This Release Notes document provides essential installation and operating requirements for the R70.1 Release.

Note - The latest available version of this document is at: http://supportcenter.checkpoint.com/documentation_download?ID=10067

In This Document

Introduction  page 3
What’s New in R70.1  page 3
Supported Platforms and Versions  page 6
Installing R70.1  page 8
Installing the R70.1 SmartConsole or MDG  page 13
Uninstalling R70.1  page 13
Known Limitations  page 15
Managing Check Point Appliances Using the LCD Panel  page 16
Related Resources  page 17
Documentation Feedback  page 18
Introduction

Thank you for updating to Check Point Suite R70.1 including SmartWorkflow Blade. This release is a recommended update that contains new features and resolves various issues for the Check Point Suite.

Please read this document carefully prior to installing Check Point Suite R70.1. We also recommend that you refer to the appropriate Check Point user documentation and Release Notes, which contain hardware requirements, software requirements, and version recommendations.

You can see the latest version of this document at: http://supportcontent.checkpoint.com/documentation_download?ID=10067

What’s New in R70.1

Quality Improvements

Check Point Suite R70.1 delivers significant improvements in quality and resolves issues from R70 and previous releases. For a list of resolved issues, see sk42333 at http://supportcontent.checkpoint.com/solutions?id=sk42333.

SmartWorkflow Blade

SmartWorkflow is a full-featured security policy change management solution incorporated into the Security Management Server and Provider-1 environments.

- SmartWorkflow sessions allow administrators to work with discrete sets of proposed changes to the network security configuration.
- Comprehensive audit features allow administrators to track, control, and analyze changes to the network security configuration as follows:
  - New or modified elements are highlighted in the SmartDashboard object tree and Rule Base.
  - The Session Information window documents specific changes and provides justification for these actions.
  - Audit logs provide detailed information regarding all changes and can be viewed in SmartView Tracker.
  - The Change Summary Report provides a list of changes made to the Rule Base and Network objects.
  - The Compare Policies feature provides a comparison between the installed policy and the currently defined policy or between selected policy versions.
- Role segregation, with separate administrator and manager roles, ensures that proposed changes are approved by authorized managers prior to implementation and that only authorized managers can configure SmartWorkflow properties. This feature is optional.
- SmartWorkflow contains a user-friendly toolbar, menu, and other convenient user interface elements that make it easy to learn and use.

For detailed information on SmartWorkflow, see the R70.1 SmartWorkflow Blade Administration Guide at:

http://supportcontent.checkpoint.com/documentation_download?ID=10069
Additional Features

R70.1 contains the following additional features:

**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 in Check Point appliances. The information is available via SNMP.

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

For more information see the *Hardware Health Monitoring for R70.1 Appliances and Open Servers Administration Guide* at http://supportcontent.checkpoint.com/documentation_download?ID=8650

**Remote Deployment Tool**

The Remote Deployment tool enables deployment of Power-1 and UTM-1 appliances in branch offices or any location that is not accessible by the security or network administrator. The Remote Deployment tool consists of a USB key that includes a simple configuration file for the installation process. Once the USB key is inserted into the appliance and the appliance is turned on, the appliance reads configuration information that enables it to be deployed remotely.

For more information see the *Remote Deployment Tool R70.1 Administration Guide* at: http://supportcontent.checkpoint.com/documentation_download?ID=10098

**Enhanced LCD Panel Menus**

Configure the management IP address, netmask, and default gateway of the Check Point appliance directly from the front panel. The appliance can also be rebooted from the front panel.

For more information see “Managing Check Point Appliances Using the LCD Panel” on page 16.

**Link Aggregation is Now Available on SecurePlatform**

Link Aggregation (also known as NIC teaming) involves bonding multiple network interfaces on a Security Gateway. The Load Sharing mode of Link Aggregation can significantly increase total throughput by supplying load sharing, in addition to high availability. All interfaces are active, and connections are balanced between the bond’s interfaces. Connections are balanced according to network layers three and four, and follow either the IEEE 802.3ad standard or XOR.

