© 2011 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page (http://www.checkpoint.com/copyright.html) for a list of our trademarks.

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

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

Latest Documentation
The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=12276
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 July 2011</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

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

Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on SecurePlatform R75.20 Administration Guide).
Contents

Important Information .............................................................................................................. 3
Introduction to SecurePlatform .............................................................................................. 7
Preparing to Install SecurePlatform ...................................................................................... 8
  SecurePlatform Hardware Requirements ............................................................................ 8
  Preparing the SecurePlatform Machine ........................................................................... 8
  Hardware Compatibility Testing Tool ................................................................................ 8
  Before Using the Tool ......................................................................................................... 9
  Obtaining the Hardware Compatibility Testing Tool ......................................................... 9
  Running the Hardware Compatibility Testing Tool ............................................................ 9
  Using the Hardware Compatibility Testing Tool ............................................................... 9
  BIOS Security Configuration Recommendations ........................................................... 10
Installing Products on SecurePlatform .................................................................................. 10
Installing SecurePlatform on Computers without Optical Drives .................................... 11
  General Procedure ............................................................................................................ 11
  Client Setup ..................................................................................................................... 11
  Server Setup ..................................................................................................................... 12
  Required Packages ........................................................................................................... 12
  DHCP Daemon Setup ....................................................................................................... 12
  TFTP and FTP Daemon Setup ......................................................................................... 13
  Hosting Installation Files ................................................................................................. 13
Configuration Using the Web Interface .................................................................................... 14
  First Time Setup Using the Web Interface ......................................................................... 14
  Connecting to the Web Interface ...................................................................................... 14
  Changing the Settings of the SecurePlatform Portal ....................................................... 15
  Obtaining and Installing a Trusted Server Certificate ...................................................... 15
  Viewing the Certificate .................................................................................................... 17
Status ................................................................................................................................... 17
  Device Status ................................................................................................................... 17
Network ................................................................................................................................ 17
  Network Connections ...................................................................................................... 17
  Routing Table .................................................................................................................. 18
  DNS Servers ..................................................................................................................... 18
  Host and Domain Name ................................................................................................. 19
  Local Hosts Configuration ............................................................................................... 19
Device ................................................................................................................................... 19
  Device Control ................................................................................................................ 19
  device Date and Time Setup ............................................................................................ 19
Backup .................................................................................................................................. 20
Upgrade ............................................................................................................................... 22
Device Administrators ......................................................................................................... 22
Web and SSH Clients ........................................................................................................... 22
Administrator Security Settings ........................................................................................... 22
Product Configuration ......................................................................................................... 23
  Security Management Administrator ............................................................................... 23
  Security Management GUI Clients .................................................................................. 23
Certificate Authority ........................................................................................................... 23
Download SmartConsole Applications .............................................................................. 23
Licenses ............................................................................................................................... 24
Products ............................................................................................................................... 24
Performance Optimization ................................................................................................. 24
Configuration Using the Command Line ............................................................................... 25
  First Time Setup Using the Command Line ...................................................................... 25
Chapter 1

Introduction to SecurePlatform

Thank you for using SecurePlatform. This document describes how to prepare a hardware platform for SecurePlatform, and how to configure and administer SecurePlatform.

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.

The SecurePlatform DVD can be installed on any PC with an Intel x86 compatible architecture. 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 is distributed on a bootable DVD which includes Check Point's product suite, that includes software blades for firewall, VPN, and many others.

Chapter 2

Preparing to Install SecurePlatform

In This Chapter

- SecurePlatform Hardware Requirements 8
- Preparing the SecurePlatform Machine 8
- Hardware Compatibility Testing Tool 8
- BIOS Security Configuration Recommendations 10
- Installing Products on SecurePlatform 10

SecurePlatform Hardware Requirements


For details regarding SecurePlatform on specific hardware platforms, see the SecurePlatform Hardware Compatibility List (http://www.checkpoint.com/services/techsupport/hcl/).


Preparing the SecurePlatform Machine

SecurePlatform can be installed from an optical drive or from a network server.

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

- If the target computer has an optical 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 DVD, or if you wish to install using a remote file server, refer to the instructions in the R75.20 Installation and Upgrade Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12269).

⚠️ Important - 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

The Hardware Compatibility Testing Tool enables you to determine whether SecurePlatform is supported on a specific hardware platform.
The tool detects all hardware components on the platform, checks whether they are supported, and displays its conclusions.

It is possible to view detailed information on all the devices found on the machine. You can also save 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 Check Point Security Gateway, more than one controller is needed)

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

**Before Using the Tool**

Before selecting hardware to be used with SecurePlatform, you should refer to the Hardware Compatibility List ([http://www.checkpoint.com/products/supported_platforms/secureplatform.html](http://www.checkpoint.com/products/supported_platforms/secureplatform.html)), which lists Open Servers and Devices that are tested on a regular basis for compatibility by Check Point and are recommended for use with SecurePlatform.

**Obtaining the Hardware Compatibility Testing Tool**

The utility is available as an ISO image (hw.iso).

1. Download the Hardware Compatibility Testing Tool ([http://www.checkpoint.com/services/techsupport/hcl/testing_tool.html](http://www.checkpoint.com/services/techsupport/hcl/testing_tool.html)).
2. Burn the ISO image on a blank CD-R or on CD-RW media, using a CD-burning tool.

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

**Running the Hardware Compatibility Testing Tool**

Run the Hardware Compatibility Testing Tool by booting from the CD that contains it.

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

**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.

**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 the tool has finished analyzing the hardware, a summary page is displayed 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.

Installing Products on SecurePlatform

Chapter 3

Installing SecurePlatform on Computers without Optical Drives

To install SecurePlatform on computers without optical drives you must set up a server for network installation, and do 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.

In This Chapter

General Procedure 11
Client Setup 11
Server Setup 12

General Procedure

To perform the network installation:
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 requires the following items to be installed:
   - DHCP daemon
   - TFTP daemon
   - PXE boot loader
   - Kernel
   - 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

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 Check Point DVD and installed, by default, on SecurePlatform)
- Xinetd (/SecurePlatform/RPMS/xinetd-2.3.11-4cp.i386.rpm on the Check Point DVD)
- 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 DVD at /SecurePlatform/kernel)
- Ramdisk (can be found on the SecurePlatform DVD at /SecurePlatform/ramdisk-pxe)

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:

```
default bootnet
label bootnet
kernel kernel
append initrd=ramdisk lang= devfs=nomount \
ramdisk_size=80024 console=tt0
```

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 that is connected to the DHCP server.
   - The configuration should include a host declaration, for each host that will use this server for remote installation.

A sample configuration file follows:
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:
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 ftpd.)
3. Install the TFTP Daemon RPM:
   
4. Install the FTP Daemon RPM:
   
5. Force xinetd to reread its configuration:
   
Hosting Installation Files

The installation files are hosted on an FTP server installed on SecurePlatform. During the installation process, you are asked to provide the following information:

<table>
<thead>
<tr>
<th>Information Requested</th>
<th>Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP of the installation server</td>
<td>IP of the SecurePlatform installation server</td>
</tr>
<tr>
<td>Credentials on that server</td>
<td>Administrator's credentials</td>
</tr>
<tr>
<td>Path to the installation</td>
<td>Path to the SecurePlatform packages</td>
</tr>
</tbody>
</table>

You can also use different FTP servers, or HTTP servers, to host SecurePlatform installation files.
Chapter 4

Configuration Using the Web Interface

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

This section describes SecurePlatform's Web Interface. Most of the common operations can be done by using the Web Interface on the SecurePlatform Administration Portal.

