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=11648](http://supportcontent.checkpoint.com/documentation_download?ID=11648)
For additional technical information, visit the Check Point Support Center ([http://supportcenter.checkpoint.com](http://supportcenter.checkpoint.com)).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 March 2011</td>
<td>Additional improvements to the chapter: Advanced Security Management Server Upgrade and Database Migration (on page 89)</td>
</tr>
<tr>
<td>13 January 2011</td>
<td>Improved Installation and Advanced Upgrade procedures</td>
</tr>
<tr>
<td>15 December 2010</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 R75 Installation and Upgrade Guide](mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on R75 Installation and Upgrade Guide)).
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>9</td>
</tr>
<tr>
<td>Welcome</td>
<td>9</td>
</tr>
<tr>
<td>R75 Documentation</td>
<td>9</td>
</tr>
<tr>
<td>For New Check Point Customers</td>
<td>9</td>
</tr>
<tr>
<td>Getting Started</td>
<td>10</td>
</tr>
<tr>
<td>Downloading R75</td>
<td>10</td>
</tr>
<tr>
<td>Terminology</td>
<td>10</td>
</tr>
<tr>
<td>Multi-Domain Security Management Glossary</td>
<td>11</td>
</tr>
<tr>
<td>Compatibility Tables</td>
<td>12</td>
</tr>
<tr>
<td>Licensing</td>
<td>12</td>
</tr>
<tr>
<td>Software Licensing</td>
<td>12</td>
</tr>
<tr>
<td>Licensing Multi-Domain Security Management</td>
<td>13</td>
</tr>
<tr>
<td>Licensing SmartEvent</td>
<td>13</td>
</tr>
<tr>
<td>Installing</td>
<td>14</td>
</tr>
<tr>
<td>Installing Security Gateways, Security Management and Endpoint Security</td>
<td>15</td>
</tr>
<tr>
<td>Introduction</td>
<td>15</td>
</tr>
<tr>
<td>Installation on SecurePlatform</td>
<td>16</td>
</tr>
<tr>
<td>Installing SecurePlatform Using the DVD</td>
<td>16</td>
</tr>
<tr>
<td>Installing SecurePlatform using the CLI</td>
<td>16</td>
</tr>
<tr>
<td>Installing Gateway &amp; Management Features</td>
<td>17</td>
</tr>
<tr>
<td>Installing Endpoint Security</td>
<td>18</td>
</tr>
<tr>
<td>Completing the Installation</td>
<td>18</td>
</tr>
<tr>
<td>Installation on Solaris or Linux</td>
<td>19</td>
</tr>
<tr>
<td>Installing Security Management servers</td>
<td>19</td>
</tr>
<tr>
<td>Installing Endpoint Security</td>
<td>20</td>
</tr>
<tr>
<td>Completing the Installation</td>
<td>20</td>
</tr>
<tr>
<td>Installation on IPSO</td>
<td>21</td>
</tr>
<tr>
<td>Installing the R75 Package</td>
<td>21</td>
</tr>
<tr>
<td>Initial Configuration</td>
<td>22</td>
</tr>
<tr>
<td>Installation on Windows</td>
<td>22</td>
</tr>
<tr>
<td>Installing Gateway &amp; Management Features</td>
<td>23</td>
</tr>
<tr>
<td>Installing Endpoint Security</td>
<td>24</td>
</tr>
<tr>
<td>Completing the Installation</td>
<td>24</td>
</tr>
<tr>
<td>Post-Installation Configuration</td>
<td>25</td>
</tr>
<tr>
<td>Logging In for the First Time</td>
<td>25</td>
</tr>
<tr>
<td>Where to Go From Here</td>
<td>26</td>
</tr>
<tr>
<td>Installing Multi-Domain Security Management</td>
<td>27</td>
</tr>
<tr>
<td>Overview</td>
<td>27</td>
</tr>
<tr>
<td>Basic Architecture</td>
