -d <device> -t <timeout(sec)> -s <ok|init|problem> register
  cphaprob -f <file> register
  cphaprob -d <device> unregister
  cphaprob -a unregister
  cphaprob -d <device> -s <ok|init|problem> report
  cphaprob [-i[a]] [-e] list
  cphaprob state
  cphaprob [-a] if
```

### Parameters

#### Table 4-21 cphaprob Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>register</td>
<td>Register <code>&lt;device&gt;</code> as a critical process.</td>
</tr>
<tr>
<td>-d <code>&lt;device&gt;</code></td>
<td><code>&lt;device&gt;</code> should be the name of the device as it will appear in the output of the <code>cphaprob list</code>.</td>
</tr>
<tr>
<td>-t <code>&lt;timeout&gt;</code></td>
<td>If <code>&lt;device&gt;</code> fails to contact the CPHA Module in <code>&lt;timeout&gt;</code> seconds, <code>&lt;device&gt;</code> will be considered to have failed. To disable this parameter, enter <code>&lt;0&gt;</code> as the timeout value. The state will stay as last reported, until explicitly reported otherwise.</td>
</tr>
<tr>
<td>-s</td>
<td>The status to be reported — one of:</td>
</tr>
<tr>
<td></td>
<td>• “ok” — <code>&lt;device&gt;</code> is alive</td>
</tr>
<tr>
<td></td>
<td>• “init” — <code>&lt;device&gt;</code> is initializing</td>
</tr>
<tr>
<td></td>
<td>• “problem” — <code>&lt;device&gt;</code> has failed</td>
</tr>
<tr>
<td>-f <code>&lt;file&gt;</code> register</td>
<td>This option allows you to automatically register several devices. The file defined in the <code>&lt;file&gt;</code> field should contain the list of devices with the following parameters:</td>
</tr>
<tr>
<td></td>
<td>• device name,</td>
</tr>
<tr>
<td></td>
<td>• timeout, and</td>
</tr>
<tr>
<td></td>
<td>• state</td>
</tr>
<tr>
<td>Unregister</td>
<td>Unregister <code>&lt;device&gt;</code> as a critical process. <code>-a unregister</code> will unregister all devices.</td>
</tr>
<tr>
<td>report</td>
<td>Report status of <code>&lt;device&gt;</code> to the VPN/FireWall Module.</td>
</tr>
</tbody>
</table>
A process, specified by `<device>`, should run `cphaprob` with the `-s ok` parameter, to notify the ClusterXL (High Availability) Module that the process is alive. If this notification is not received in `<timeout>` seconds, the process (and the machine) will be considered to have failed.

**fwm**

`fwm` executes SmartCenter server commands.

**Syntax**

```
fwm ver [-h] ... targets
fwm unload [opts] targets
fwm dbload [targets]
FWM logexport [-h] ...
fwm gen [-RouterType [-import]] rule-base
fwm dbexport [-h] ...
fwm ikecrypt <key> <password>
fwm ver [-h] ...
fwm load [opts] [filter-file|rule-base] targets
fwm unload [opts] targets
fwm dbload [targets]
fwm logexport [-h] ...
fwm gen [-RouterType [-import]] rule-base
fwm dbexport [-h] ...
fwm ikecrypt <key> <password>
fwm dbimport [-h] ...
```
Parameters

Table 4-22 fwm Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>fwm ver [-h]</td>
<td>Display version</td>
</tr>
<tr>
<td>fwm load [opts] [filter-file</td>
<td>rule-base] targets</td>
</tr>
<tr>
<td>fwm unload [opts] targets</td>
<td>Uninstall targets</td>
</tr>
<tr>
<td>fwm dbload [targets]</td>
<td>Download the database</td>
</tr>
<tr>
<td>fwm logexport [-h] ...</td>
<td>Export log to ascii file</td>
</tr>
<tr>
<td>fwm gen [-RouterType [import]] rule-base</td>
<td>Generate an inspection script or a router access-list</td>
</tr>
<tr>
<td>fwm dbexport [-h] ...</td>
<td>Export the database</td>
</tr>
<tr>
<td>fwm ikecrypt &lt;key&gt; &lt;password&gt;</td>
<td>Encrypt a secret with a key</td>
</tr>
<tr>
<td>fwm dbimport [-h] ...</td>
<td>Import to database (for the dbexport command)</td>
</tr>
</tbody>
</table>

vvpn

This command and subcommands are used for working with various aspects of VPN. VPN commands executed on the command line generate status information regarding VPN processes, or are used to stop and start specific VPN services. All VPN commands are executed on the VPN-1 module. The vpn command sends to the standard output a list of available commands.
- `vpn ver` displays the VPN-1 major version number, the build number, and a copyright notice. Usage and options are the same as for `fw ver`.
- `vpn debug` instructs the VPN daemon to write debug messages to the VPN log file: in `$FWDIR/log/vpnd.elg`.
- `vpn debug ikeon | ikeoff` instructs the VPN daemon to write debug messages to the IKE log file: `$FWDIR/log/IKE.elg`.
- `vpn drv` installs the vpnk kernel and connects to the fwk kernel, attaching the corresponding drivers.

For more information, refer to the *CheckPoint R65 Command Line Interface Administration Guide*.

**Syntax**

```plaintext
vpn ver
vpn debug on | off
vpn debug ikeon | ikeoff
vpn drv on | off
```

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ver</code></td>
<td>Displays the VPN-1 major version number, the build number, and a copyright notice.</td>
</tr>
<tr>
<td>`debug on</td>
<td>off`</td>
</tr>
<tr>
<td>`debug ikeon</td>
<td>ikeoff`</td>
</tr>
<tr>
<td>`drv on</td>
<td>off`</td>
</tr>
</tbody>
</table>
LSMcli

LSMcli configures Smart LSM. See the CheckPoint R65 SmartLSM Administration Guide for information about the command’s parameters.

Syntax

| LSMcli [-h | --help] |
|---------------------|
| LSMcli [-d] <Server> <User> <Pswd> <Action> |

LSMenabler

LSMenabler enables or disables Smart LSM. See the CheckPoint R65 SmartLSM Administration Guide for information about the command’s parameters.

Syntax

| LSMMenabler [-d] [-r] <off|on> |

Network Diagnostics Commands

In This Section

- ping page 96
- traceroute page 98
- netstat page 100

ping

send ICMP ECHO_REQUEST packets to network hosts.
Syntax

```
```

Parameters

Table 4-24 ping Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c count</td>
<td>Stop after sending (and receiving) count ECHO_RESPONSE packets.</td>
</tr>
<tr>
<td>-d</td>
<td>Set the SO_DEBUG option for the socket being used.</td>
</tr>
<tr>
<td>-f</td>
<td>Flood ping. Outputs packets as fast as they come back, or one hundred times per second, whichever is greater. For every ECHO_REQUEST sent, a period &quot;.&quot; is printed, while for every ECHO_REPLY received, a backspace is printed. This provides a rapid display of how many packets are being dropped. Only the super-user may use this option. This can place a very heavy load on a network and should be used with caution.</td>
</tr>
<tr>
<td>-i wait</td>
<td>Wait: wait i seconds between sending each packet. The default is to wait for one second between each packet. This option is incompatible with the -f option.</td>
</tr>
<tr>
<td>-l</td>
<td>Preload: if preload is specified, ping sends that many packets as fast as possible before falling into its normal mode of behavior. Only the super-user may use this option.</td>
</tr>
<tr>
<td>-n</td>
<td>Numeric output only. No attempt will be made to lookup symbolic names for host addresses.</td>
</tr>
<tr>
<td>-p pattern</td>
<td>You may specify up to 16 &quot;pad&quot; bytes to fill out the packet you send. This is useful for diagnosing data-dependent problems in a network. For example, &quot;-p ff&quot; will direct the sent packet to be filled with a series of ones (&quot;1&quot;).</td>
</tr>
<tr>
<td>-q</td>
<td>Quiet output. Nothing is displayed except the summary lines at the time of startup and finish.</td>
</tr>
<tr>
<td>-R</td>
<td>Record route. Includes the RECORD_ROUTE option in the ECHO_REQUEST packet and displays the route buffer on returned packets. Note that the IP header is only large enough for nine such routes. Many hosts ignore or discard this option.</td>
</tr>
</tbody>
</table>
Network Diagnostics Commands

**traceroute**

Tracking the route a packet follows (or finding the miscreant gateway that is discarding your packets) can be difficult. Traceroute utilizes the IP protocol ‘time to live’ field and attempts to elicit an ICMP *TIME_EXCEEDED* response from each gateway along the path to a designated host.

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-r</td>
<td>Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it.</td>
</tr>
<tr>
<td>-s packetsize</td>
<td>Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes, when combined with the 8 bytes of ICMP header data.</td>
</tr>
<tr>
<td>-v</td>
<td>Verbose (detailed) output. Lists ICMP packets (other than <em>ECHO_RESPONSE</em>) that are received.</td>
</tr>
</tbody>
</table>

**Table 4-24** ping Parameters
Syntax