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

In This Chapter

- First Time Setup Using the Web Interface
- Connecting to the Web Interface
- Status
- Network
- Device
- Product Configuration

First Time Setup Using the Web Interface

After the installation from the DVD is completed, and the computer has been rebooted, a first time setup using the First-Time Configuration Wizard 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

These settings can also be configured after completing the first time setup, using the SecurePlatform Web Interface

Connecting to the Web Interface

The initial configuration of SecurePlatform is performed using the First-Time Configuration Wizard. The SecurePlatform Web Interface lets you further configure SecurePlatform.

To connect to the SecurePlatform Administration Portal:

1. Initiate a connection from a browser to the administration IP address:
   - For appliances - https://<IP_address>:4434.
   - For open servers - https://<IP_address>
Note - Pop-ups must always be allowed on https://IP_address>.

The login page appears.

2. Login with the system administrator login name/password and click Login.
   (To log out of the Web Interface, click Close, in the top right of the page.)

Changing the Settings of the SecurePlatform Portal

Configure the settings of the SecurePlatform administration portal in SmartDashboard from the properties of the gateway > SecurePlatform Settings. From there you can configure:

- The primary URL of the SecurePlatform administration portal.
- Aliases that automatically redirect to the administration portal.
- A p12 certificate that the portal uses for authentication.
- How the portal can be accessed.

Configure the settings on the page:

- **Main URL** - The primary URL for the portal. You can use the same IP address for all of the portals with this variation:
  - SecurePlatform Web User interface - https://<main gateway IP address>/admin
  - Mobile Access Portal - https://<main gateway IP address>/sslvpn
  - DLP Portal - https://<main gateway IP address>/dlp
  You may choose to have the Mobile Access portal on an external IP address while others are on an internal IP address.

- **Aliases** - Click the Aliases button to Add URL aliases that are redirected to the main portal URL. Aliases can be in clear (http://) and will redirect users to the secure portal over HTTPS. For example, portal.example.com can send users to the portal. To make the alias work, it must be resolved to the main URL on your DNS server.

- **Certificate** - Click Import to import a p12 certificate for the portal website to use. If you do not import a certificate, the portal uses a Check Point auto-generated certificate. This might cause browser warnings if the browser does not recognize the gateway's management. All portals on the same IP address use the same certificate.

- **Accessibility** - Click Edit to select from where the portal can be accessed. The options are based on the topology configured for the gateway.
  The portal is accessible through these interfaces:
  - Through all interfaces
  - Through internal interfaces
    - Including undefined internal interfaces
    - Including DMZ internal interfaces
  - According to the Firewall policy - Select this if there is a rule that states who can access the portal.

Obtaining and Installing a Trusted Server Certificate

To be accepted by an endpoint computer without a warning, gateways must have a server certificate signed by a known certificate authority (such as Entrust, VeriSign or Thawte). This certificate can be issued directly to the gateway, or be a chained certificate that has a certification path to a trusted root certificate authority (CA).

The next sections describe how to get a certificate that is signed by a known certificate authority (CA) for a gateway.
Generating the Certificate Signing Request

First, generate a Certificate Signing Request (CSR). The CSR is for a server certificate, because the gateway acts as a server to the clients.

Note - This procedure creates private key files. If private key files with the same names already exist on the machine, they are overwritten without warning.

1. From the gateway command line, log in to expert mode.
2. Run:
   ```bash
   cpopenssl req -new -out <CSR file> -keyout <private key file> -config $CPDIR/conf/openssl.cnf
   ```
   This command generates a private key. You see this output:
   ```
   Generating a 2048 bit RSA private key
   +++
   ...+++ 
   writing new private key to 'server1.key'
   Enter PEM pass phrase:
   ```
   3. Enter a password and confirm. You see this message:
   ```
   You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank. For some fields there will be a default value. If you enter '.', the field will be left blank.
   Fill in the data.
   - The Common Name field is mandatory. This field must have the Fully Qualified Domain Name (FQDN). This is the site that users access. For example: portal.example.com.
   - All other fields are optional.
   4. Send the CSR file to a trusted certificate authority. Make sure to request a Signed Certificate in PEM format. Keep the .key private key file.

Generating the P12 File

After you get the Signed Certificate for the gateway from the CA, generate a P12 file that has the Signed Certificate and the private key.

1. Get the Signed Certificate for the gateway from the CA.
   If the signed certificate is in P12 or P7B format, convert these files to PEM (Base-64) format.
2. Make sure that the .crt file has the full certificate chain up to a trusted CA.
   Usually you get the certificate chain from the signing CA. Sometimes it is in a separate file. If the signed certificate and the trust chain are in separate files, use a text editor to combine them into one file.
3. From the gateway command line, log in to expert mode.
4. Use the *.crt file to install the certificate with the *.key file that you generated.
   a) Run:
      ```bash
      cpopenssl pkcs12 -export -out <output file> -in <signed cert chain file> -inkey <private key file>
      ```
      For example:
      ```bash
      cpopenssl pkcs12 -export -out server1.p12 -in server1.crt -inkey server1.key
      ```
   b) Enter the certificate password when prompted.
Installing the Signed Certificate

All portals on the same IP address use the same certificate. Define the IP address of the portal in the Portal Settings page for the blade/feature.

1. Import the new certificate to the gateway in SmartDashboard from a page that contains the Portal Settings for that blade/feature. For example:
   - Gateway Properties > Mobile Access > Portal Settings
   - Gateway Properties > SecurePlatform Settings
   - Gateway Properties > Data Loss Prevention
   - Gateway Properties > Identity Awareness > Captive Portal > Settings > Access Settings

   In the Certificate section, click Import or Replace.

2. Install the policy on the gateway.

Note - The Repository of Certificates on the IPSec VPN page of the SmartDashboard gateway object is only for self-signed certificates. It does not affect the certificate installed manually using this procedure.

Viewing the Certificate

To see the new certificate from a Web browser:

The gateway uses the certificate when you connect with a browser to the portal. To see the certificate when you connect to the portal, click the lock icon that is next to the address bar in most browsers.

The certificate that users see depends on the actual IP address that they use to access the portal - not only the IP address configured for the portal in SmartDashboard.

To see the new certificate from SmartDashboard:

From a page that contains the portal settings for that blade/feature, click the View button in the Certificate section.

Status

Use the Status page to view device and network information about the SecurePlatform machine.

Device Status

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

Network

This section allows you to configure the network interfaces, routing table, DNS and Host Name.

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 the following interface:

- VLAN
- Secondary IP
- PPPoE
- PPTP
- Bond
Network Configuration Using the Web Interface

- Bridge
- ISDN
- Loopback

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

**To configure network connections:**
- To edit the properties of an interface, click the **Name** of the interface.
- To delete a connection, select the connection checkbox and click **Delete**.

**Note** -
- Loopback and Ethernet connection cannot be deleted.
- When a Bridge or Bond is deleted, interfaces allocated for the specific connection are released.
- To disable a connection without deleting it, select the checkbox and click **Disable**.
- To configure a connection to work without an IP address, click **Remove IP**.
- To add a connection, click **New** and select the connection type from the drop-down list.
- If the connections were changed while on this page, click **Refresh**.

**Routing Table**

This page enables you to manage the routing table on your device. You can add or delete static and default routes.

**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 checkbox of the specific route and click **Delete**.

**To add a new static route:**
1. On the **Routing Table** page, click **New** and select **Route**. The **Add New Route** page appears.
2. Supply the:
   - Destination IP Address
   - Destination Netmask
   - Interface (from the drop-down box)
   - Gateway
   - Metric
3. Click **Apply**.

**To add a default route:**
1. On the **Routing Table** page, click **New** and select **Default Route**. The **Add Default Route** page appears.
2. Supply the following:
   - Gateway
   - Metric
3. Click **Apply**.

**DNS Servers**

In the **DNS Servers** page, you can define up to three DNS servers.
Note - Changes in the DNS configuration will take effect only after restarting the device services. To restart device services, use the Device Control page.

Host and Domain Name

In the Host and Domain Name page:
1. Supply a Hostname.
2. Supply a Domain Name.
3. Select a Management Interface from the drop-down box. The Hostname will be associated with the IP of this interface.

Local Hosts Configuration

This page enables you to configure the host's local resolving configuration.

Note - Host entries cannot be edited. They must be deleted and recreated. The entry for the local machine is automatically generated, based on the Domain configuration information.

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

To delete a Host:
- Select the checkbox of the entry and click Delete.

Device

Use these pages to configure the SecurePlatform machine.

Device 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 all of the Check Point products. In addition, you can Shutdown the device, Reboot it, or download a diagnostic file (cpinfo output) useful for support.

To refresh the information displayed in the page click Refresh.

device Date and Time Setup

This page allows you to define the device date and time, optionally using NTP.

Manual device date and time configuration

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).

Use Network Time Protocol (NTP) to synchronize the clock

NTP is used to synchronize clocks of computers on the network.
If the Primary NTP Server fails to respond, the Secondary NTP Server will be queried. The Shared Secret field is optional. Click Apply to set the date and time.

**Backup**

This page allows you to configure backup settings. You can choose to configure a scheduled backup, or you can choose to perform an immediate backup operation. The backup data can be stored on your desktop computer, locally (on the device), on a TFTP Server, an SCP Server or an FTP Server.

**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 utility is compliant with the environment that you are working in.

The SecurePlatform backup mechanism enables exporting snapshots of the user configurable configuration. Exported configurations can later be imported in order to restore a previous state in case of failure.

Two common use cases for backup 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

To make a backup now, click the **Backup now** link.

To configure a backup schedule, click **Scheduled backup**.

The Backup page displays the **Current device date and time**. This may be different than the browser machine time.

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

**Information Backed Up**

The information backed up includes:

- All settings performed by the Admin GUI
- Network configuration data

**Viewing the Scheduling Status**

The following information is displayed:

- **Status**: Scheduled backup is *enabled or disabled*.
- **Backup to**: The backup destination which can be one of the following: your desktop computer, locally (on the device), on a TFTP Server or a SCP Server.
- **Start at**: The time to start the backup. The current device date and time is displayed, which may be different than the browser machine time
- **Recur every**: recurrence interval.
Restoring the Backup

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

Syntax  
```
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</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 TFTP server, from which the configuration is restored, and the filename.</td>
</tr>
<tr>
<td>--scp &lt;ServerIP&gt; &lt;Username&gt; &lt;Password&gt; [ &lt;Filename&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>--file &lt;Filename&gt;</td>
<td>Specify a filename for restore operation, performed locally.</td>
</tr>
</tbody>
</table>