For more information see the *ClusterXL R70.1 Administration Guide* at: http://supportcontent.checkpoint.com/documentation_download?ID=10068

**Security Management Enhancements**

New Security Management enhancements have been added based on requests from our valued customers. The features are:

- **Quick Add Object** - Allows you to easily find and insert objects into the Security Rule Base

- **Where Used > Go To** - Allows you to jump from the Where Used window to the locations it references.
- **Easily View Group Members** - When hovering over a Group in the Rule Base, a tooltip displays the Group members.

- **Extended Clone Functionality** - The Clone functionality, which allows creating a new object based on an existing one, is extended to include Services, IP ranges, Group objects, etc.

- **Read Only State for Object Properties** - In numerous key fields of the object properties it is now possible to copy the text of the fields while in 'Read-only' state.

- **Delete Multiple Database Versions** - While in the Database Revision Control window, it is possible to select multiple Database Versions and delete them at once.

For details see [sk42042](http://supportcontent.checkpoint.com/solutions?id=sk42042).

**URL Filtering Enhancements**

This release improves the coverage and performance of Check Point's URL Filtering engine, focusing on hazardous and malicious websites.

Total Security customers that enable URL Filtering do not necessarily have to install this release, but it is recommended for improved URL Filtering results.

**Important** - During installation of the new URL Filtering engine, no default database is installed; therefore, the URL Filtering policy is not enforced until a signature update is performed. The first update may take several minutes, depending on your environment. Subsequent updates should take significantly less time, as only incremental information is downloaded.

**Eventia on VMware ESX Server**

Beginning with Check Point Suite R70, the Eventia Suite is supported on VMware ESX server version 3.5.
Supported Platforms and Versions

Builds

Table 1  Builds Included in this Release

<table>
<thead>
<tr>
<th>Component</th>
<th>Build Number</th>
<th>Command for Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Gateway</td>
<td>All Platforms: 079</td>
<td>fw ver -k</td>
</tr>
<tr>
<td>All Platforms: 079</td>
<td>IPSO: 080</td>
<td></td>
</tr>
<tr>
<td>Security Management server</td>
<td>030</td>
<td>fwm ver</td>
</tr>
<tr>
<td>Provider-1 MDS</td>
<td>730610033</td>
<td>cpvinfo $MDSDIR/lib/libmds.so</td>
</tr>
<tr>
<td>SmartConsole</td>
<td>730610136</td>
<td>Go to Help &gt; About Check Point SmartDashboard</td>
</tr>
<tr>
<td>MDG</td>
<td>730610018</td>
<td>Go to Help &gt; About Check Point Provider-1/SiteManager-1</td>
</tr>
<tr>
<td>SecurePlatform</td>
<td>097</td>
<td>ver</td>
</tr>
</tbody>
</table>

Security Products by Platform

Table 2  Management Products and Software Blades by Platform

<table>
<thead>
<tr>
<th>Software Blade / Product</th>
<th>Platform and Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point</td>
<td>Check Point</td>
</tr>
<tr>
<td>Check Point IPSO</td>
<td>Check Point IPSO Flash-based</td>
</tr>
<tr>
<td>Platform</td>
<td>Light 6.2 &amp; 6.0.7</td>
</tr>
<tr>
<td>Security Gateway</td>
<td>Windows Server 2003 (SP1-2) 32bit</td>
</tr>
<tr>
<td>Security Management</td>
<td>Windows Server 2008 (SP1-2) 32bit</td>
</tr>
<tr>
<td>Provider-1/SiteManager-1</td>
<td>Linux RHEL 5.0 kernel 2.6.18</td>
</tr>
<tr>
<td>Server (MDS)</td>
<td>Crossbeam X-Series</td>
</tr>
<tr>
<td>SmartWorkflow Blade</td>
<td>Solaris Ultra-SPARC 8.9.10</td>
</tr>
<tr>
<td>Performance Pack</td>
<td></td>
</tr>
<tr>
<td>ClusterXL (including third party clustering)</td>
<td>Third party only</td>
</tr>
</tbody>
</table>

Minimum System Requirements

The system requirements for R70.1 are the same as for R70. See the R70 Release Notes available at: http://supportcontent.checkpoint.com/documentation_download?ID=8712
Supported Upgrade Path

R70.1 must be installed on top of an R70 Security Management server, Provider-1 MDS, or Security Gateway. If you do not already have R70 installed, see the R70 Installation and Upgrade Guide at:

http://supportcontent.checkpoint.com/documentation_download?ID=8753

Note - Management servers prior to R70.1 cannot manage R70.1 Gateways. You must upgrade all Management servers to R70.1 before upgrading Security Gateways.