```
traceroute [ -d | -f | -I | -m | -n | -p port ] [ -q nqueries | -s src_addr | -t tos | -w waittime ] host [ packetlen ]
```

Parameters

Table 4-25  traceroute Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f first_ttl</td>
<td>Set the initial time-to-live, used in the first outgoing probe packet.</td>
</tr>
<tr>
<td>-F</td>
<td>Set the &quot;don't fragment&quot; bit.</td>
</tr>
<tr>
<td>-d</td>
<td>Enable socket level debugging.</td>
</tr>
<tr>
<td>-g</td>
<td>Gateway: specify a loose source route gateway (8 maximum).</td>
</tr>
<tr>
<td>-i iface</td>
<td>iface: specify a network interface, to obtain the source IP address for outgoing probe packets. This is normally only useful on a multi-homed host. (See the -s flag for another way to do this.)</td>
</tr>
<tr>
<td>-I</td>
<td>Use ICMP ECHO instead of UDP datagrams.</td>
</tr>
<tr>
<td>-m max_ttl</td>
<td>Set the max time-to-live (maximum number of hops) used in outgoing probe packets. The default is 30 hops (the same default used for TCP connections).</td>
</tr>
<tr>
<td>-n</td>
<td>Print hop addresses numerically, rather than symbolically and numerically (saves a nameserver address-to-name lookup, for each gateway found on the path).</td>
</tr>
<tr>
<td>-p port</td>
<td>Set the base UDP port number used in probes (default is 33434). Traceroute hopes that nothing is listening on UDP ports base to base + nhops - 1 at the destination host (so an ICMP PORT_UNREACHABLE message will be returned to terminate the route tracing). If something is listening on a port in the default range, this option can be used to pick an unused port range.</td>
</tr>
<tr>
<td>-q nqueries</td>
<td>Number of queries to run.</td>
</tr>
<tr>
<td>-r</td>
<td>Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it.</td>
</tr>
</tbody>
</table>
### Table 4-25  traceroute Parameters (continued)

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s src_addr</td>
<td>Use the following IP address (which usually is given as an IP number, not a hostname) as the source address in out-going probe packets. On multi-homed hosts (those with more than one IP address), this option can be used to force the source address to be something, other than the IP address of the interface that the probe packet is sent on. If the IP address is not one of this machine's interface addresses, an error is returned and nothing is sent. (See the -i flag for another way to do this.)</td>
</tr>
<tr>
<td>-t tos</td>
<td>Set the type-of-service in probe packets to the following value (default zero). The value must be a decimal integer in the range 0 to 255. This option can be used to see if different types-of-service result in different paths. (If you are not running 4.4bsd, this may be irrelevant, since the normal network services like telnet and ftp don't let you control the TOS. Not all values of TOS are legal or meaningful, see the IP spec for definitions. Useful values are probably &quot;-t 16&quot; (low delay) and &quot;-t 8&quot; (high throughput).</td>
</tr>
<tr>
<td>-v</td>
<td>Verbose (detailed) output. Received ICMP packets other than TIME_EXCEEDED and UNREACHABLES are listed.</td>
</tr>
<tr>
<td>-w waittime</td>
<td>Set the time (in seconds) to wait for a response to a probe (default is 5 seconds).</td>
</tr>
<tr>
<td>-x</td>
<td>Toggle checksums. Normally, this prevents traceroute from calculating checksums. In some cases, the operating system can overwrite parts of the outgoing packet, but not recalculate the checksum (In some cases, the default is not to calculate checksums. Using -x causes checksums to be calculated). Checksums are usually required for the last hop, when using ICMP ECHO probes (-I).</td>
</tr>
</tbody>
</table>

### netstat

Show network statistics.
**Syntax**

```
netstat [-veenCnP] [<AF>] -r
netstat (-V|--version|--help)
netstat [-vmNcaol] [<Socket> ...]
netstat { [-veenNC] -i | [-cnNe] -M | -s }
```

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
<th>extended meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-r</td>
<td>route</td>
<td>display routing table</td>
</tr>
<tr>
<td>-i</td>
<td>interfaces</td>
<td>display interface table</td>
</tr>
<tr>
<td>-g</td>
<td>groups</td>
<td>display multicast group memberships</td>
</tr>
<tr>
<td>-s</td>
<td>statistics</td>
<td>display networking statistics (like SNMP)</td>
</tr>
<tr>
<td>-M</td>
<td>masquerade</td>
<td>display masqueraded connections</td>
</tr>
<tr>
<td>-v</td>
<td>verbose</td>
<td>be verbose (detailed)</td>
</tr>
<tr>
<td>-n</td>
<td>numeric</td>
<td>do not resolve names</td>
</tr>
<tr>
<td>-N</td>
<td>symbolic</td>
<td>resolve hardware names</td>
</tr>
<tr>
<td>-e</td>
<td>extend</td>
<td>display other/more information</td>
</tr>
<tr>
<td>-p</td>
<td>programs</td>
<td>display PID/Program name for sockets</td>
</tr>
<tr>
<td>-c</td>
<td>continuous</td>
<td>continuous listing</td>
</tr>
<tr>
<td>-l</td>
<td>listening</td>
<td>display listening server sockets</td>
</tr>
<tr>
<td>-a</td>
<td>all, listening</td>
<td>display all sockets (default: connected)</td>
</tr>
<tr>
<td>-o</td>
<td>timers</td>
<td>display timers</td>
</tr>
<tr>
<td>-F</td>
<td>fib</td>
<td>display Forwarding Information Base (default)</td>
</tr>
<tr>
<td>-C</td>
<td>cache</td>
<td>display routing cache, instead of FIB</td>
</tr>
<tr>
<td>&lt;Socket&gt;</td>
<td></td>
<td>Type of socket, may be one of the following:</td>
</tr>
<tr>
<td>-A &lt;AF&gt;,</td>
<td>af &lt;AF&gt;</td>
<td>Address family, may be one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>netrom (AMPR NET/ROM) ipx (Novell IPX) ddp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Appletalk DDP)</td>
</tr>
</tbody>
</table>
Network Configuration Commands

In This Section

arp
addarp
delarp
hosts
ifconfig
vconfig
route
hostname
domainname
dns
sysconfig
webui

arp

arp manipulates the kernel's ARP cache in various ways. The primary options are clearing an address mapping entry and manually setting one up. For debugging purposes, the ARP program also allows a complete dump of the ARP cache.

Syntax

```
arp [-vn] [-H type] [-i if] -a [hostname]
arp [-v] [-i if] -d hostname [pub]
arp [-v] [-H type] [-i if] -s hostname hw_addr [temp]
arp [-v] [-H type] [-i if] -s hostname hw_addr [netmask nm] pub
arp [-v] [-H type] [-i if] -Ds hostname ifa [netmask nm] pub
arp [-vnD] [-H type] [-i if] -f [filename]
```
**addarp**

Addarp adds a persistent ARP entry (one that will survive re-boot).

**Syntax**

```
addarp <hostname> <hwaddr>
```

**delarp**

Delarp removes ARP entries created by addarp.

**Syntax**

```
delarp <hostname> <MAC>
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
<th>Extended Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-v</td>
<td>verbose</td>
<td>Tell the user the details of what is going on.</td>
</tr>
<tr>
<td>-n</td>
<td>numeric</td>
<td>Shows numerical addresses instead of trying to determine symbolic host, port or user names.</td>
</tr>
<tr>
<td>-H type, hw-type</td>
<td></td>
<td>When setting, or reading the ARP cache, this optional parameter tells arp which class of entries it should check for. The default value of this parameter is ether (i.e. hardware code 0x01 for IEEE 802.3 10Mbps Ethernet). Other values might include network technologies such as ARCnet (arcnet), PROnet (pronet), AX.25 (ax25) and NET/ROM (netrom).</td>
</tr>
<tr>
<td>-a [hostname]</td>
<td>display [hostname]</td>
<td>Shows the entries of the specified hosts. If the hostname parameter is not used, all entries will be displayed.</td>
</tr>
<tr>
<td>-d hostname</td>
<td>delete hostname</td>
<td>Remove any entry for the specified host. This can be used if the indicated host is brought down, for example.</td>
</tr>
</tbody>
</table>
Network Configuration Commands

Table 4-27  arp Parameters (continued)

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
<th>extended meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-D</td>
<td>use-device</td>
<td>Use the interface ifa’s hardware address.</td>
</tr>
<tr>
<td>-i If</td>
<td>device If</td>
<td>Select an interface. When dumping the ARP cache, only entries matching the specified interface will be printed. When setting a permanent, or temp ARP, entry this interface will be associated with the entry. If this option is not used, the kernel will guess, based on the routing table. For public entries, the specified interface is the interface, on which ARP requests will be answered.</td>
</tr>
<tr>
<td>-f filename</td>
<td>file filename</td>
<td>Similar to the -s option, only this time the address info is taken from file filename set up. The name of the data file is very often /etc/ethers. If no filename is specified /etc/ethers is used as default.</td>
</tr>
</tbody>
</table>
**hosts**

Show, set or remove hostname to IP-address mappings.