Example  When the restore command is executed by itself, without any additional flags, the following menu is displayed:

Output

```
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
```

Scheduling a Backup

To schedule a backup:
1. On the Backup page, click Scheduled backup. The Scheduled backup page appears.
2. Select Enable backup recurrence.
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 s 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 the device:
1. **Download an upgrade package**, as directed. If you already downloaded the file, you can skip this step.
2. **Browse** to the upgrade package file.
3. Click **Upload package to device**.
4. When you have finished uploading the package, you can click on the **Package currently found on device** 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.

Device Administrators

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

To create a device Administrator:
1. On the **device Administrators** page, click **New**. The **Add Administrator** page appears.
2. For Check Point appliances only: It is recommended to select **Secure Password Scheme**, so that the password strength is validated when the Administrator is created.
3. Provide a name and a password for the device Administrator.
4. Click **Apply**.

To download a One Time Login Key:
1. Click **Download**.
   The **Login Key Challenge** page is displayed.
2. Supply a challenge-question and answer to protect your Login Key from unauthorized usage.
3. Click **OK**.
   **Note** - The One Time Login Key will be required in case you forget your password. Save this file in a safe place.

Web and 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. Define the host with any of the following list of options:
   - IP address
   - Resolvable name (resolved locally, not by DNS)
   - "Any" - Enables a connection from any Web/SSH Client.
   - Wildcards - Use in IP format only (Right: 192.168.10.* Wrong: *.company.com).
3. Click **Apply**.

Administrator Security Settings

In the **Administrator Security** page, you can configure session and login parameters for device administrators.
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.

Product Configuration

Use these pages to configure the installed Check Point products on the SecurePlatform machine.

Security Management Administrator

The Security Management Administrators page lists the configured administrators. If no Security Management administrator has been configured, you can add one. This Security Management Administrator has Read/Write Permissions to Security Management and is allowed to manage the Security Gateway objects and Administrator accounts.

Only one administrator can be added to this list. To add more administrators, use SmartDashboard.

To delete a Security Management Administrator:
- Select the specific Security Management Administrator checkbox and click Remove.

To add the first administrator:
1. In the Add Security Management Administrator page, enter an Administrator Name and a New Password.
2. Confirm the password.
3. Click Apply.

Security Management GUI Clients

The Security Management GUI Clients page specifies the remote computers from which administrators will be allowed to connect to the Security Management Server. It lists the type, hostname/IP address and netmask of the configured GUI Clients, and enables you to add additional GUI Clients or to remove them.

To delete a GUI Client:
- Select the checkbox and click Remove.

To add a new GUI client:
1. Click Add. The Add GUI Client page opens.
2. Enter either a Hostname/IP address, 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.
3. Click Apply.

Certificate Authority

The Certificate Authority page lists key parameters of the Security Management Certificate Authority. The certificate authority is the entity that issues certificates for the Security Management Server, Security Gateways, users and other trusted entities such as OPSEC applications used in the system.

To create a new root certificate for the CA, click Reset.

Download SmartConsole Applications

From this window you can download the SmartConsole applications package from the device.
Configuring a Security Policy requires SmartConsole. Use the SmartConsole applications to connect to the Security Management Server and manage your Check Point Security Gateways.

If you already have SmartConsole installed, verify that you have the proper version. If you wish to obtain the proper version, click **Start Download**.

## Licenses

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

**To apply a license:**

1. Click the **Check Point User Center** link to obtain a license from the User Center ([http://usercenter.checkpoint.com](http://usercenter.checkpoint.com)), if you do not yet have the required license.
2. Click **New**.
3. Enter the **IP Address**, **Expiration Date**, **SKU/Features**, and **Signature Key**; or copy the license string into the clipboard, and click **Paste License** to copy all the information into the fields.
4. Click **Apply**.

**Note** - The recommended way of applying licenses is by using SmartUpdate.

## Products

Use this page to see which products and versions are installed on the device.

## Performance Optimization

In this page you can download the **Performance Optimization Guide** ([http://downloads.checkpoint.com/dc/download.htm?ID=8711](http://downloads.checkpoint.com/dc/download.htm?ID=8711)) which describes how to optimize the performance of Security Gateway for version R70 and later versions. The document also provides an overview of some of the firewall technologies in order to provide a basic understanding of how to configure the gateway parameters to best optimize network performance.

Click **Start Download** to obtain this document.
Chapter 5

Configuration Using the Command Line

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

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.

In This Chapter

First Time Setup Using the Command Line 25
Using sysconfig 25
Check Point Products Configuration 26

First Time Setup Using the Command Line

After the installation from the DVD 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 initial setup, if selected

These settings can also be configured after completing the first time setup, using sysconfig.

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 you to enter all relevant configuration parameters. As soon as all the parameters are completed, the change is applied.