Important - Before upgrading a SecurePlatform gateway to R70 from R65 with HFA 40 or HFA 5 instructions in sk43247 (http://supportcontent.checkpoint.com/solutions?id=sk43247).

Required Disk Space

The tables below show the amount of disk space required to install R70.1 on a Management server and on a Security Gateway for each supported Operating System. Note that it is safe to delete the .tgz file after it is extracted in order to allow more disk space for installation.

Table 3  Required Disk Space for Installation on a Security Management Server or MDS

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Packed and Extracted .tgz File</th>
<th>Installation Size</th>
<th>Total Space Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSO6</td>
<td>/opt - 400 MB /opt - 360 MB</td>
<td>/opt - 760 MB</td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td>660 MB 450 MB</td>
<td>1110 MB</td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>350 MB 530 MB</td>
<td>880 MB</td>
<td></td>
</tr>
<tr>
<td>Solaris</td>
<td>520 MB 530 MB</td>
<td>1050 MB</td>
<td></td>
</tr>
</tbody>
</table>

Table 4  Required Disk Space for Installation on a Security Gateway

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Packed and Extracted .tgz File</th>
<th>Installation Size</th>
<th>Total Space Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSO6</td>
<td>/opt - 400 MB /opt - 360 MB</td>
<td>/opt - 760 MB</td>
<td></td>
</tr>
<tr>
<td>IPSO6 Diskless</td>
<td>/opt - 400 MB /opt - 230 MB /preserve - 400 MB</td>
<td>790 MB</td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>350 MB 230 MB</td>
<td>580 MB</td>
<td></td>
</tr>
</tbody>
</table>

* This total refers to the maximum disk space required before the user deletes the 195 MB of the Check_Point_R70.1.ipso6.tgz file after it is extracted.
Installing R70.1

In This Section:
- Installing on Power-1, UTM-1, SecurePlatform, or Linux page 8
- Installing on Provider-1 page 10
- Installing on IPSO page 10
- Installing on Windows page 11
- Installing on Solaris page 11
- Installing Using SmartUpdate page 12

Installing R70.1 must be installed on top of an R70 Security Management server, Provider-1 MDS, or Security Gateway. If you do not already have R70 installed, see the R70 Installation and Upgrade Guide at:
http://supportcontent.checkpoint.com/documentation_download?ID=8753

Note - R70.1 can be installed on a Security Gateway, Security Management server, or Provider-1 MDS. The procedure is the same for all.

You may want to backup your system before installing R70.1. On SecurePlatform, you can use snapshots. See Snapshot Image Management in the SecurePlatform/SecurPlatform Pro Administration Guide at:
http://supportcontent.checkpoint.com/documentation_download?ID=10107

Installing on Power-1, UTM-1, SecurePlatform, or Linux

Note - Installing R70.1 involves extracting a .tgz file to your Management server or Security Gateway. It is safe to delete the .tgz file once it has been extracted.

Installation Using Web User Interface (not on Linux)

You can use the SecurePlatform Web User Interface to install R70.1 on Check Point Power-1 and UTM-1 appliances or on open servers running SecurePlatform.

To install R70.1 on SecurePlatform (Power-1, UTM-1, or open-servers) using the Web User Interface:

2. Connect to the SecurePlatform WebUI:
   - On an open-server: https://<IP>
   - On Power-1 and UTM-1: https://<IP>:4434

3. Open the Upgrade page:
   - On an open-server: Device > Upgrade
   - On Power-1 and UTM-1: Appliance > Upgrade

4. Follow the on-screen instructions to complete the installation.

See “Installing the R70.1 SmartConsole or MDG” on page 13 for information on connecting to the upgraded machine from your GUI client.
Verifying Installation with SecurePlatform Web User Interface

Once you have installed R70.1, the login page of the Web User Interface will look like this:

To verify R70.1 installation through the SecurePlatform Web User Interface, make sure that R70.1 appears in the Build information, according to the platform type:

- On an open-server: **Status > Version and Build**
- On Power-1 and UTM-1: **Information > Appliance Status > Version and Build**

Installation Using CLI (not on Power-1 or UTM-1)

You can use the CLI to install R70.1 on SecurePlatform and Linux machines.