**Syntax**

```
hosts add <IP-ADDRESS> <host1> [...]
hosts remove <IP-ADDRESS> <host1> [...]
hosts
```

**Parameters**

**Table 4-28**)  hosts Parameters

<table>
<thead>
<tr>
<th>hosts</th>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running</td>
<td>hosts</td>
<td>Running hosts, with no parameters, displays the current host names to IP mappings.</td>
</tr>
<tr>
<td>add</td>
<td>IP-ADDRESS</td>
<td>IP address, to which hosts will be added.</td>
</tr>
<tr>
<td></td>
<td>host1, host2...</td>
<td>Hosts to be added.</td>
</tr>
<tr>
<td>remove</td>
<td>IP-ADDRESS</td>
<td>IP address, to which hosts will be removed.</td>
</tr>
<tr>
<td></td>
<td>host1, host2...</td>
<td>The name of the hosts to be removed.</td>
</tr>
</tbody>
</table>

**ifconfig**

Show, configure or store network interfaces settings.
Syntax

```
ifconfig [-a] [-i] [-v] [-s] <interface> [[<AF>] <address>]
[add <address>[/<prefixlen>]]
[del <address>[/<prefixlen>]]
[[-]broadcast [<address>]] [[-]pointopoint [<address>]]
[netmask <address>] [dstaddr <address>] [tunnel <address>]
[outfill <NN>] [keepalive <NN>]
[hw <HW> <address>] [metric <NN>] [mtu <NN>]
[[-]trailers] [[-]arp] [[-]allmulti]
[multicast] [[-]promisc]
[mem_start <NN>] [io_addr <NN>] [irq <NN>] [media <type>]
[txqueuelen <NN>]
[[-]dynamic]
[up|down]
[=--save]
```

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>interface</strong></td>
<td>The name of the interface. This is usually a driver name, followed by a unit number, for example eth0 for the first Ethernet interface.</td>
</tr>
<tr>
<td><strong>up</strong></td>
<td>This flag causes the interface to be activated. It is implicitly specified if an address is assigned to the interface.</td>
</tr>
<tr>
<td><strong>down</strong></td>
<td>This flag causes the driver, for this interface, to be shut down.</td>
</tr>
<tr>
<td><strong>[-]arp</strong></td>
<td>Enable or disable the use of the ARP protocol, on this interface.</td>
</tr>
<tr>
<td><strong>[-]promisc</strong></td>
<td>Enable or disable the promiscuous mode of the interface. If selected, all packets on the network will be received by the interface.</td>
</tr>
<tr>
<td><strong>[-]allmulti</strong></td>
<td>Enable or disable all-multicast mode. If selected, all multicast packets on the network will be received by the interface.</td>
</tr>
<tr>
<td><strong>metric N</strong></td>
<td>This parameter sets the interface metric.</td>
</tr>
<tr>
<td><strong>mtu N</strong></td>
<td>This parameter sets the Maximum Transfer Unit (MTU) of an interface.</td>
</tr>
<tr>
<td><strong>dstaddr addr</strong></td>
<td>Set the remote IP address for a point-to-point link (such as PPP). This keyword is now obsolete; use the point-to-point keyword instead.</td>
</tr>
<tr>
<td><strong>netmask addr</strong></td>
<td>Set the IP network mask, for this interface. This value defaults to the usual class A, B or C network mask (as derived from the interface IP address), but it can be set to any value.</td>
</tr>
</tbody>
</table>
### Table 4-29  ifConfig Parameters (continued)

| Parameter     | Meaning                                                                联网配置命令
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>irq addr</td>
<td>Set the interrupt line used by this device. Not all devices can</td>
</tr>
<tr>
<td></td>
<td>dynamically change their IRQ setting.</td>
</tr>
<tr>
<td>io_addr addr</td>
<td>Set the start address in I/O space for this device.</td>
</tr>
<tr>
<td>mem_start addr</td>
<td>Set the start address for shared memory used by this device. Only a few</td>
</tr>
<tr>
<td></td>
<td>devices need this parameter set.</td>
</tr>
<tr>
<td>media type</td>
<td>Set the physical port, or medium type, to be used by the device.</td>
</tr>
<tr>
<td></td>
<td>Not all devices can change this setting, and those that can vary</td>
</tr>
<tr>
<td></td>
<td>in what values they support. Typical values for type are 10base2 (thin</td>
</tr>
<tr>
<td></td>
<td>Ethernet), 10baseT (twisted-pair 10Mbps Ethernet), AUI (external</td>
</tr>
<tr>
<td></td>
<td>transceiver) and so on. The special, medium type of auto can be used</td>
</tr>
<tr>
<td></td>
<td>to tell the driver to auto-sense the media. Not all drivers support</td>
</tr>
<tr>
<td>[-]broadcast [addr]</td>
<td>If the address argument is given, set the protocol broadcast</td>
</tr>
<tr>
<td></td>
<td>address for this interface. Otherwise, set (or clear) the</td>
</tr>
<tr>
<td></td>
<td>IFF_BROADCAST flag for the interface.</td>
</tr>
<tr>
<td>[-]pointopoint [addr]</td>
<td>This keyword enables the point-to-point mode of an interface,</td>
</tr>
<tr>
<td></td>
<td>meaning that it is a direct link between two machines, with</td>
</tr>
<tr>
<td></td>
<td>nobody else listening on it. If the address argument is also</td>
</tr>
<tr>
<td></td>
<td>given, set the protocol address of the other side of the link, just</td>
</tr>
<tr>
<td></td>
<td>like the obsolete dstaddr keyword does. Otherwise, set or clear the</td>
</tr>
<tr>
<td></td>
<td>IFF_POINTOPOINT flag for the interface.</td>
</tr>
<tr>
<td>hw class address</td>
<td>Set the hardware address of this interface, if the device driver</td>
</tr>
<tr>
<td></td>
<td>supports this operation. The keyword must be followed by the</td>
</tr>
<tr>
<td></td>
<td>name of the hardware class and the printable ASCII equivalent of the</td>
</tr>
<tr>
<td></td>
<td>hardware address. Hardware classes currently supported include: ether</td>
</tr>
<tr>
<td></td>
<td>(Ethernet), ax25 (AMPR AX.25), ARCnet and netrom (AMPR NET/ROM).</td>
</tr>
<tr>
<td>multicast</td>
<td>Set the multicast flag on the interface. This should not normally</td>
</tr>
<tr>
<td></td>
<td>be needed, as the drivers set the flag correctly themselves.</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address to be assigned to this interface.</td>
</tr>
<tr>
<td>txqueuelen length</td>
<td>Set the length of the transmit queue of the device. It is useful to</td>
</tr>
<tr>
<td></td>
<td>set this to small values, for slower devices with a high latency</td>
</tr>
<tr>
<td></td>
<td>(modem links, ISDN), to prevent fast bulk transfers from</td>
</tr>
<tr>
<td></td>
<td>disturbing interactive traffic, like telnet, too much.</td>
</tr>
<tr>
<td>--save</td>
<td>Saves the interface IP configuration. Not available when</td>
</tr>
<tr>
<td></td>
<td>VPN-1 UTM is installed.</td>
</tr>
</tbody>
</table>
**vconfig**

Configure virtual LAN interfaces.