Note - Entering e at any point during sysconfig takes you one menu level up.
Table 5-1  Sysconfig Configuration Options

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Purpose</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 Configuration</td>
<td>Configure SecurePlatform DHCP Server.</td>
</tr>
<tr>
<td>8  DHCP Relay Configuration</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.</td>
</tr>
<tr>
<td>11 Products Configuration</td>
<td>Configure Check Point products (cpconfig).</td>
</tr>
<tr>
<td>12 Enable / Disable hardware monitoring</td>
<td>Enable hardware sensors monitoring via SNMP (on supported Open Servers only)</td>
</tr>
</tbody>
</table>

Check Point Products Configuration

- To configure installed Check Point products, run the cpconfig application from the SecurePlatform Shell. For more about configuring Check Point products, see the R75.20 Installation and Upgrade Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12269).

When you finish the Check Point products configuration procedure as part of the first time setup, you are asked to reboot your system. After reboot, your system is available for use.

Note - You must run the Check Point Products Configuration procedure (cpconfig) to activate the products.

- To learn how to connect to your Security Management Server using the Check Point SmartConsole, see the R75.20 Installation and Upgrade Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12269).

- To learn how to set up a Firewall and Address Translation policy, see the R75.20 Firewall Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12267).
Chapter 6

Managing Your SecurePlatform System

This section provides information on how to manage your SecurePlatform 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 Firewall and Address Translation policies and QoS policies, use SmartConsole.

In This Chapter

Connecting to SecurePlatform by Using Secure Shell  
User Management  
SecurePlatform Administrators  
FIPS 140-2 Compliant Systems  
Using TFTP  
Backup and Restore

Connecting to SecurePlatform by Using Secure Shell

SecurePlatform 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 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.

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

Expert Mode

The Expert Mode provides 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 administrator 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.

**Important** - 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.

**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.

SecurePlatform Administrators

SecurePlatform 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:

Enter the following command:

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

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:

Enter the following command:

deluser <name>

You can also define additional administrators through the Web GUI.

How to Authenticate Administrators via RADIUS

Note - Authentication of SecurePlatform Administrators via RADIUS is available only if the Advanced Networking Software Blade is enabled on the gateway.

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:

- 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. Enter expert mode.
2. Type the command

   `pro enable`

3. 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>`

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

   - 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>`

   - 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>`

5. 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>`
To control local RADIUS users:

- 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 correctly.

To configure SecurePlatform to be FIPS 140-2 compliant:

- 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 (on page 30)).
3. Removes the Web GUI daemon, thus disabling the Web GUI.
4. Removes the Check Point Remote Installation daemon, thus disabling SmartUpdate.
5. Configures the Check Point Security Gateway'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

The Trivial File Transfer Protocol (TFTP) provides an easy way for transferring files to and from SecurePlatform. 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 readily available on 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.

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

SecurePlatform provides both 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 to an FTP server, TFTP server or SCP server. You can perform backups on request, or according to a predefined schedule.

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 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 37), and restore (on page 40).
Chapter 7

SecurePlatform Shell

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.

In This Chapter

Command Shell
Management Commands
Documentation Commands
Date and Time Commands
System Commands
Snapshot Image Management
System Diagnostic Commands
Check Point Commands
Network Diagnostics Commands
Network Configuration Commands
User and Administrator Commands

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 37)):

Table 7-2 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>
</tbody>
</table>
### Key Commands

<table>
<thead>
<tr>
<th>Key</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<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

#### exit

Exit the current Mode:

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

**Syntax**

```
exit
```

### Expert Mode

Switch from Standard Mode to Expert Mode.

**Syntax**

```
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.

**Syntax**

```bash
passwd
```

**Documentation Commands**

**help**

List the available commands and their respective descriptions.

**Syntax**

```bash
help
or
?
```

**Date and Time Commands**

**date**

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

**Syntax**

```bash
date [MM-DD-YYYY]
```
**Parameters**

*Table 7-3  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 7-4  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 7-5  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>
</tbody>
</table>
Date and Time Commands

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<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>]]
ntp -n <interval> <server1> [<server2>[<server3>]]
```

**Parameters**

*Table 7-6 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 &quot;--n&quot; 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.

**Syntax**

```
ntpstop
```

**ntpstart**

Start polling the NTP server.

**Syntax**

```
ntpstart
```
System Commands

audit

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

Syntax

audit setlines <number_of_lines>
audit show <number_of_lines>
audit clear <number_of_lines>

Parameters

Table 7-7 Audit Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>lines&lt;number_of_lines&gt;</td>
<td>restrict the length of the command history that can be shown to &lt;number_of_lines&gt;</td>
</tr>
<tr>
<td>show &lt;number_of_lines&gt;</td>
<td>show &lt;number_of_lines&gt; recent commands entered</td>
</tr>
<tr>
<td>clear</td>
<td>clear 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

backup -hbackup [-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>]] [--ftp <ServerIP> <Username> <Password> [-path <Path>] [<Filename>]] [--file [-path <Path>] [<Filename>]]
## Parameters

### Table 7-8 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 backup of the Check Point Security Gateway log (By default, logs are not backed up.)</td>
</tr>
<tr>
<td>-p or --purge</td>
<td>delete old backups from previous backup attempts</td>
</tr>
<tr>
<td>--sched [on hh:mm &lt;-m DayOfMonth</td>
<td>&lt;-w DaysOfWeek]</td>
</tr>
<tr>
<td></td>
<td>• On - specify time and day of week, or day of month</td>
</tr>
<tr>
<td></td>
<td>• Off - disable schedule</td>
</tr>
<tr>
<td>--tftp &lt;ServerIP&gt;</td>
<td>List of IP addresses of TFTP servers, to which the configuration will be backed up, and optionally the filename.</td>
</tr>
<tr>
<td></td>
<td>[-path &lt;Path&gt;] [&lt;Filename&gt;]</td>
</tr>
<tr>
<td>--scp &lt;ServerIP&gt;</td>
<td>List of IP addresses of SCP servers, to 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></td>
<td>&lt;Username&gt; &lt;Password&gt; [-path &lt;Path&gt;] [ &lt;Filename&gt;]</td>
</tr>
<tr>
<td>--ftp &lt;ServerIP&gt;</td>
<td>List of IP addresses of FTP servers, to which the configuration will be backed up, the username and password used to access the FTP Server, and optionally, the filename.</td>
</tr>
<tr>
<td></td>
<td>&lt;Username&gt; &lt;Password&gt; [-path &lt;Path&gt;] [ &lt;Filename&gt;]</td>
</tr>
<tr>
<td>--file [-path &lt;Path&gt;]</td>
<td>When the backup is performed locally, specify an optional filename</td>
</tr>
<tr>
<td></td>
<td>[&lt;Filename&gt;]</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
```

Puts the backup file in (local) /tmp and names it filename
The backup file is saved on:

1. tftp server with ip1, the backup file is saved in the tmp directory (under the tftp server default directory – usually /tftproot) with the default file name – backup_SystemName_Timestamp.tgz
2. tftp server with ip2, the backup file is saved on var (under the tftp server default directory – usually /tftproot) as file1
3. scp server with ip3, the backup file is 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.

Syntax

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>
<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 DVD</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,</td>
</tr>
<tr>
<td></td>
<td>/var/tmp/mypatch.tgz)</td>
</tr>
</tbody>
</table>

**restore**

Restore the system configuration.

**Syntax**


**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 TFTP server, from</td>
</tr>
<tr>
<td></td>
<td>which the configuration is restored, and the filename.</td>
</tr>
<tr>
<td>--scp &lt;ServerIP&gt; &lt;Username&gt; &lt;Password&gt; [&lt;Filename&gt;]</td>
<td>IP address of SCP server, from</td>
</tr>
<tr>
<td></td>
<td>which the configuration is restored, the username and</td>
</tr>
<tr>
<td></td>
<td>password used to access the SCP Server, and the filename.</td>
</tr>
</tbody>
</table>
--ftp <ServerIP> 
<Username> 
<Password> [-path <Pat>] [<Filename>]  
List of IP addresses of FTP servers, to which the configuration will be backed up, the username and password used to access the FTP Server, and optionally, the filename.

--file <Filename>  
Specify a filename for restore operation, performed locally.

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
- [V] Restore backup package from FTP server
- [R] Remove local backup package
- [Q] Quit

Select the operation of your choice.

**shutdown**

Shut down the system.

**Syntax**