<td>27</td>
</tr>
<tr>
<td>Multi-Domain Security Management Glossary</td>
<td>28</td>
</tr>
<tr>
<td>Creating the Multi-Domain Security Management Environment</td>
<td>30</td>
</tr>
<tr>
<td>Setting Up Multi-Domain Security Management Networking</td>
<td>30</td>
</tr>
<tr>
<td>Installing the Gateways</td>
<td>30</td>
</tr>
<tr>
<td>Installing the Multi-Domain Server</td>
<td>30</td>
</tr>
<tr>
<td>Installing SmartConsole and SmartDomain Manager Clients</td>
<td>33</td>
</tr>
<tr>
<td>Using the SmartDomain Manager for the First Time</td>
<td>33</td>
</tr>
<tr>
<td>Launching the SmartDomain Manager</td>
<td>33</td>
</tr>
<tr>
<td>Managing Licenses Using SmartUpdate</td>
<td>34</td>
</tr>
<tr>
<td>Adding Licenses using the SmartDomain Manager</td>
<td>35</td>
</tr>
<tr>
<td>Demo Mode</td>
<td>36</td>
</tr>
</tbody>
</table>
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where To From Here?</td>
<td>36</td>
</tr>
<tr>
<td><strong>Installing SmartEvent and SmartReporter</strong></td>
<td>36</td>
</tr>
<tr>
<td>SmartEvent and SmartReporter Planning</td>
<td>36</td>
</tr>
<tr>
<td>Standalone Deployment</td>
<td>36</td>
</tr>
<tr>
<td>Distributed Deployment</td>
<td>37</td>
</tr>
<tr>
<td>Log Server Configuration</td>
<td>37</td>
</tr>
<tr>
<td>Security Management Server Configuration</td>
<td>37</td>
</tr>
<tr>
<td>SmartEvent and SmartReporter Configuration</td>
<td>38</td>
</tr>
<tr>
<td>Multi-Domain Security Management Deployment</td>
<td>38</td>
</tr>
<tr>
<td>Log Server Configuration</td>
<td>38</td>
</tr>
<tr>
<td>Defining Log Servers as Global Servers</td>
<td>39</td>
</tr>
<tr>
<td>Defining the Reporting or SmartEvent Server as a Local Server</td>
<td>39</td>
</tr>
<tr>
<td><strong>Installing SmartEvent Intro</strong></td>
<td>40</td>
</tr>
<tr>
<td>SmartEvent Intro Planning</td>
<td>40</td>
</tr>
<tr>
<td>Standalone Deployment</td>
<td>40</td>
</tr>
<tr>
<td>Distributed Deployment</td>
<td>41</td>
</tr>
<tr>
<td>Multi-Domain Security Management Deployment</td>
<td>41</td>
</tr>
<tr>
<td><strong>Installing Mobile Access</strong></td>
<td>43</td>
</tr>
<tr>
<td>Mobile Access Overview</td>
<td>43</td>
</tr>
<tr>
<td>Mobile Access Installation</td>
<td>43</td>
</tr>
<tr>
<td>The Mobile Access Wizard</td>
<td>44</td>
</tr>
<tr>
<td>Step 1: Configure a Web Application</td>
<td>44</td>
</tr>
<tr>
<td>Step 2: Configure Authorized Users</td>
<td>44</td>
</tr>
<tr>
<td>The Mobile Access Wizard is Complete</td>
<td>45</td>
</tr>
<tr>
<td>Results of Enabling Mobile Access</td>
<td>45</td>
</tr>
<tr>
<td>Upgrading from Connecta to Mobile Access</td>
<td>45</td>
</tr>
<tr>
<td><strong>Installing and Configuring DLP</strong></td>
<td>47</td>
</tr>
<tr>
<td>DLP and Privacy</td>
<td>47</td>
</tr>
<tr>
<td>DLP Requirement Notes</td>
<td>48</td>
</tr>
<tr>
<td>Installing the DLP gateway</td>
<td>48</td>
</tr>
<tr>
<td>Configuring SecurePlatform using the WebUI</td>
<td>48</td>
</tr>
<tr>
<td>Configuring SecurePlatform using the CLI</td>
<td>49</td>
</tr>
<tr>
<td>Where To From Here?</td>
<td>49</td>
</tr>
<tr>
<td><strong>Installing IPS-1 Sensors</strong></td>