**Syntax**

```
vconfig add [interface-name] [vlan_id]
vconfig rem [vlan-name]
```

**Parameters**

Table 4-30  vconfig Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-name</td>
<td>The name of the Ethernet card that hosts the VLAN.</td>
</tr>
<tr>
<td>vlan_id</td>
<td>The identifier (0-4095) of the VLAN.</td>
</tr>
<tr>
<td>skb_priority</td>
<td>The priority in the socket buffer (sk_buff).</td>
</tr>
<tr>
<td>vlan_qos</td>
<td>The 3 bit priority field in the VLAN header.</td>
</tr>
<tr>
<td>name-type</td>
<td>One of:</td>
</tr>
<tr>
<td></td>
<td>• VLAN_PLUS_VID (e.g. vlan0005),</td>
</tr>
<tr>
<td></td>
<td>• VLAN_PLUS_VID_NO_PAD (e.g. vlan5),</td>
</tr>
<tr>
<td></td>
<td>• DEV_PLUS_VID (e.g. eth0.0005),</td>
</tr>
<tr>
<td></td>
<td>• DEV_PLUS_VID_NO_PAD (e.g. eth0.5)</td>
</tr>
<tr>
<td>bind-type</td>
<td>One of:</td>
</tr>
<tr>
<td></td>
<td>• PER_DEVICE  # Allows vlan 5 on eth0 and eth1 to be unique</td>
</tr>
<tr>
<td></td>
<td>• PER_KERNEL  # Forces vlan 5 to be unique across all devices</td>
</tr>
<tr>
<td>flag-num</td>
<td>Either 0 or 1 (REORDER_HDR). If set, the VLAN device will</td>
</tr>
<tr>
<td></td>
<td>move the Ethernet header around to make it look exactly like a real</td>
</tr>
<tr>
<td></td>
<td>Ethernet device.</td>
</tr>
</tbody>
</table>

**route**

Show, configure or save the routing entries.
Network Configuration Commands

Chapter 4 Administration 109

Syntax

route [-nNvee] [-FC] [<AF>] List kernel routing tables
route [-v] [-FC] {add|del|flush} ... Modify routing table for AF.
route (-h|--help) [<AF>] Detailed usage syntax for specified AF.
route (-V|--version) Display version/author and exit.
route --save

Table 4-31 route Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
<th>extended meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-v</td>
<td>verbose</td>
<td>be verbose (detailed)</td>
</tr>
<tr>
<td>-n</td>
<td>numeric</td>
<td>do not resolve names</td>
</tr>
<tr>
<td>-N</td>
<td>symbolic</td>
<td>resolve hardware names</td>
</tr>
<tr>
<td>-e</td>
<td>extend</td>
<td>display other or more information</td>
</tr>
<tr>
<td>-F</td>
<td>fib</td>
<td>display Forwarding Information Base (default)</td>
</tr>
<tr>
<td>-C</td>
<td>cache</td>
<td>display routing cache, instead of FIB</td>
</tr>
<tr>
<td>-A &lt;AF&gt;</td>
<td>af &lt;AF&gt;</td>
<td>Address family, may be one of the following: inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)</td>
</tr>
</tbody>
</table>

netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)

| save | | |
|------| | Save the routing configuration |

hostname

Show or set the system’s host name.
**Network Configuration Commands**

**Syntax**

```bash
hostname [--help]
hostname <host>
hostname <host> <external_ip_address>
```

**Table 4-32  hostname Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>show host name</td>
<td>show host name</td>
</tr>
<tr>
<td>host</td>
<td>new host name</td>
</tr>
<tr>
<td>external_ip_address</td>
<td>IP address of the interface to be assigned</td>
</tr>
<tr>
<td>help</td>
<td>show usage message</td>
</tr>
</tbody>
</table>

**domainname**

Show or set the system's domain name.

**Syntax**

```bash
domainname [<domain>]
```

**Parameters**

**Table 4-33  domainname Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show domainname</td>
<td>Show domainname</td>
</tr>
<tr>
<td>domain</td>
<td>Set domainname to domain</td>
</tr>
</tbody>
</table>

**dns**

Add, remove, or show the Domain Name resolving servers.
**Syntax**

\[ \text{dns } [\text{add|del } <\text{ip_of_nameserver}>] \]

**Parameters**

**Table 4-34** dns Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>show DNS servers configured</td>
<td></td>
</tr>
<tr>
<td>add</td>
<td>add new nameserver</td>
</tr>
<tr>
<td>del</td>
<td>delete existing nameserver</td>
</tr>
<tr>
<td>&lt;ip_of_nameserver&gt;</td>
<td>IP address of the nameserver</td>
</tr>
</tbody>
</table>

**sysconfig**

Interactive script to set networking and security of the system.

**Syntax**

\[ \text{sysconfig} \]

**webui**

webui configures the port the SecurePlatform HTTPS web server uses for the management interface.

**Syntax**

\[ \text{webui enable [https_port]} \]
\[ \text{webui disable} \]

**Parameters**

**Table 4-35** webui parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable [https_port]</td>
<td>enable the Web GUI on port https_port</td>
</tr>
<tr>
<td>disable</td>
<td>disable the Web GUI</td>
</tr>
</tbody>
</table>
Dynamic Routing Commands

Only SecurePlatform Pro supports Dynamic Routing Commands.

**router**

Configures Check Point Dynamic Routing.

**Syntax**

```
router [enable | config | disable]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable Dynamic Routing</td>
</tr>
<tr>
<td>config</td>
<td>invokes the Dynamic Routing CLI (For more information, refer to “Command Line Interface” on page 123.)</td>
</tr>
<tr>
<td>disable</td>
<td>disable Dynamic Routing</td>
</tr>
</tbody>
</table>
User and Administrator Commands

In This Section

- adduser  
- deluser  
- showusers  
- lockout  
- unlockuser  
- checkuserlock

adduser

adduser adds a SecurePlatform administrator. (SecurePlatform supports RADIUS authentication for SecurePlatform administrators.)

Syntax

```
adduser [-x EXTERNAL_AUTH] <user name>
```

deluser

deluser deletes a SecurePlatform administrator.

Syntax

```
deluser <user name>
```

showusers

showusers displays all SecurePlatform administrators.

Syntax

```
showusers
```
**lockout**

Lock out a SecurePlatform administrator.

**Syntax**

```
lockout enable <attempts> <lock_period>
lockout disable
lockout show
```

**Parameters**

**Table 4-37  lockout Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable attempts</td>
<td>Activate lockout after a specified number of unsuccessful attempts to login, and lock the account for lock_period minutes.</td>
</tr>
<tr>
<td>lock_period</td>
<td></td>
</tr>
<tr>
<td>disable</td>
<td>Disable the lockout feature.</td>
</tr>
<tr>
<td>show</td>
<td>Display the current settings of the lockout feature.</td>
</tr>
</tbody>
</table>

**unlockuser**

Unlock a locked administrator (see “lockout” on page 114).

**Syntax**

```
unlockuser <username>
```

**checkuserlock**

Display the lockout status of a SecurePlatform administrator (whether or not the administrator is locked out).

**Syntax**

```
checkuserlock <username>
```
SNMP Support

In This Section

Configuring the SNMP Agent ... page 115
Configuring SNMP Traps ... page 116

SNMP support is fully integrated in SecurePlatform:

- Net-SNMP Support for full OS-MIB-II.
- Monitoring of Check Point Status Information (AMON) through SNMP.
- SNMP V.2 and V.3 Support.

Configuring the SNMP Agent

For basic SNMP configuration use the `snmp` command in the restricted shell, as follows:

```shell
snmp service enable [<portnumber>]
snmp service stat
snmp service disable
snmp user add noauthuser <username> [oidbase <OID>]
snmp user add authuser <username> pass <passphrase> [priv <privacyphrase>] [oidbase <OID>]
snmp user del [<username>]
snmp user show [<username>]
```
Configuring SNMP Traps

Parameters

Table 4-38  snmp Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp service enable</td>
<td>starts SNMP agent daemon listening on the specified UDP port.</td>
</tr>
<tr>
<td>snmp service disable</td>
<td>stops the SNMP agent daemon.</td>
</tr>
<tr>
<td>snmp service stat</td>
<td>displays service status.</td>
</tr>
<tr>
<td>snmp user</td>
<td>adds an SNMP v3 user to the agent. Authentication and encryption passwords can be specified for the user. Additionally, the user’s access can be restricted to the specified OID sub-tree.</td>
</tr>
<tr>
<td>snmp user del</td>
<td>deletes a user. SNMP v1 and v2 users can also be deleted using this command.</td>
</tr>
<tr>
<td>snmp user show</td>
<td>displays a list of existing users.</td>
</tr>
<tr>
<td>snmp user show [&lt;username&gt;]</td>
<td>displays the specified user's (or all users') details: access level information and OID subtree restriction.</td>
</tr>
</tbody>
</table>

Configuring SNMP Traps

SNMP traps can be sent using the snmptrap command (in expert mode only).

snmpd.conf file

In addition, SNMP traps can be configured in the /etc/snmp/snmpd.conf file. snmpd.conf is the configuration file which defines how the Net-SNMP SNMP-agent operates. This file is not required for the agent to operate and respond to requests.

Important snmpd.conf directives are described below.

authtrapenable NUMBER

Setting authtrapenable to 1 enables the generation of authentication failure traps. The default value is disabled, 2. Ordinarily the corresponding object (snmpEnableAuthenTraps.0) is read-write, but setting its value makes the object read-only. Further attempts to set the value of the object will result in a notWritable error response.
**trapcommunity STRING**

`trapcommunity STRING` defines the default community string to be used when sending traps. This command must be used before using any of the following three commands, that use the community string.

- `trapsink HOST [COMMUNITY [PORT]]`
- `trap2sink HOST [COMMUNITY [PORT]]`
- `informsink HOST [COMMUNITY [PORT]]`

These commands designate hosts to receive traps (and/or inform notifications). The daemon sends a Cold Start trap, when it starts up. If enabled, it also sends traps on authentication failures. Multiple `trapsink`, `trap2sink` and `informsink` lines may be specified to specify multiple destinations. Use `trap2sink` to send SNMPv2 traps, and `informsink` to send inform notifications.

If `COMMUNITY` is not specified, the string from a preceding `trapcommunity` directive will be used.

If `PORT` is not specified, the well-known SNMP trap port (162) will be used.

**trapsess [SNMPCMD_ARGS] HOST**

`trapsess [SNMPCMD_ARGS] HOST` is a more generic trap configuration token, that allows any type of trap destination to be specified with any version of SNMP. See the `snmpcmd(1)` manual page for further details on the arguments that can be passed as `SNMPCMD_ARGS`.

In addition to the arguments listed there, the special argument `-Ci` specifies that inform notifications are to be used instead of unacknowledged traps. This requires that you specify a version number of v2c or v3.

**agentSecName NAME**

The DISMAN-EVENT-MIB support requires a valid user name for which to scan your agent.

This can either be specified using the `agentSecName` token, or by explicitly listing one on the “monitor” lines described below using the `-u` switch. In either case, a “rouser” line (or equivalent access control settings) must be specified with the same security name.
Example

agentSecName internal
rouser internal

**monitor [OPTIONS] NAME EXPRESSION**

This directive instructs the agent to monitor itself for problems, based on EXPRESSION. EXPRESSION is a simple expression based on an oid, a comparison operator (!=, ==, <, <=, >, >=) and an integer value (see the examples below).

NAME is an arbitrary name of your choosing, for administrative purposes only.

OPTIONS include the following possibilities:

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-r FREQUENCY</td>
<td>Monitors the given expression every FREQUENCY seconds. The default is 600 (10 minutes).</td>
</tr>
<tr>
<td>-u SECNAME</td>
<td>Uses the SECNAME security name for scanning the local host. Specifically, this SECNAME must then be given access control rights, via something like the “rouser” snmpd.conf token for this expression to be valid at all. If not specified, it uses the default security name, specified by the agent secname snmpd.conf token. Either the -u flag or a valid agentsecname token must be specified (and that name must be given proper access control rights via a “rouser” token).</td>
</tr>
<tr>
<td>-o OID</td>
<td>Specifies additional object values to be delivered with the resulting trap, in addition to the normal trap objects. See the examples below for more details.</td>
</tr>
</tbody>
</table>

The following example configuration checks the hrSWRunPerfTable table (listing running processes) for any process which is consuming more than 10Mb of memory. It performs this check every 600 seconds (the default). For every process found, exceeding the limit, it will send out exactly one notification. In addition to the normal hrSWRunPerfMem oid and value, sent in the trap, the hrSWRunName object will also be sent.

The hrSWRunName object actually occurs in a different table, but since the indexes to the two tables are the same this has no effect.
rouser admin

monitor -u me -o sysUpTime.0 -o hrSWRunName "high process memory"
hrSWRunPerfMem > 10000

The above line would produce a trap which is formatted by snmptrapd, as follows:

2002-04-05 13:33:53 localhost.localdomain [udp:127.0.0.1:32931]:
sysUpTimeInstance = Timeticks: (1629) 0:00:16.29
snmpTrapOID.0 = OID: mteTriggerFired mteHotTrigger = high process memory
mteHotTargetName = mteHotContextName = mteHotOID = OID: hrSWRunPerfMem.1968
mteHotValue = 28564 hrSWRunName.1968 = "fw"

This shows the fw process using 28Mb of resident memory.

**defaultMonitors yes**

By default, the agent and the DISMAN-EVENT-MIB support do nothing, until configured. Typically, users wish to watch a number of tables within the UCD-SNMP-MIB, which are designed specifically for reporting problems.

If the defaultMonitors yes line is present in the snmpd.conf file (which must be accompanied by an appropriate agentSecName line and a rouser line), the following monitoring conditions will be installed:

monitor -o prNames -o prErrMessage "process table" prErrorFlag != 0
monitor -o memErrorName -o memSwapErrorMsg "memory" memSwapError != 0
monitor -o extNames -o extOutput "extTable" extResult != 0
monitor -o dskPath -o dskErrorMsg "dskTable" dskErrorFlag != 0
monitor -o laNames -o laErrMsg "laTable" laErrorFlag != 0
monitor -o fileName -o fileErrorMsg "fileTable" fileErrorFlag != 0
Check Point Dynamic Routing

In This Section

- Supported Features  page 120
- Command Line Interface  page 123

Check Point now supports Dynamic Routing (Unicast and Multicast) protocols, as an integral part of SecurePlatform. Configuration is done via an "Industry-Standard" Command-Line-Interface that is integrated into the SecurePlatform Shell. Other administration tasks, such as log viewing, are performed via the standard SecurePlatform tools. This chapter discusses the integration of SecurePlatform and Dynamic Routing.

Supported Features

In This Section:

- Supported Protocols  page 120
- Enabling and Disabling Dynamic Routing Support  page 121
- Tracing and Logging Options  page 121
- Status Monitoring via SNMP  page 122
- Backup and Restore  page 122

This section discusses several key features supported by Check Point Dynamic Routing.

Supported Protocols

The following protocols are supported by Check Point Dynamic Routing:

- Unicast
  - RIP-1
  - RIP-2
  - OSPF
  - BGP
- Multicast
Supported Features

- PIM-DM
- PIM-SM
- IGMP

**Enabling and Disabling Dynamic Routing Support**

The following CLI command is essential for use of Check Point Dynamic Routing:

- **router**: Configures Check Point Dynamic Routing.

The `router` command syntax and parameter description are provided below:

```
router [enable | config | disable]
```

**Syntax**

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable Dynamic Routing</td>
</tr>
<tr>
<td>config</td>
<td>invokes the Dynamic Routing CLI (For more information, refer to “Command Line Interface” on page 123.)</td>
</tr>
<tr>
<td>disable</td>
<td>disable Dynamic Routing</td>
</tr>
</tbody>
</table>

The Check Point Dynamic Routing state is preserved during the reboot operation, for example if it was `Enabled` before the reboot, it remains `Enabled` after the reboot.

**Note** - The Dynamic Routing configuration, however, is not preserved during the reboot operation. Only the last configuration, saved via the CLI, is preserved during the reboot.

**Tracing and Logging Options**

Check Point Dynamic Routing's tracing options can be configured at many levels. Tracing options include the file specifications and global and protocol-specific tracing options. The trace files can later be viewed by using the Log Switch mechanism.
The Dynamic Routing logging messages are stored in 'routing_messages' and can be viewed using the standard SecurePlatform logging mechanism.

For more detailed information, refer to “log” on page 81.

**Status Monitoring via SNMP**

Check Point Dynamic Routing supports SNMP, via the RFC 1227 SMUX interface. It is enabled by default. Use a standard SNMP client to retrieve the Dynamic Routing status information, via SNMP.

Only SNMP version 1 is supported, and all MIB variables are read-only. For more detailed information, refer to “SNMP Support” on page 115.

**Backup and Restore**

The SecurePlatform mechanism stores and restores the Dynamic Routing configuration, as well. This is also true, if you use the snapshot and revert commands.

**Note** - The Dynamic Routing configuration is stored as part of the system configuration. For more detailed information, refer to “Backup and Restore” on page 63.
Command Line Interface

In This Section:

Overview ................................................. page 123
Command Line Editing and Completion .......... page 123
Context-Sensitive Help ................................. page 123
Command History ....................................... page 123
Disabling/Enabling CLI Tracing .................... page 124

Overview
Check Point Dynamic Routing utilizes industry standard commands for configuration. The basic features of the CLI include the following:

• Command line editing and completion
• Context-sensitive help
• Command history
• Disabling/Enabling CLI Tracing

Command Line Editing and Completion
At any point when typing a command line, you can hit the Tab key to either complete the current command, or show a list of possible completions.

Context-Sensitive Help
Type "?" immediately after any command to obtain context-sensitive help about the last command that you typed. Type "?" after any set of commands to obtain a list of options that can be used in the command.

Command History
All commands entered during a CLI session are saved in a command history. The history can be toggled on and off.
Disabling/Enabling CLI Tracing

The CLI provides a flexible tracing mechanism. Events to be traced are divided into several classes, each of which can be traced individually. Classes can be traced to any or to all three of the following locations: the terminal, a file, or the underlying system's tracing system (i.e., syslog).
SecurePlatform Boot Loader

In This Section

- Booting in Maintenance Mode page 125
- Customizing the Boot Process page 126
- Snapshot Image Management page 126

Each time the SecurePlatform machine is booted the boot loader screen is displayed. The boot loader offers a selection of boot options and allows customization of the boot process, including the possibility to boot from a snapshot image (if one is present).

By default, if there is no user intervention, the boot loader will select the boot option selected last time (or the default option, if no option was ever selected).

Booting in maintenance mode and customizing the boot process require a password. The password is the system’s Expert mode password.

**Tip** - The first time that you switch to Expert mode you will be asked to select a password. Until then, it is the same as the Standard password, i.e. you need to enter the first replacement password that you used when logging in as the admin user. Any sequential admin password change will not update the expert password that you must enter at the first-time expert user password change.

**Warning** - Changing the boot options and customizing the boot process requires a high level of understanding of system administration and Linux.

**Booting in Maintenance Mode**

Maintenance Mode should be used in rare system emergencies, such as when there is a problem rebooting the system, or the Standard admin password is lost. To reboot in this mode, position the selection bar on “SecurePlatform with Application Intelligence [Maintenance Mode]” and click **Enter**. You will be asked to enter a password.

Selecting the **Maintenance Mode** boot option will boot your SecurePlatform in a special mode, known on Unix systems as “single-user mode”. In this mode, your computer boots to runlevel 1. Your local file systems will be mounted, but your network will not be activated. You will have a usable system maintenance shell.
Customizing the Boot Process

To customize the boot process, click **p** in order to enter a password and unlock the next set of features. The password is the Expert password that you set for your system. The following options are available:

- Click **e** to edit any of the boot options (position the selection bar on the relevant boot option).
- Click **c** to perform root level system operations.

Snapshot Image Management

At boot time, the user is given the option of switching to any of the available snapshots. For more information, see “Snapshot Image Management” on page 78.
Chapter 5

SecurePlatform Pro
Advanced Routing Suite

In This Chapter

Introduction  page 128
Check Point Advanced Routing Suite  page 129
SecurePlatform Pro integrates support for dynamic routing. For more information regarding SecurePlatform Pro see: “SecurePlatform Pro” on page 18

**Note** - Advanced Routing Suite does not allow the configuration of static routes. Use standard SecurePlatform tools to maintain static routes
Check Point Advanced Routing Suite

In This Section

Supported Features  page 129
Command Line Interface  page 133

Check Point now supports Dynamic Routing (Unicast and Multicast) protocols, as an integral part of SecurePlatform Pro. Configuration is done via an “Industry-Standard” Command-Line-Interface that is integrated into the SecurePlatform Shell. Other administration tasks, such as log viewing, are performed via the standard SecurePlatform tools. This chapter discusses the integration of SecurePlatform and Dynamic Routing.

The Advanced routing suite is also supported with ClusterXL. For more information, see the CheckPoint R65 ClusterXL Administration Guide.

Supported Features

In This Section:

Dynamic Routing  page 129
Supported Protocols  page 131
Enabling and Disabling Dynamic Routing Support  page 131
Configuring Dynamic Routing Protocols  page 132
Tracing and Logging Options  page 132
Backup and Restore  page 132

Dynamic Routing

Dynamic routing in Provider-1/SiteManager-1NGX is implemented in the following way:

• Each Virtual Device (Virtual System or Virtual Router) has its own routing daemon.
• Each Virtual Device on the VSX gateway has to be configured separately.
• For a VSX cluster, each Virtual Device on the cluster members has to be configured separately. This means if you have two physical machines combined to a single cluster, the Virtual Devices on each machine have to be configured independently.

**To enable dynamic routing**

1. Open a Secure Shell connection to the VSX gateway. You are automatically in the default (VSX:0) context. Run `fw vsx stat -v` to view the Virtual Systems and their IDs:

   ```
   [Expert@vsx57:vs0]# vsx stat -v
   VSX Gateway Status
   ==============
   Name: vsx57
   Management IP Address: 172.23.3.57
   Security Policy: Standard
   Installed at: 1May2005 15:37:36
   SIC Status: Trust
   
   Number of Virtual Systems allowed by license: 100
   Virtual Systems [active / configured]: 3 / 3
   Virtual Routers and Switches [active / configured]: 0 / 0
   
   Virtual Devices Status
   ================
   
<table>
<thead>
<tr>
<th>ID</th>
<th>Type &amp; Name</th>
<th>Security Policy</th>
<th>Installed at</th>
<th>SIC Stat</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>S vsx57_vs1</td>
<td>Standard</td>
<td>1May2005 15:37</td>
<td>Trust</td>
</tr>
<tr>
<td>2</td>
<td>S vsx57_vs2</td>
<td>Standard</td>
<td>1May2005 15:37</td>
<td>Trust</td>
</tr>
<tr>
<td>3</td>
<td>S vsx57_vs3</td>
<td>Standard</td>
<td>1May2005 15:37</td>
<td>Trust</td>
</tr>
</tbody>
</table>
   