```
shutdown
```

**ver**

Display the SecurePlatform system's version.

**Syntax**

```
ver
```

**Snapshot Image Management**

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 administrator 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, a SCP Server or and FTP 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 Security Management Server, Log Server, Multi-Domain Security Management, 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.

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

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>--ftp &lt;ServerIP&gt; &lt;Username&gt; &lt;Password&gt; [--path &lt;Pat&gt;] [&lt;Filename&gt;]</td>
<td>List of IP addresses of FTP servers, to which the configuration will be backed up, the username and password used to access the FTP Server, and optionally, the filename.</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>]
          [--ftp <ServerIP> <Username> <Password> <Filename>]
          [--file <Filename>]
```

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 made, 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 made, the username and password used to access the SCP Server, and the filename of the snapshot.</td>
</tr>
<tr>
<td>--ftp &lt;ServerIP&gt; &lt;Username&gt; &lt;Password&gt; [-path &lt;Pat&gt;] [&lt;Filename&gt;]</td>
<td>List of IP addresses of FTP servers, to which the configuration will be backed up, the username and password used to access the FTP Server, and optionally, the filename.</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

diag

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

Syntax

```
diag <log_file_name> tftp <tftp_host_ip_address>
```
### Parameters

**Table 7-11 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_addr</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.

**Syntax**

```
log --help
log list
log limit <log-index><max-size><backlog-copies>
log unlimit <log-index>
log show <log-index> [<lines>]
```

### Parameters

**Table 7-12 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

top

Check Point Commands


Network Diagnostics Commands

ping

Send ICMP ECHO_REQUEST packets to network hosts.

Syntax


Parameters

Table 7-13 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>
</tbody>
</table>
### Network Diagnostics Commands

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-i wait</code></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 <code>-f</code> option.</td>
</tr>
<tr>
<td><code>-l</code></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><code>-n</code></td>
<td>Numeric output only. No attempt will be made to lookup symbolic names for host addresses.</td>
</tr>
<tr>
<td><code>-p pattern</code></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, <code>-p ff</code> will direct the sent packet to be filled with a series of ones (&quot;1&quot;).</td>
</tr>
<tr>
<td><code>-q</code></td>
<td>Quiet output. Nothing is displayed except the summary lines at the time of startup and finish.</td>
</tr>
<tr>
<td><code>-R</code></td>
<td>Record route. Includes the <code>RECORD_ROUTE</code> option in the <code>ECHO_REQUEST</code> 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>
<tr>
<td><code>-r</code></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><code>-s packetsize</code></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><code>-v</code></td>
<td>Verbose (detailed) output. Lists ICMP packets (other than <code>ECHO_RESPONSE</code>) that are received.</td>
</tr>
</tbody>
</table>

### 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.

#### Syntax

```
traceroute [ -dFInrvx ] [ -f first_ttl ] [ -g gateway ] [ -i iface ] [ -m max_ttl ] [ -p port ] [ -q nqueries ] [ -s src_addr ] [ -t tos ]
```
[ -w waittime ] host [ packetlen ]

**Parameters**

*Table 7-14 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>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 name server 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>
### Network Diagnostics Commands

<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

```bash
netstat [-vnenCnCF] [<A|F>] -r
netstat {-V|--version|--h|--help}
netstat [-vnenCnCaol] [<Socket> ...]
netstat {-vnenNac} -i | [-cnNe] -M | -s }
```
### Parameters

**Table 7-15 netstat 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: {-t</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) netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)</td>
</tr>
</tbody>
</table>
Network Configuration Commands

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>parameter</td>
<td>meaning</td>
<td>extended meaning</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-H type, hw</td>
<td>type</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</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</td>
<td>Remove any entry for the specified host. This can be used if the indicated host is brought down, for example.</td>
</tr>
<tr>
<td>-D</td>
<td>use-device</td>
<td>Use the interface ifa's hardware address.</td>
</tr>
<tr>
<td>-i If device</td>
<td></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</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> [<host2> ...]
hosts remove <IP_ADDRESS> <host1> [<host2> ...]
hosts
defaultroute
```

SecurePlatform Shell  Page 51
Parameters

Table 7-17 hosts Parameters

<table>
<thead>
<tr>
<th>hosts</th>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Running hosts, with no parameters, displays the current host names to IP mappings.</td>
<td></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]

ifConfig Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</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>parameter</td>
<td>meaning</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>up</td>
<td>Causes the interface to be activated. It is implicitly specified if an address is assigned to the interface.</td>
</tr>
<tr>
<td>down</td>
<td>Causes the driver for this interface, to be shut down.</td>
</tr>
<tr>
<td>[-]arp</td>
<td>Enable or disable the use of the ARP protocol, on this interface.</td>
</tr>
<tr>
<td>[-]promisc</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>[-]allmulti</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>metric N</td>
<td>Sets the interface metric.</td>
</tr>
<tr>
<td>mtu N</td>
<td>Sets the Maximum Transfer Unit (MTU) of an interface.</td>
</tr>
<tr>
<td>dstaddr addr</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>netmask addr</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>
<tr>
<td>irq addr</td>
<td>Set the interrupt line used by this device. Not all devices can 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 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. Not all devices can change this setting, and those that can vary in what values they support. Typical values for type are 10base2 (thin Ethernet), 10baseT (twisted-pair 10Mbps Ethernet), AUI (external transceiver) and so on. The special, medium type of auto can be used to tell the driver to auto-sense the media. Not all drivers support this feature.</td>
</tr>
<tr>
<td>[-]broadcast [addr]</td>
<td>If the address argument is given, set the protocol broadcast address for this interface. Otherwise, set (or clear) the 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, meaning that it is a direct link between two machines, with nobody else listening on it. If the address argument is also given, set the protocol address of the other side of the link, just like the obsolete dstaddr keyword does. Otherwise, set or clear the 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 supports this operation. The keyword must be followed by the name of the hardware class and the printable ASCII equivalent of the hardware address. Hardware classes currently supported include: ether (Ethernet), ax25 (AMPR AX.25), ARCnet and netrom (AMPR NET/ROM).</td>
</tr>
<tr>
<td>parameter</td>
<td>meaning</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>multicast</td>
<td>Set the multicast flag on the interface. This should not normally 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</td>
<td>Set the length of the transmit queue of the device. It is useful to set this to small values, for slower devices with a high latency (modem links, ISDN), to prevent fast bulk transfers from disturbing interactive traffic, like telnet, too much.</td>
</tr>
<tr>
<td>--save</td>
<td>Saves the interface IP configuration. Not available when UTM-1 is installed.</td>
</tr>
</tbody>
</table>

**vconfig**

Configure virtual LAN interfaces.

**Syntax**

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

**Parameters**

*Table 7-18 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>
</tbody>
</table>
flag-num

Either 0 or 1 (REORDER_HDR). If set, the VLAN device will move the Ethernet header around to make it look exactly like a real Ethernet device.

**route**

Show, configure or save the routing entries.

**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
```

**Parameters**

*Table 7-19  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>
<tr>
<td>netrom</td>
<td>(AMPR NET/ROM)</td>
<td>ipx</td>
</tr>
<tr>
<td>(Novell IPX)</td>
<td>ddp</td>
<td>(Appletalk DDP)</td>
</tr>
<tr>
<td>save</td>
<td></td>
<td>Save the routing configuration</td>
</tr>
</tbody>
</table>
hostname

Show or set the system's host name.