Linux RHEL does not support R70.1 Security Gateways. Security Management servers and Provider-1 MDSs are supported on Linux RHEL.

**Important** - The default idle timeout on SecurePlatform is ten minutes. After this time, the user is logged out. To ensure that installation is not interrupted by this timeout, before entering **expert** mode, type: `idle 120` in the command line.

To install the package on SecurePlatform or Linux using the CLI:


2. Verify that there is enough free disk space to install R70.1. See “Required Disk Space” on page 7 for details.

3. Create a new directory under `/var` on the target machine.

4. Download `Check_Point_R70.1.linux.tgz` from the Check Point Download Center, [http://supportcenter.checkpoint.com](http://supportcenter.checkpoint.com). Transfer the file to the new directory on the Security Management server, Security Gateway, or MDS using SFTP, SCP, or any other secure method.

5. Change to the new directory.

6. Extract the `.tgz` package by running the command:
   ```bash
tar -zxvf Check_Point_R70.1.linux.tgz
   ```

7. To start the installation, run:
   ```bash
./UnixInstallScript
   ```
8. Follow the on-screen instructions to install all of the components. When the installation completes, it says **succeeded** for each component. Follow the prompt to reboot the machine.

See "Installing the R70.1 SmartConsole or MDG" on page 13 for information on connecting to the upgraded machine from your GUI client.

**Installing on Provider-1**

Install R70.1 on all Provider-1 MDSs using the instructions for your platform in “Installing R70.1” on page 8. After installation, activate the **Workflow Blade** Plug-in on each CMA on which you want to enable SmartWorkflow.

To activate Plug-ins on a CMA:
1. In the MDG, right-click on a customer and select **Configure Customer**.
2. In the Customer Configuration window, select the **Plug-ins** tab.
3. Select each Plug-in you want to activate on the CMA and click **Add**.
4. Click **OK** to confirm changes.

**Installing on IPSO**

You can install R70.1 on IPSO and IPSO Diskless machines. Only Security Gateways on IPSO Diskless machines are supported. Security Management servers and MDSs are supported on other IPSO machines.

**Important** - Installation and uninstallation of R70.1 are only supported using the CLI and are **not** supported using Voyager. Using Voyager to install or uninstall the package may cause instability.

**Note** - Installing R70.1 involves extracting a .tgz file to your Management server or Security Gateway. It is safe to delete the .tgz file once it has been extracted.

1. Log in to the Security Management server or Security Gateway.
2. Verify that there is enough free disk space in the `/opt` directory to install R70.1. See “Required Disk Space” on page 7 for details.
3. Create a new directory under `/opt` on the target machine.
4. Download `Check_Point_R70.1.ipso6.tgz` from the Check Point Download Center, [http://supportcenter.checkpoint.com](http://supportcenter.checkpoint.com). Transfer the file to the new directory on the Security Management server, MDS, or Security gateway using SFTP, SCP, or any other secure method.
5. Change to the new directory.
6. Extract the .tgz package by running:
   ```sh
tar -zxvf Check_Point_R70.1.ipso6.tgz
   ```
7. To start the installation, run:
   ```sh
./UnixInstallScript
   ```
8. Follow the on-screen instructions to install all of the components. When the installation completes, it says **succeeded** for each component. Follow the prompt to reboot the machine.
See “Installing the R70.1 SmartConsole or MDG” on page 13 for information on connecting to the upgraded server from your GUI client.

Installing on Windows

Note: Installing R70.1 involves extracting a .tgz file to your Management server or Security Gateway. It is safe to delete the .tgz file once it has been extracted.