<td>50</td>
</tr>
<tr>
<td>Overview of IPS-1</td>
<td>50</td>
</tr>
<tr>
<td>IPS-1 System Architecture</td>
<td>50</td>
</tr>
<tr>
<td>IPS-1 Sensor Deployment</td>
<td>50</td>
</tr>
<tr>
<td>Installing and Configuring IPS-1 Sensors</td>
<td>51</td>
</tr>
<tr>
<td>Installing IPS-1 Sensors with SecurePlatform</td>
<td>51</td>
</tr>
<tr>
<td>Configuring IPS-1 Sensors</td>
<td>52</td>
</tr>
<tr>
<td>Post-Configuration Steps</td>
<td>53</td>
</tr>
<tr>
<td>Where To From Here?</td>
<td>55</td>
</tr>
<tr>
<td><strong>Upgrading</strong></td>
<td>56</td>
</tr>
<tr>
<td><strong>Introduction to the Upgrade Process</strong></td>
<td>57</td>
</tr>
<tr>
<td>Contract Verification</td>
<td>57</td>
</tr>
<tr>
<td>Terminology</td>
<td>57</td>
</tr>
<tr>
<td>Upgrade Tools</td>
<td>58</td>
</tr>
<tr>
<td>Upgrading Successfully</td>
<td>58</td>
</tr>
<tr>
<td><strong>Service Contract Files</strong></td>
<td>59</td>
</tr>
<tr>
<td>Introduction</td>
<td>59</td>
</tr>
<tr>
<td>Working with Contract Files</td>
<td>59</td>
</tr>
<tr>
<td>Installing a Contract File on Security Management server</td>
<td>59</td>
</tr>
<tr>
<td>On a Windows Platform</td>
<td>59</td>
</tr>
<tr>
<td>On SecurePlatform, Linux, and Solaris</td>
<td>60</td>
</tr>
<tr>
<td>On IPSO</td>
<td>61</td>
</tr>
<tr>
<td>Installing a Contract File on a Gateway</td>
<td>61</td>
</tr>
<tr>
<td>On a Windows Platform</td>
<td>61</td>
</tr>
<tr>
<td>On SecurePlatform</td>
<td>62</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Restoring Your Original Environment</td>
<td>126</td>
</tr>
<tr>
<td>Changing the Multi-Domain Server IP Address and External Interface</td>
<td>126</td>
</tr>
<tr>
<td>IP Address Change</td>
<td>126</td>
</tr>
<tr>
<td>Interface Change</td>
<td>126</td>
</tr>
<tr>
<td>IPS with Multi-Domain Security Management</td>
<td>127</td>
</tr>
<tr>
<td><strong>Upgrading SmartLSM Security (ROBO) Gateways</strong></td>
<td>128</td>
</tr>
<tr>
<td>Planning the ROBO Gateway Upgrade</td>
<td>128</td>
</tr>
<tr>
<td>ROBO Gateway Upgrade Package to SmartUpdate Repository</td>
<td>128</td>
</tr>
<tr>
<td>License Upgrade for a Security Gateway ROBO Gateway</td>
<td>129</td>
</tr>
<tr>
<td>Using SmartProvisioning to Attach the Upgraded Licenses</td>
<td>129</td>
</tr>
<tr>
<td>License Upgrade on Multiple ROBO Gateways</td>
<td>129</td>
</tr>
<tr>
<td>Upgrading a ROBO Gateway Using SmartProvisioning</td>
<td>129</td>
</tr>
<tr>
<td>Upgrading a Security Gateway ROBO Gateway</td>
<td>129</td>
</tr>
<tr>
<td>Upgrading a UTM-1 Edge ROBO Gateway</td>
<td>130</td>
</tr>
<tr>
<td>Upgrading a Security Gateway ROBO Gateway In Place</td>
<td>131</td>
</tr>
<tr>
<td>Using the Command Line Interface</td>
<td>131</td>
</tr>
<tr>
<td>SmartLSM Upgrade Tools</td>
<td>131</td>
</tr>
<tr>
<td>Upgrading a Security Gateway ROBO Gateway Using LSMcli</td>
<td>132</td>
</tr>
<tr>
<td>Upgrading a UTM-1 Edge ROBO Gateway Using LSMcli</td>
<td>133</td>
</tr>
<tr>
<td>Using the LSMcli in Scripts</td>
<td>134</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>137</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