Syntax

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

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>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show domainname</td>
<td></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**

dns [add|del <ip_of_nameserver>]

**Parameters**

*Table 7-22 dns Parameters*

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>show DNS servers configured</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**

sysconfig

**webui**

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

**Syntax**

webui enable [https_port]
webui disable

**Parameters**

*Table 7-23 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>
User and Administrator Commands

**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 7-24 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 58) for more information about a locked administrator.)

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

SNMP support is based on the Net-SNMP open source package, and provides the following features:

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

In This Chapter

Configuring the SNMP Agent
SNMP Monitoring

Configuring the SNMP Agent

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

```
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>]
```

Parameters

*Table 8-25 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>
</tbody>
</table>
SNMP Monitoring

Introduction to SNMP Monitor

Hardware health sensors and RAID disks can be monitored using the SecurePlatform SNMP monitoring daemon. SNMP traps can be set to fire once an OID value is in breach of a configurable threshold. When the OID value is back within threshold boundaries a "clear" trap is sent.

The SNMP monitoring daemon `snmpmonitor` integrates with the default SecurePlatform net-snmp / Agentx components that are part of the standard SecurePlatform installation.

SNMP Monitor Configuration Guidelines

For each OID that you wish to monitor, a monitoring rule must be defined in the `/etc/snmp/snmpd.conf` file. The following parameters are required for each monitoring rule:

- The OID to monitor.
- A comparison operator: one of: !=, <, >, ==.
- A threshold value: either an integer (not enclosed within double quotes "") or a string (enclosed within double quotes "").
- A polling Interval (in seconds).
- A message (e.g. "HA sync link 1 down", "Internet VLAN down", "Low REAL memory", etc.).

General configuration guidelines are:

- All configuration is performed in the `/etc/snmp/snmpd.conf` file.
- Double quotes are required for enclosing string values.
- Single quotes are not supported for enclosing string values but may be used inside string values.
- Lines that start with # are ignored.
- All lines that do not start with `snmp monitor` daemon commands are ignored.

Commands used by SNMP Monitor

`cp_monitor`

The `cp_monitor` command defines a single monitoring rule.

```
cp_monitor <OID> <Operator> <Threshold> <Frequency> <Message>
```

Once the expression `<oid> <operator> <threshold>` evaluates to true, traps are sent until the expression evaluates back to false. At that point one or more clear traps are sent to indicate that the OID value has fallen back within acceptable boundaries.
Table 8-26 cp_monitor parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>Use standard OID notation. OID types supported are: Integer, String.</td>
</tr>
<tr>
<td>Operator</td>
<td>For OIDs of type Integer: Use one of: !=, &lt;, &gt;, == For OIDs of type String: Use one of: !=, ==</td>
</tr>
<tr>
<td>Threshold</td>
<td>For OIDs of type Integer: an integer value For OIDs of type String: a string enclosed within double quotes &quot;&quot;</td>
</tr>
<tr>
<td>Frequency</td>
<td>Integer value representing polling interval in seconds. The daemon polls each monitored OID at the given interval. If a trap should fire it is then fired.</td>
</tr>
<tr>
<td>Message</td>
<td>A textual message to describe the trap (sent as part of the trap), must be enclosed within double quotes &quot;&quot;.</td>
</tr>
</tbody>
</table>

Example:

```
cp_monitor 1.3.6.1.4.1.2021.4.6.0 < 2000 5 "memAvailReal"
cp_monitor 1.3.6.1.4.1.2620.1.5.6.0 != "active" 5 "Cluster State"
```

To verify correctness of OID used in a cp_monitor line make sure the equivalent snmpget command returns a value. For example, if attempting to configure the above example cp_monitor "memAvailReal" line, then the following snmpget command should return a value:

```
"snmpget -v 2c -c public localhost 1.3.6.1.4.1.2021.4.6.0"
```

**cp_cleartrap**

The optional cp_cleartrap command can instruct the daemon about the number of clear traps to send and the interval between each. That is, once a rule's OID value falls back to being within configured threshold.

```
cp_cleartrap <interval> <retries>
```

Default values are: 3 packets at 10 seconds intervals.

Table 8-27 cp_cleartrap parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval</td>
<td>A number indicating time between clear trap packets, in seconds.</td>
</tr>
<tr>
<td>Retries</td>
<td>A number indicating number of clear trap packets to send.</td>
</tr>
</tbody>
</table>

**trap2sink**

The trap2sink command designates a host that receives traps.
SNMP Monitoring

The snmpmonitor daemon requires a trap2sink command to exist inside the /etc/snmp/snmpd.conf file. The trap2sink command is required (as opposed to the trapsink command) because the snmpmonitor daemon sends SNMP version 2c traps. Note this command is part of the net-snmp syntax.

**Table 8-28 trap_2_sink parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>sink-server</td>
<td>A sink server for which traps are sent.</td>
</tr>
<tr>
<td>port</td>
<td>An optional (UDP) port number on which the server listens. The default is port 162.</td>
</tr>
<tr>
<td>community</td>
<td>An SNMP community</td>
</tr>
</tbody>
</table>

Example:

```
trap2sink 10.10.10.10 public
trap2sink 10.10.10.10:1610 MyCommunity
```

**Configuring SNMP Monitoring and Traps**

To configure SNMP monitoring and traps:

1. Edit the /etc/snmp/snmpd.conf configuration file and define the SNMP monitoring rules and the trap server.

   The following is an example configuration file:

   ```
   trap2sink 10.10.10.10 public
cp_cleartrap 10 2
proc syslogd 1 1
disk /var 20%
cp_monitor 1.3.6.1.2.1.2.2.1.8.1 == 2 60 "link 1 down"
cp_monitor prErrorFlag.1 != "0" 60 "process monitor"
cp_monitor dskErrorFlag.1 != 0 60 "disk monitor"
cp_monitor 1.3.6.1.4.1.2021.10.1.5.1 > 100 60 "CPU load 1 min"
cp_monitor 1.3.6.1.4.1.2021.10.1.5.2 > 90 60 "CPU load 5 min"
cp_monitor 1.3.6.1.4.1.2021.4.4.0 < 2000 60 "memAvailSwap"
cp_monitor 1.3.6.1.4.1.2021.4.6.0 < 2000 60 "memAvailReal"
cp_monitor 1.3.6.1.4.1.2620.1.5.6.0 != "active" 20 "Cluster State"
cp_monitor 1.3.6.1.4.1.2620.1.125.3.0 > 50000 20 "Firewall connections"
cp_monitor 1.3.6.1.2.1.25.2.3.1.6.6 > 60000 60 "/opt hrStorageUsed"
```

2. At the SecurePlatform command prompt, start the snmp service. Run:

   ```
   snmp service enable
   ```
Chapter 9

Hardware Health Monitoring

SecurePlatform enables a number of hardware health monitoring capabilities for Check Point appliances and for open servers.

In This Chapter

- Introduction to Hardware Health Monitoring 64
- RAID Monitoring with SNMP 64
- Sensors Monitoring with SNMP 66
- Sensors Monitoring Via the Web Interface on Power-1, UTM-1 and Smart-1 69

Introduction to Hardware Health Monitoring

SecurePlatform features the following Hardware Health Monitoring capabilities:

- **RAID health**: Monitor the health of the disks in the RAID array, and be notified of the states of the volumes and disks. The information is available via SNMP.

- **Sensors**: Monitor fan speed, motherboard voltages and temperatures on the hardware. The information is available via SNMP and, for Check Point appliances, also via the SecurePlatform Web interface.