1. Log in to the Security Management server or Security Gateway.
2. Verify that there is enough free disk space to install R70.1. See “Required Disk Space” on page 7 for details.
4. Extract the .tgz package using an extraction utility.
5. Run the extracted executable file from the folder that was automatically created, using the command:
   setup.bat
6. Follow the on-screen instructions to install all of the R70.1 components. When the installation completes, it says succeeded for each component. Follow the prompt to reboot the machine.

See “Installing the R70.1 SmartConsole or MDG” on page 13 for information on connecting to the upgraded server from your GUI client.

Installing on Solaris

Note: Installing R70.1 involves extracting a .tgz file to your Management server or Security Gateway. It is safe to delete the .tgz file once it has been extracted.

R70.1 cannot be installed on Security Gateways on the Solaris Platform. It can be installed on a Security Management server or Provider-1 MDS running on Solaris.

2. Verify that there is enough free disk space in the /var directory to install R70.1. See “Required Disk Space” on page 7 for details.
3. Create a new directory under /var on the target machine.
4. Download Check_Point_R70.1.solaris2.tgz from the Check Point Download Center, http://supportcenter.checkpoint.com. Transfer the file to the new directory on the Security Management server or MDS using SFTP, SCP, or any other secure method.
5. Change to the new directory.
6. Extract the .tgz package by running:
   gunzip Check_Point_R70.1.solaris2.tgz
   The file extension changes to .tar
7. Run:
   `tar -xvf Check_Point_R70.1.solaris2.tar`

8. To start the installation, run:
   `./UnixInstallScript`

9. Follow the on-screen instructions to install all of the components. When the installation completes, it says succeeded for each component. Follow the prompt to reboot the machine.

   See "Installing the R70.1 SmartConsole or MDG" on page 13 for information on connecting to the upgraded server from your GUI client.

## Installing Using SmartUpdate

You can use SmartUpdate to remotely install R70.1 on SecurePlatform (open-server or appliance), Windows, and IPSO Security Gateways.

To install using SmartUpdate:

1. Install R70.1 on the Security Management server, using the Command Line or SecurePlatform Web User Interface.

2. Open SmartUpdate and make sure that SmartDashboard is closed.

3. Click Packages > Get Data from All.

   When the Operation Status of the known gateways is Done, the installed packages and their versions are listed.


5. Add the R70.1 .tgz file of each required gateway platform to the Package Repository (Packages > Add; or drag-and-drop).

   Wait until the Operation Status of adding the package is Done. The R70.1 package appears in the Package Repository.

6. Right-click the package and choose Distribute.

   The Distribute Package window opens.

7. Select the Security Gateways on which you want to install the package.

8. Click Distribute.

   The package is distributed to and installed on the selected Security Gateways. The gateways are rebooted automatically; except for Windows gateways, which must be rebooted manually.

   **Note** - If a Windows gateway does not accept traffic after installing the package, re-install the policy.
Installing the R70.1 SmartConsole or MDG

R70.1 requires the R70.1 SmartConsole installed on a GUI client. If you are using the Check Point Suite R70.1 on Provider-1, you also need the R70.1 MDG.

Installing the SmartConsole

R70.1 provides a new, streamlined functionality, that automatically upgrades the SmartConsole on your GUI client machine the first time you connect to an R70.1 Security Management server with an R70 SmartConsole.

Note - R70.1 SmartConsole and MDG can be installed on a machine along with other SmartConsole and MDG versions. You do not need to uninstall other SmartConsole or MDG versions installed on your GUI client machine.

You can also install SmartConsole manually by downloading Check_Point_SmartConsole_R70_1_Windows.exe from http://supportcenter.checkpoint.com. Extract the package and double-click setup.exe to run the SmartConsole.

Installing the MDG

To install the R70.1 MDG, download Check_Point_MDG_R70_1_Windows.exe from http://supportcenter.checkpoint.com. Extract the package and double-click setup.exe to run the MDG.

Uninstalling R70.1

In This Section:
- Uninstalling on SecurePlatform, Linux, IPSO, or Solaris page 13
- Uninstalling on Provider-1 page 14
- Uninstalling on Windows page 14
- Uninstalling SmartConsole R70.1 page 14

Uninstalling on SecurePlatform, Linux, IPSO, or Solaris

When uninstalling Check Point Suite R70.1, you must uninstall two separate packages.