In This Chapter

Welcome 9
R75 Documentation 9
For New Check Point Customers 9

Welcome

Thank you for choosing Check Point software blades for your security solution. We hope that you will be satisfied with this solution and our support services. Check Point products provide your business with the most up to date and secure solutions available today.

Check Point also delivers worldwide technical services including educational, professional, and support services through a network of Authorized Training Centers, Certified Support Partners, and Check Point technical support personnel to ensure that you get the most out of your security investment.

To extend your organization’s growing security infrastructure and requirements, we recommend that you consider adopting the OPSEC platform (Open Platform for Security). OPSEC is the industry's open, multi-vendor security framework, which has over 350 partners and the largest selection of best-of-breed integrated applications and deployment platforms.

For additional information on the Internet Security Product Suite and other security solutions, go to: http://www.checkpoint.com or call Check Point at 1(800) 429-4391. For additional technical information, visit the Check Point Support center (http://supportcenter.checkpoint.com).

Welcome to the Check Point family. We look forward to meeting all of your current and future network, application, and management security needs.

R75 Documentation

This guide is intended for administrators responsible for installing and upgrading Check Point security products on the corporate network.

Technical documentation is available on your DVD. These documents can also be found at the Check Point Support Center (http://supportcenter.checkpoint.com). To find out about what's new in R75, refer to the R75 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=11647).

For New Check Point Customers

New Check Point customers can access the Check Point User Center (http://usercenter.checkpoint.com) to:

- Manage users and accounts
- Activate products
- Get support offers
- Open service requests
- Search the Technical Knowledge Base
Chapter 2

Getting Started

This chapter contains information and terminology related to installing R75.
Before you install or upgrade to R75, you must read the R75 Release Notes. (http://supportcontent.checkpoint.com/documentation_download?ID=11647)

In This Chapter

Downloading R75 10
Terminology 10
Multi-Domain Security Management Glossary 11
Compatibility Tables 12
Licensing 12

Downloading R75

You can get the R75 software in the official media pack, or you can download the software images from the Support Center (http://supportcenter.checkpoint.com).

- The media pack includes DVDs that can install on any supported operating system.
- The Support Center includes different DVD images for each operating system.
- To use a DVD image from the Support Center, download a DVD image and burn it to a DVD.

Terminology

These terms are used throughout this chapter:

- **Distributed Deployment**: When the gateway and the Security Management server are installed on separate machines.
- **Gateway**: The software component that enforces the organization’s security policy and acts as a security enforcement point.
- **Security Policy**: The policy created by the system administrator that regulates the flow of incoming and outgoing communication.
- **Security Management server**: The server used by the system administrator to manage the security policy. The organization's databases and security policies are stored on the Security Management server and downloaded to the gateway.
- **SmartConsole**: GUI applications that are used to manage various aspects of security policy enforcement. For example, SmartView Tracker is a SmartConsole application that manages logs.
- **SmartDashboard**: A SmartConsole GUI application that is used by the system administrator to create and manage the security policy.
- **Standalone Deployment**: When Check Point components responsible for the management of the security policy (the Security Management server and the gateway) are installed on the same machine.
# Multi-Domain Security Management Glossary

This glossary includes product-specific terms used in this guide.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Security administrator with permissions to manage elements of a Multi-Domain Security Management deployment.</td>
</tr>
<tr>
<td>Global Policy</td>
<td>Policies that are assigned to all Domains, or to specified groups of Domains.</td>
</tr>
<tr>
<td>Global Objects</td>
<td>Network objects used in global policy rules. Examples of global objects include hosts, global Domain Management Servers, and global VPN communities.</td>
</tr>
<tr>
<td>Internal Certificate Authority (ICA)</td>
<td>Check Point component that authenticates administrators and users. The ICA also manages certificates for Secure Internal Communication (SIC) between Security Gateways and Multi-Domain Security Management components.</td>
</tr>
<tr>
<td>Multi-Domain Security Management</td>
<td>Check Point centralized management solution for large-scale, distributed environments with many different network Domains.</td>
</tr>
<tr>
<td>Domain</td>
<td>A network or group of networks belonging to a specified entity, such as a company, business unit or organization.</td>
</tr>
<tr>
<td>Multi-Domain Server</td>
<td>Multi-Domain Security Management server that contains all system information as well as the security policy databases for individual Domains.</td>
</tr>
<tr>
<td>Multi-Domain Log Server</td>
<td>Physical log server that hosts the log database for all Domains.</td>
</tr>
<tr>
<td>Domain Log Server</td>
<td>Virtual log server for a specified Domain.</td>
</tr>
<tr>
<td>Primary Multi-Domain Server</td>
<td>The first Multi-Domain Server that you define and log into in a High Availability deployment.</td>
</tr>
<tr>
<td>Secondary Multi-Domain Server</td>
<td>Any subsequent Multi-Domain Server that you define in a High Availability deployment.</td>
</tr>
<tr>
<td>Active Multi-Domain Server</td>
<td>The only Multi-Domain Server in a High Availability deployment from which you can add, change or delete global objects and global policies. By default, this is the primary Multi-Domain Server. You can change the active Multi-Domain Server.</td>
</tr>
<tr>
<td>Standby Multi-Domain Server</td>
<td>All other Multi-Domain Servers in a High Availability deployment, which cannot manage global policies and objects. Standby Multi-Domain Servers are synchronized with the active Multi-Domain Server.</td>
</tr>
<tr>
<td>Active Domain Management Server</td>
<td>In a High Availability deployment, the only Domain Management Server that can manage a specific Domain.</td>
</tr>
<tr>
<td>Standby Domain Management Server</td>
<td>In a High Availability deployment, any Domain Management Server for a specified Domain that is not designated as the active Domain Management Server.</td>
</tr>
</tbody>
</table>
Compatibility Tables