The following matrix summarizes the supported health monitoring features:

<table>
<thead>
<tr>
<th>Hardware sensors monitoring with SNMP (polling and traps)</th>
<th>Check Point Appliances</th>
<th>Open Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Power-1</td>
<td>UTM-1</td>
</tr>
<tr>
<td>Hardware sensors monitoring with SNMP (polling and traps)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(1)</td>
</tr>
<tr>
<td>Hardware sensors monitoring with the Web UI (polling and traps)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(1)</td>
</tr>
<tr>
<td>RAID monitoring with SNMP</td>
<td>(3)</td>
<td></td>
</tr>
</tbody>
</table>

1. **Hardware sensors monitoring** is supported on all UTM-1 models except the xx50 series.

2. **Hardware sensors monitoring** for open servers is supported on certified servers with an Intelligent Platform Management Interface (IPMI) card installed. The IPMI specification defines a set of common interfaces to a computer system, which system administrators can use to monitor system health.

3. **RAID Monitoring with SNMP** is supported on Power-1 servers with RAID card installed (Power-1 9070 and Power-1 11070).

4. **RAID Monitoring with SNMP** on HP servers is supported with a P400 RAID controller.

RAID Monitoring with SNMP

The health of disks’ RAID array can be monitored using the SecurePlatform SNMP monitoring daemon. SNMP traps can be set to fire once an OID value is in breach of a configurable threshold.

The raidInfo MIB branch is 1.3.6.1.4.1.2620.1.6.7.7. The information it contains is detailed below.

Data is available in the form of two SNMP tables:
SNMP Table | OID
--- | ---
Volumes | 1.3.6.1.4.1.2620.1.6.7.7.1.1
Disks | 1.3.6.1.4.1.2620.1.6.7.7.2.1

Each volume in the RAID configuration has an entry in the Volumes table. Each volume's entry in the Volumes table contains the following OID values:

<table>
<thead>
<tr>
<th>Disk Volume Information</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>.1</td>
<td></td>
</tr>
<tr>
<td>Volume ID</td>
<td>.2</td>
<td></td>
</tr>
<tr>
<td>Volume Type (RAID level)</td>
<td>.3</td>
<td>For check Point appliances, will normally be RAID_1</td>
</tr>
<tr>
<td>Number Of Disks in the RAID</td>
<td>.4</td>
<td></td>
</tr>
<tr>
<td>Volume size</td>
<td>.5</td>
<td>Maximum supported LBA (Logical Block Addressing)</td>
</tr>
</tbody>
</table>
| Volume state            | .6  | One of:  
  - OPTIMAL  
  - DEGRADED  
  - FAILED  |
| Volume state            | .7  | One or more of:  
  - ENABLED  
  - QUIESCED  
  - RESYNC_IN_PROGRESS  
  - VOLUME_INACTIVE  |

Each disk participating in the RAID configuration has an entry in the disks table. Each disk's entry in the table contains the following OID values:

<table>
<thead>
<tr>
<th>Physical Disks information</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>.1</td>
<td></td>
</tr>
<tr>
<td>Volume ID</td>
<td>.2</td>
<td></td>
</tr>
<tr>
<td>SCSI ID</td>
<td>.3</td>
<td></td>
</tr>
<tr>
<td>Disk number</td>
<td>.4</td>
<td>On Check Point Power-1 9070 appliance: 0 - upper disk, 1 - lower disk</td>
</tr>
<tr>
<td>Vendor</td>
<td>.5</td>
<td></td>
</tr>
<tr>
<td>Product ID</td>
<td>.6</td>
<td></td>
</tr>
<tr>
<td>Revision</td>
<td>.7</td>
<td></td>
</tr>
<tr>
<td>Size</td>
<td>.8</td>
<td>Maximum supported LBA (Logical Block Addressing)</td>
</tr>
</tbody>
</table>
### Physical Disks information

<table>
<thead>
<tr>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>.9</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• ONLINE</td>
</tr>
<tr>
<td></td>
<td>• MISSING</td>
</tr>
<tr>
<td></td>
<td>• NOT_COMPATIBLE</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• INITIALIZING</td>
</tr>
<tr>
<td></td>
<td>• OFFLINE_REQUESTED</td>
</tr>
<tr>
<td></td>
<td>• FAILED_REQUESTED</td>
</tr>
<tr>
<td></td>
<td>• OTHER_OFFLINE</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>.10</td>
<td>One of:</td>
</tr>
<tr>
<td></td>
<td>• OUT_OF_SYNC</td>
</tr>
<tr>
<td></td>
<td>• QUIESCED</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>.11</td>
<td>A percentage. Shows how much of the backup disk is synchronized with the primary disk</td>
</tr>
</tbody>
</table>

### Example RAID Monitoring OIDs

<table>
<thead>
<tr>
<th>OID</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.2620.1.6.7.7.1.1.3.1.0</td>
<td>RAID type field of entry #1 from the volumes table</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2620.1.6.7.7.1.1.4.1.0</td>
<td>Number of disks field of entry #1 from the volumes table</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2620.1.6.7.7.2.1.4.2.0</td>
<td>Disk number field of entry #2 from the disks table</td>
</tr>
</tbody>
</table>

SNMP monitoring rules are defined in the `snmpd.conf` configuration file. For full details see SNMP Monitoring (on page 61).

### Sensors Monitoring with SNMP

Hardware health sensors can be monitored using the SecurePlatform SNMP monitoring daemon. SNMP traps can be set to fire once an OID value is in breach of a configurable threshold.

The sensorInfo MIB branch is 1.3.6.1.4.1.2620.1.6.7.8. The information it contains is detailed below.

Data is available in the form of 3 SNMP tables:

<table>
<thead>
<tr>
<th>SNMP Table</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperatures</td>
<td>1.3.6.1.4.1.2620.1.6.7.8.1.1</td>
</tr>
<tr>
<td>Fan speeds</td>
<td>1.3.6.1.4.1.2620.1.6.7.8.2.1</td>
</tr>
<tr>
<td>Voltages</td>
<td>1.3.6.1.4.1.2620.1.6.7.8.3.1</td>
</tr>
</tbody>
</table>

Each sensor in the system has an entry in one of the 3 tables. Each sensor’s entry contains the following OID values:
<table>
<thead>
<tr>
<th>Sensors Table Entry</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>.1</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>.2</td>
<td></td>
</tr>
<tr>
<td>Value</td>
<td>.3</td>
<td></td>
</tr>
<tr>
<td>Unit of measurement</td>
<td>.4</td>
<td>One of:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Degrees C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RPM (Revolutions per Minute)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Volts</td>
</tr>
<tr>
<td>Type</td>
<td>.5</td>
<td>One of:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Temperature</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Voltage</td>
</tr>
<tr>
<td>Status</td>
<td>.6</td>
<td>One of:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 - In normal range</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 - Out of normal range</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 - Reading error</td>
</tr>
</tbody>
</table>

**Example Sensors Monitoring OIDs**

<table>
<thead>
<tr>
<th>OID</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.2620.1.6.7.8.1.1.2.1.0</td>
<td>Name of sensor #1 from the Temperatures table</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2620.1.6.7.8.2.1.3.4.0</td>
<td>Value of sensor #4 from the Fan Speeds table</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2620.1.6.7.8.3.1.6.5.0</td>
<td>Status of sensor #5 from the Voltages table</td>
</tr>
</tbody>
</table>

SNMP monitoring rules are defined in the `snmpd.conf` configuration file. For full details see SNMP Monitoring (on page 61).

**Sensors Monitoring with SNMP on Power-1, UTM-1 and Smart-1 Appliances**

*Note* - The information in this section is taken from SecureKnowledge solution sk42426 ([http://supportcontent.checkpoint.com/solutions?id=sk2426](http://supportcontent.checkpoint.com/solutions?id=sk2426))

On Power-1, UTM-1 and Smart-1 appliances the hardware status can be monitored using WebUI and SNMP polling, or by defining the SNMP trap using the `cp_monitor` mechanism.