Note - When uninstalling the R70.1 package from SecurePlatform, the SecurePlatform build number will not change because certain components remain installed on the operating system.

To uninstall Check Point Suite R70.1, perform the following steps on the Security Management server, MDS, or Security Gateway:

1. Change the directory to:
   /opt/CPUninstall/Check_Point_R70.1

2. Run:
   ./UnixInstallScript -u

3. Follow the on-screen instructions to finish uninstalling Check_Point_R70.1.
Uninstalling on Provider-1

To uninstall R70.1 in a Provider-1 deployment:

1. Deactivate the Workflow Plug-in in the Global SmartDashboard and on all CMAs.
   - To deactivate Plug-ins on a CMA:
     A. In the MDG, right-click on a customer and select Configure Customer.
     B. In the Customer Configuration window, select the Plug-ins tab.
     C. Select each Plug-in you want to deactivate on the CMA and click Remove.
     D. Click OK to confirm changes.

2. Uninstall R70.1 from the MDSs, using the instructions per platform in "Uninstalling R70.1" on page 13.

Uninstalling on Windows

**Important** - Do not use Add or Remove Programs to uninstall the package on Windows. It is not supported and may cause instability.

1. Go to:
   C:\Program Files\CheckPoint\CPUninstall\Check_Point_R70.1

2. Run:
   Setup.bat -u

3. Follow the on-screen instructions to finish uninstalling Check_Point_R70.1

4. Go to:
   C:\Program Files\CheckPoint\CPUninstall\R70_HFA_10

5. Run:
   Setup.bat -u

6. Follow the on-screen instructions to finish uninstalling R70_HFA_10.

Uninstalling SmartConsole R70.1

Use the Windows Add or Remove Programs tool to uninstall SmartConsole R70.1 and/or MDG. A screen with various options appears; select only Remove.
Known Limitations

Note - Known Limitations are published in the following SKs:

Managing Check Point Appliances Using the LCD Panel

Check Point appliances have an LCD panel that can be used to perform basic management operations. The management IP address, netmask, and default gateway of the Check Point appliance can be configured. The appliance can also be rebooted.

Menu options

<table>
<thead>
<tr>
<th>Menu</th>
<th>Sub-menu</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>DHCP</td>
<td>Enable or disable IP address allocation using DHCP</td>
</tr>
<tr>
<td></td>
<td>Set Internal IP or Set Mgmt IP</td>
<td>Set the management interface IP address (cannot be edited when DHCP is enabled)</td>
</tr>
<tr>
<td></td>
<td>Set Netmask</td>
<td>Set the management interface network mask (cannot be edited when DHCP is enabled)</td>
</tr>
<tr>
<td></td>
<td>Set Default GW</td>
<td>Set the management interface default gateway (cannot be edited when DHCP is enabled)</td>
</tr>
<tr>
<td>System</td>
<td>Reboot</td>
<td>Reboot the appliance</td>
</tr>
</tbody>
</table>

LCD Panel Keys

<table>
<thead>
<tr>
<th>To</th>
<th>Press</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the main menu</td>
<td>ENTER</td>
</tr>
<tr>
<td>Navigate the menu</td>
<td>▲ or ▼</td>
</tr>
<tr>
<td>Select a menu option</td>
<td>ENTER</td>
</tr>
<tr>
<td>Go back to previous menu</td>
<td>▲</td>
</tr>
</tbody>
</table>

When Entering an IP Address

<table>
<thead>
<tr>
<th>To</th>
<th>Press</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move to the next digit</td>
<td>▲</td>
</tr>
<tr>
<td>Move back to the previous digit</td>
<td>▼</td>
</tr>
<tr>
<td>Approve the change</td>
<td>ENTER when cursor is located on the last digit</td>
</tr>
<tr>
<td>Cancel the IP change</td>
<td>ENTER when cursor is located on the first digit</td>
</tr>
<tr>
<td>Change current digit</td>
<td>▲ or ▼</td>
</tr>
</tbody>
</table>
Related Resources

For related documentation and other resources, see the R70.1 Homepage at sk41810, http://supportcontent.checkpoint.com/solutions?id=sk41810.