   Type: S - Virtual System, B - Virtual System in Bridge mode, R - Virtual Router, W - Virtual Switch.
   ```

2. Run `drouter` to either enable or disable the routing daemon on the Virtual Device.

   • `drouter enable <vs_id>` enables and starts dynamic routing for the Virtual Device
   • `drouter disable <vs_id>` stops and disables dynamic routing for the Virtual Device
   • `drouter start <vs_id>` starts dynamic routing for the Virtual Device
   • `drouter stop <vs_id>` stops dynamic routing for the Virtual Device
To Configure Dynamic Routing

1. Open the Command Line Interface to the dynamic routing application.
   
   - `router` starts the Advanced Routing Suite Command Line Interface.
   - `vrf-connect` is a command that determines for which Virtual Device the dynamic routing configuration applies. For example:

   ```
   [Expert@vsx57:vs0]# router
   >vrf-connect 2
   localhost.localdomain-VRF-2>enable
   localhost.localdomain-VRF-2#
   ```

Backward Compatibility Support

From current release you create and manage:

- VSX 2.0.1 objects
- VSX_NG_AI objects

Supported Protocols

The following protocols are supported by Check Point Dynamic Routing:

- Unicast
  - RIP-1
  - RIP-2
  - OSPF
  - BGP
- Multicast
  - PIM-DM
  - PIM-SM
  - IGMP

Enabling and Disabling Dynamic Routing Support

Enabling and disabling the Advanced Routing Suite is performed through cpconfig by selecting the relevant option.
Configuring Dynamic Routing Protocols

The following CLI command is essential for use of Check Point Dynamic Routing:

- **router**: Configures Check Point Dynamic Routing.

Tracing and Logging Options

Check Point Dynamic Routing's tracing options can be configured at many levels. Tracing options include the file specifications and global and protocol-specific tracing options. The trace files can later be viewed by using the Log Switch mechanism.

The Dynamic Routing logging messages are stored in 'routing_messages' and can be viewed using the standard SecurePlatform logging mechanism.

Backup and Restore

The SecurePlatform mechanism stores and restores the Dynamic Routing configuration, as well.

**Note** - The Dynamic Routing configuration is stored as part of the system configuration.
Command Line Interface

In This Section:

- Overview page 133
- Command Line Editing and Completion page 133
- Context-Sensitive Help page 133
- Command History page 133
- Disabling/Enabling CLI Tracing page 134

Overview

Check Point Dynamic Routing utilizes industry standard commands for configuration. The basic features of the CLI include the following:

- Command line editing and completion
- Context-sensitive help
- Command history
- Disabling/Enabling CLI Tracing

Command Line Editing and Completion

At any point when typing a command line, you can hit the Tab key to either complete the current command, or show a list of possible completions.

Context-Sensitive Help

Type "?" immediately after any command to obtain context-sensitive help about the last command that you typed. Type "?" after any set of commands to obtain a list of options that can be used in the command.

Command History

All commands entered during a CLI session are saved in a command history. The history can be toggled on and off.
Disabling/Enabling CLI Tracing

The CLI provides a flexible tracing mechanism. Events to be traced are divided into several classes, each of which can be traced individually. Classes can be traced to any or to all three of the following locations: the terminal, a file, or the underlying system's tracing system (i.e., syslog).
Appendix A

Installation on Computers without Floppy or CDROM Drives

In This Appendix

General Procedure  page 136  
Client Setup  page 136  
Server Setup  page 137  

You must set up a server for network installation, and perform some client setup on the host, on which SecurePlatform is being installed.

Note - It is not recommended to use a system that was installed in this manner in a production environment. It should only be used as an Installation Server for SecurePlatform.
General Procedure

The network installation is performed as follows:

1. The client boots from the network, using the PXE network loader.
2. The client sends a broadcast request, using the BOOTP protocol.
3. The server responds to the client, by providing the client's assigned IP address and a filename (pxelinux.0 by default), to which to download the PXE boot loader.
4. The client downloads the PXE Boot Loader, using TFTP, and executes it.
5. The PXE boot loader downloads a PXE configuration file from the server, containing the names of the kernel and the ramdisk that the client requires.
6. The PXE boot loader downloads the kernel and the ramdisk.
7. The kernel is run, using ramdisk as its environment.
8. The Installer is executed.
9. At this point the installation can be configured to load files from the FTP server.

The client's requirements are minimal. Only PXE is required.

The server needs a little more configuring. You must install a DHCP daemon, a TFTP daemon, the PXE boot loader, the kernel and the ramdisk.

Client Setup

On the client machine, enable the network boot, using PXE, from the BIOS setup. (It sometimes appears as DHCP.) The procedure differs from machine to machine. Consult specific machine documentation, if necessary.
Server Setup

In This Section

- Required Packages
- DHCP Daemon Setup
- TFTP and FTP Daemon Setup
- Hosting Installation Files

The following setup details and instructions apply to a server running SecurePlatform, as its operating system. Setup on a server running a different OS may differ slightly.

Required Packages

The following packages are required for server setup:

- DHCP daemon (located on the Checkpoint CDROM and installed, by default, on SecurePlatform)
- Xinetd (/SecurePlatform/RPMS/xinetd-2.3.11-4cp.i386.rpm on the Checkpoint CDROM)
- TFTP daemon (/SecurePlatform/RPMS/tftp-server-0.32-5cp.i386.rpm)
- FTP server (/SecurePlatform/RPMS/ftpd-0.3.3-118.4cp.i386.rpm)
- TCP-Wrappers package (/SecurePlatform/RPMS/tcp_wrappers-7.6-34.4cp.i386.rpm)
- Kernel (can be found on the SecurePlatform CD at /SecurePlatform/kernel)
- Ramdisk (can be found on the SecurePlatform CD at /SecurePlatform/ramdisk-pxe)

Note - To access files on Check Point CDROM, insert the CDROM into the CDROM drive and enter the command: # mount/mnt/cdrom
**PXELINUX Configuration Files**

`/SecurePlatform/RPMS/tftp-server-0.32-4cp.i386.rpm` includes a default configuration file (located under `/tftpboot/pxelinux.cfg`) that will serve the kernel and ramdisk to any host. Because more than one system may be booted from the same server, the configuration file name depends on the IP address of the booting machine.

PXELINUX will search for its config file on the boot server in the following way:

1. PXELINUX will search for its config file, using its own IP address, in upper case hexadecimal, e.g. 192.0.2.91 -> C000025B.
2. If that file is not found, PXELINUX will remove one hex digit and try again. Ultimately, PXELINUX will try looking for a file named default (in lower case).

As an example, for 192.0.2.91, PXELINUX will try C000025B, C000025, C00002, C0000, C000, C00, C0, C, and default, in that order.

Assuming the kernel and ramdisk files are named `kernel` and `ramdisk`, respectively, a default configuration file, which will serve these to all clients, will look like this:

```plaintext
default bootnet
label bootnet
kernel kernel
append initrd=ramdisk lang= devfs=nomount \
ramdisk_size=24336 console=tty0
```

**DHCP Daemon Setup**

To setup the DHCP Daemon, perform the following procedure:

1. Enter the `sysconfig` utility and enable the DHCP server.
2. Edit the daemon's configuration file, found at /etc/dhcpd.conf. The configuration file should include a subnet declaration for each subnet, the DHCP server is connected to. In addition, configuration should include a host declaration, for each host that will use this server for remote installation. A sample configuration file follows:

```plaintext
subnet 192.92.93.0 netmask 255.255.255.0 {
  host foo {
    # The client's MAC address
    # The IP address that will be assigned to the
    # client by this server
    fixed-address 192.92.93.32;
    # The file to upload
    filename "/pxelinux.0";
  }
}
```

### TFTP and FTP Daemon Setup

To setup the TFTP and FTP Daemons, perform the following procedure:

1. Install `/SecurePlatform/RPMS/tcp_wrappers-7.6-34.4cp.i386.rpm` (The TCP wrappers package)
2. Install `/SecurePlatform/RPMS/xinetd-2.3.11-4cp.i386.rpm`. (The xinetd package is a prerequisite for the tftp-server and ftput.)
3. Install the TFTP Daemon RPM:
   ```bash
   # rpm -i /SecurePlatform/RPMS/tftp-server-0.32-5cp.i386.rpm
   ```
4. Install the FTP Daemon RPM:
   ```bash
   # rpm -i /SecurePlatform/RPMS/ftpd-0.3.3-118.4cp.i386.rpm
   ```
5. Force xinetd to reread its configuration:
   ```bash
   # service xinetd restart
   ```
Hosting Installation Files

An FTP server installed on SecurePlatform will be used to host the installation files. During the installation process, you will be asked to supply the IP of the installation server, the credentials on that server, and the path to the installation packages. Supply the IP of the SecurePlatform installation server, the Administrator’s credentials, and the path to the SecurePlatform packages.

You can also use different FTP servers, or HTTP servers, to host SecurePlatform installation files.
THIRD PARTY TRADEMARKS AND COPYRIGHTS

Entrust is a registered trademark of Entrust Technologies, Inc. in the United States and other countries. Entrust's logos and Entrust product and service names are also trademarks of Entrust Technologies, Inc. Entrust Technologies Limited is a wholly owned subsidiary of Entrust Technologies, Inc. FireWall-1 and SecuRemote incorporate certificate management technology from Entrust.

Verisign is a trademark of Verisign Inc.

The following statements refer to those portions of the software copyrighted by University of Michigan. Portions of the software copyright © 1992-1996 Regents of the University of Michigan. All rights reserved. Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty. Copyright © Sax Software (terminal emulation only).

The following statements refer to those portions of the software copyrighted by Carnegie Mellon University.

Copyright 1997 by Carnegie Mellon University. All Rights Reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The following statements refer to those portions of the software copyrighted by The Open Group.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE OPEN GROUP BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

The following statements refer to those portions of the software copyrighted by The OpenSSL Project. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The following statements refer to those portions of the software copyrighted by Eric Young. THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. Copyright © 1998 The Open Group.
The following statements refer to those portions of the software copyrighted by Jean-loup Gailly and Mark Adler Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler. This software is provided “as-is”, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

The following statements refer to those portions of the software copyrighted by the GNU General Public License. This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

The following statements refer to those portions of the software copyrighted by Thai Open Source Software Center Ltd and Clark Cooper Copyright (c) 2001, 2002 Expat maintainers. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.


Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

The curl license

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2004, Daniel Stenberg, <daniel@haxx.se>. All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose
with or without fee is hereby granted, provided that the above copyright
notice and this permission notice appear in all copies.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

The PHP License, version 3.0

Copyright (c) 1999 - 2004 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.

4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo".

5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes PHP, freely available from <http://www.php.net>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the PHP Group. The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project, please see <http://www.php.net>. This product includes the Zend Engine, freely available at <http://www.zend.com>.

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Copyright © 2003, 2004 NextHop Technologies, Inc. All rights reserved.

Confidential Copyright Notice

Except as stated herein, none of the material provided as a part of this document may be copied, reproduced, distributed, republished, downloaded, displayed, posted or transmitted in any form or by any means, including, but not limited to, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of NextHop Technologies, Inc. Permission is granted to display, copy, distribute and download the materials in this document for personal, non-commercial use only, provided you do not modify the materials and that you retain all copy-right and other proprietary notices contained in the materials unless otherwise stated. No material contained in this document may be "mirrored" on any server without written permission of NextHop. Any unauthorized use of any material contained in this document may violate copyright laws, trademark laws, the laws of privacy and publicity, and communications regulations and statutes. Permission terminates automatically if any of these terms or conditions are breached. Upon termination, any downloaded and printed materials must be immediately destroyed.

Trademark Notice

The trademarks, service marks, and logos (the "Trademarks") used and displayed in this document are registered and unregistered Trademarks of NextHop in the US and/or other countries. The names of actual companies and products mentioned herein may be Trademarks of their respective owners. Nothing in this document should be construed as granting, by implication, estoppel, or otherwise, any license or right to use any Trademark displayed in the document. The owners aggressively enforce their intellectual property rights to the fullest extent of the law. The Trademarks may not be used in any way, including in advertising or publicity pertaining to distribution of, or access to, materials in this document, including use, without prior, written permission. Use of Trademarks as a "hot" link to any website is prohibited unless establishment of such a link is approved in advance in writing. Any questions concerning the use of these Trademarks should be referred to NextHop at U.S. +1 734 222 1600.

U.S. Government Restricted Rights

The material in document is provided with "RESTRICTED RIGHTS." Software and accompanying documentation are provided to the U.S. government ("Government") in a transaction subject to the Federal Acquisition Regulations with Restricted Rights. The Government's rights to use, modify, reproduce, release, perform, display or disclose are restricted by paragraph (b)(3) of the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation clause at DFAR 252.227-7014 (Jun 1995), and the other restrictions and terms in paragraph (g)(3)(i) of Rights in Data-General clause at FAR 52.227-14, Alternative III (Jun 87) and paragraph (c)(2) of the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19 (Jun 1987).

Use of the material in this document by the Government constitutes acknowledgment of NextHop's proprietary rights in them, or that of the original creator. The Contractor/Licensor is NextHop located at 1911 Landings Drive, Mountain View, California 94043. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in applicable laws and regulations.

Disclaimer Warranty Disclaimer Warranty Disclaimer Warranty Disclaimer Warranty

THE MATERIAL IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND EITHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT POSSIBLE PURSUANT TO THE APPLICABLE LAW, NEXTHOP DISCLAIMS ALL WARRANTIES,

EXpressed or IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OR OTHER VIOLATION OF RIGHTS. NEITHER NEXTHOP NOR ANY OTHER PROVIDER OR DEVELOPER OF MATERIAL CONTAINED IN THIS DOCUMENT WARRANTS OR MAKES ANY REPRESENTATIONS REGARDING THE USE, VALIDITY, ACCURACY, OR RELIABILITY OF, OR THE RESULTS OF THE USE OF, OR OTHERWISE RESPECTING, THE MATERIAL IN THIS DOCUMENT.

Limitation of Liability
UNDER NO CIRCUMSTANCES SHALL NEXTHOP BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOSS OF DATA OR PROFIT, ARISING OUT OF THE USE, OR THE INABILITY TO USE, THE MATERIAL IN THIS DOCUMENT, EVEN IF NEXTHOP OR A NEXTHOP AUTHORIZED REPRESENTATIVE HAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IF YOUR USE OF MATERIAL FROM THIS DOCUMENT RESULTS IN THE NEED FOR SERVICING, REPAIR OR CORRECTION OF EQUIPMENT OR DATA, YOU ASSUME ANY COSTS THEREOF. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT FULLY APPLY TO YOU.

Copyright © ComponentOne, LLC 1991-2002. All Rights Reserved.

BIND: ISC Bind (Copyright (c) 2004 by Internet Systems Consortium, Inc. ("ISC"))

Copyright 1997-2001, Theo de Raadt: the OpenBSD 2.9 Release

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language. Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service, Cambridge, England. Phone:
+44 1223 334714.

Copyright (c) 1997-2004 University of Cambridge All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Eventia Reporter includes software whose copyright is owned by, or licensed from, MySQL AB.
# Index

## A
- administrator lockout 114
- AMON 89

## B
- backup 63
- backups of system settings 63
- BIOS 25
- boot loader 125
- boot process customization 126
- boot time
  - restoring from snapshot 78, 126
- booting in maintenance mode 125

## C
- Cluster XL 90
- ClusterXL 84, 85, 93
- command
  - addarp 103
  - adduser 60
  - arp 102
  - audit clear 71
  - audit setlines 71
  - audit show 71
  - checkuserlock 114
  - cpconfig 83
  - cphaprobt 91
  - cphastart start 90
  - Cphastop 91
  - cpiinfo 88
  - cplic 90
  - cpshared_ver 90
  - cpstart 85
  - cpstat 89
  - cstop 85
- date 68
- delarp 103
- deluser 60, 113
- diag 81
- domainname 110
- exit 66
- expert 66
- fips on 62
- fw ctl 86
- fw fetch targets 86
- fw fetchlogs 86
- fw kill 86
- fw lichosts 86
- fw log 86
- fw logswitch 86
- fw lslogs 86
- fw mergefiles 86
- fw monitor 86
- fw putkey 86
- fw repairlog 86
- fw sam 86
- fw tab 86
- fw ver 86
- fwm 93
- help 67
- ifconfig 105
- lockout 62
- log 82
- log limit 82
- log list 82
- log show 82
- log unlimited 82
- netstat 100
- ntp 69
- ntpstart 70
- ntpstop 69
- passwd 67
- patch add 74
- patch list 74
- ping 96
- reboot 73
- route 108
- SDSUtil 96
- showusers 113
- shutdown 77
- sysconfig 111
- time 68
- timezone 69
- traceroute 98
- unlockuser 114
- vconfig 108
- ver 77
- vwp 95
- command line editing keys 65
- commands
  - adduser 113
  - hostname 109, 111
  - hosts 105
  - lockout 114
  - LSMcli 96, 113
  - LSMenabler 96
- configuration changes 78
- command
  - dns 110
  - vconfig 108
- critical process 91

## D
- Dynamic Routing
  - Backup and Restore 122, 132
  - CLI Commands 123, 133
  - Command History 123, 133
  - Command Line
    - Completion 123, 133
    - Interface 123, 133
  - Context-Sensitive Help 123, 133
  - Disabling/Enabling CLI
    - Tracing 124, 134
  - Interface to SNMP
    - SMUX 122
  - Reboot 122, 132
  - Supported Protocols 120, 131
  - Tracing Options 121, 132
E

Expert Mode 59

F

FIPS 140-2 32, 62
first reboot 56
fw command
  fw ctl 86
  fw fetch targets 86
  fw fetchlogs 86
  fw kill 86
  fw lichosts 86
  fw lslogs 86
  fw monitor 86
  fw putkey 86
  fw repairlog 86
  fw sam 86
  fw tab 86
  fw ver 86

H

--help 64
High Availability, see ClusterXL
HTTPS web server
  configuring port 111
  disabling 111, 112, 121
  enabling 111
  https_port 111

I

installation
  before you begin 20
  without CD-ROM 20
integrity check 62
interactive shell
  CP commands 83
  date and time commands 67
  network config
    commands 102, 112
    network diagnostics
      commands 96
    system commands 70
  system diagnostic
    commands 80

CP/SmartDashboard 31

syslog 60

L

lockout
  administrator accounts 62
  lockout administrator 114
login 56
LSM 96

N

Network Configuration Hosts
  commands 105
NTP 44

P

password complexity 60
permissions
  expert mode 59
  standard 59
process
  critical 91

R

restore 63
running sysconfig 29

S

SCP 63
serial console 20
SmartUpdate 62
snapshots 78
SNMP 115
sysconfig
  configuration options 29, 30
  CP products
    configuration 29, 31

T

TFTP 63, 78

U

Upgrade 50

V

VGA display 20
vpn command
  vpn ver 95