SNMP monitoring rules are defined in the `snmpd.conf` configuration file. For full details see SNMP Monitoring (on page 61). Examples of `cp_monitor` for various appliance types are as follows:
## Sensors Monitoring with SNMP

### UTM-1 130

| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.1.0 > 80 | "M/B Temp is too high" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.2.0 > 90 | "CPU Temp is too high" |

### UTM-1 270

| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.1.0 > 80 | "M/B Temp is too high" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.2.0 > 100 | "CPU Temp is too high" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.2.1.3.1.0 < 16320 | "Case Fan speed is too low" |

### UTM-1 570 and UTM-1 1070

| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.1.0 > 80 | "M/B Temp is too high" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.2.0 > 100 | "CPU Temp is too high" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.2.1.3.1.0 > 100 | "CPU Fan speed is too low" |

### UTM-1 2070 and UTM-1 3070

| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.1.0 > 80 | "M/B Temp is too high" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.2.0 > 100 | "CPU Temp is too high" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.2.1.3.1.0 < 4220 | "CPU Fan speed is too low" |

### Power-1 5070

| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.1.0 > 80 | "M/B Temp is too high" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.2.0 > 100 | "CPU Temp is too high" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.2.1.3.1.0 < 3000 | "CPU 1 Fan speed is too low" |

### Power-1 9070

| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.1.0 > 100 | "CPU 1 Temp is too high" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.2.0 > 100 | "CPU 2 Temp is too high" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.3.0 > 3000 | "CPU 1 Fan speed is too low" |

### Power-1 11000

| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.1.0 > 100 | "CPU 1 Temp is too high" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.2.0 > 100 | "CPU 2 Temp is too high" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.1.1.3.3.0 > 100 | "CPU 2 Fan speed is too low" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.2.1.3.1.0 < 0 | "Case Fan 1 speed is too low" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.2.1.3.2.0 < 0 | "Case Fan 2 speed is too low" |
| cp_monitor 1.3.6.1.4.1.2620.1.6.7.8.2.1.3.3.0 < 0 | "Case Fan 3 speed is too low" |
Sensors Monitoring Via the Web Interface on Power-1, UTM-1 and Smart-1

Note - Hardware sensors monitoring via the Web interface is supported only by the Check Point Power-1, UTM-1 and Smart-1 appliances.

The Hardware Sensors page provides information about temperature, voltage and fan speed of the appliance. A warning is displayed if one of the values exceeds the threshold's values. The thresholds are hard-coded in the hardware.

The following shows the Hardware Sensors page of the SecurePlatform Web interface.
Chapter 10

SecurePlatform Boot Loader

In This Chapter

Booting in Maintenance Mode 70
Customizing the Boot Process 70
Snapshot Image Management 70

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 41).
Index

A
addarp • 50
dadder • 58
Administrator Security Settings • 22
arp • 50
audit • 37

B
backup • 37
Backup • 20
Backup and Restore • 31
Before Using the Tool • 9
BIOS Security Configuration Recommendations • 10
Booting in Maintenance Mode • 70

C
Certificate Authority • 23
Changing the Settings of the SecurePlatform Portal • 15
Check Point Commands • 45
Check Point Products Configuration • 26
checkuserlock • 59
Client Setup • 11
Command Line Editing • 32
Command Output • 33
Command Set • 32
Command Shell • 32
Commands used by SNMP Monitor • 61
Configuration Using the Command Line • 25
Configuration Using the Web Interface • 14
Configuring SNMP Monitoring and Traps • 63
Configuring the SNMP Agent • 60
Connecting to SecurePlatform by Using Secure Shell • 27
Connecting to the Web Interface • 14
cp_cleartrap • 62
cp_monitor • 61
Customizing the Boot Process • 70

c

D
date • 34
Date and Time Commands • 34
delarp • 50
deluser • 58
Description • 34
Device • 19
Device Administrators • 22
Device Control • 19
device Date and Time Setup • 19
Device Status • 17
DHCP Daemon Setup • 12
diag • 43
ds • 56
DNS Servers • 18
Documentation Commands • 34
domainname • 56
Download SmartConsole Applications • 23

E
Example RAID Monitoring OIDs • 66
Example Sensors Monitoring OIDs • 67
Examples • 38
exit • 33
Expert Mode • 28, 33

F
FIPS 140-2 Compliant Systems • 30
First Time Setup Using the Command Line • 25
First Time Setup Using the Web Interface • 14

G
General Procedure • 11
Generating the Certificate Signing Request • 16
Generating the P12 File • 16

H
Hardware Compatibility Testing Tool • 8
Hardware Health Monitoring • 64
help • 34
Host and Domain Name • 19
Hosting Installation Files • 13
hostname • 56
hosts • 51
How to Authenticate Administrators via RADIUS • 29

I
ifconfig • 52
Important Information • 3
Information Backed Up • 20
Installing Products on SecurePlatform • 10
Installing SecurePlatform on Computers without Optical Drives • 11
Installing the Signed Certificate • 16
Introduction to Hardware Health Monitoring • 64
Introduction to SecurePlatform • 7
Introduction to SNMP Monitor • 61

L
Licenses • 24
Local Hosts Configuration • 19
lockout • 58
Lockout of Administrator Accounts • 30
log • 44

M
Management Commands • 33
Managing Your SecurePlatform System • 27

N
netstat • 48
Network • 17
Network Configuration Commands • 50
Network Connections • 17
Network Diagnostics Commands • 45
ntp • 36
ntpstart • 36
ntpsstop • 36
O
Obtaining and Installing a Trusted Server Certificate • 15
Obtaining the Hardware Compatibility Testing Tool • 9

P
Parameters • 35, 36, 37, 38, 40, 42, 43, 44, 45, 47, 49, 50, 52, 54, 55, 56, 57, 59, 60
passwd • 34
patch • 39
Performance Optimization • 24
ping • 45
Preparing the SecurePlatform Machine • 8
Preparing to Install SecurePlatform • 8
Product Configuration • 23
Products • 24
PXELINUX Configuration Files • 12

R
RAID Monitoring with SNMP • 64
reboot • 39
Required Packages • 12
restore • 40
Restoring the Backup • 20
Revert • 42
route • 55
Routing Table • 18
Running the Hardware Compatibility Testing Tool • 9

S
Scheduling a Backup • 21
SecurePlatform Administrators • 28
SecurePlatform Boot Loader • 70
SecurePlatform Hardware Requirements • 8
SecurePlatform Shell • 32
Security Management Administrator • 23
Security Management GUI Clients • 23
Sensors Monitoring Via the Web Interface on Power-1, UTM-1 and Smart-1 • 68
Sensors Monitoring with SNMP • 66
Sensors Monitoring with SNMP on Power-1, UTM-1 and Smart-1 Appliances • 67
Server Setup • 12
showusers • 58
shutdown • 41
Snapshot • 43
Snapshot Image Management • 41, 70
SNMP Monitor Configuration Guidelines • 61
SNMP Monitoring • 61
SNMP Support • 60
Standard Mode • 28
Status • 17
Syntax • 33, 34, 35, 36, 37, 39, 40, 41, 43, 44, 45, 46, 48, 50, 51, 52, 54, 55, 56, 57, 58, 59
sysconfig • 57
System Commands • 37
System Diagnostic Commands • 43

T
TFTP and FTP Daemon Setup • 13
time • 35
timezone • 35
top • 45
traceroute • 46
trap2sink • 62

U
unlockuser • 59
Upgrade • 21
User and Administrator Commands • 58
User Management • 27
Using sysconfig • 25
Using TFTP • 30
Using the Hardware Compatibility Testing Tool • 9

V
vconfig • 54
ver • 41
Viewing the Backup Log • 21
Viewing the Certificate • 17
Viewing the Scheduling Status • 20

W
Web and SSH Clients • 22
webui • 57