If the existing Check Point implementation contains products that are not supported by R75, the installation process terminates. For a list of compatible products by platform, refer to the R75 Release Notes (http://supportcontent.checkpoint.com/documentation_download?id=11647).

Licensing

Most of the software on this DVD is automatically enabled for a 15-day evaluation period. To obtain a permanent license, or to extend the evaluation period, visit the Check Point User Center (http://usercenter.checkpoint.com).

Customers new to Check Point User Center should visit the Check Point User Center (http://usercenter.checkpoint.com).

For further licensing assistance, contact Account Services (mailto:AccountServices@checkpoint.com). Or call: US +1 972-444-6600, option 5.

Software Licensing

Starting with version R71, customers are required to use Software Blade licenses. If you have not yet migrated to Software Blade licenses, follow the migration options from Check Point’s website (http://www.checkpoint.com/products/promo/software-blades/upgrade/index.html).

From R71, the software license enforcement module checks that users have current Software Blade Licensing. Users that have installed R71 software using NGX based licenses and not Software Blade licenses, will receive warnings on the Security Gateways and SmartDashboard.

Licenses are required for the Security Management server and security gateways. No license is required for SmartConsole management clients.

Check Point gateways enforce the installed license by counting the number of users that have accessed the gateway. If the maximum number of users is reached, warning messages are sent to the console.

Check Point software is activated using a certificate key, located on the back of the software media pack. The certificate key is used to generate a license key for products that you want to evaluate or purchase. To purchase Check Point products, contact your reseller.

Obtaining a License Key

To obtain a license key from the Check Point User Center:

1. Add the required Check Point products/evaluations to your User Center account by selecting Accounts & Products > Add Products.
2. Generate a license key for your products/evaluations by selecting Accounts & Products > Products. Select your product(s) and click Activate License. The selected product(s) evaluations have been assigned license keys.
3. Complete the installation and configuration process by doing the following:
   a) Read and accept the End Users License Agreement.
   b) Import the product license key. Licenses are imported using the Check Point Configuration Tool or SmartUpdate. SmartUpdate allows you to centrally upgrade and manage Check Point software and licenses. The certificate keys associate the product license with the Security Management server, which means that:
      - The new license remains valid even if the IP address of the Security Gateway changes.
      - Only one IP address is needed for all licenses.
      - A license can be detached from one Security Gateway and assigned to another.
Upgrading Licenses

The upgrade procedure is free of charge to purchasers of the Software Subscription service (Enterprise Base Support).

Licensing Multi-Domain Security Management

Multi-Domain Security Management licenses are associated with the IP address of the licensed entity. The Multi-Domain Server license is based on the server type: Multi-Domain Server or Multi-Domain Log Server.

Multi-Domain Log Servers: A comprehensive license that includes all Log Servers that it hosts. A Domain Log Server hosted on a Multi-Domain Log Server does not need its own license. A standalone Domain Log Server on a Multi-Domain Server requires a license.

Each gateway requires its own license. Licenses are determined according to the number of computing devices (nodes) protected by the gateway. Multi-Domain Security Management licenses can be imported using the Check Point command-line licensing tool or the SmartDomain Manager. See the R75 Multi-Domain Security Management Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11683).

Licensing SmartEvent

SmartEvent licenses are installed on the SmartEvent server and not on the Security Management Server. Correlation Units are licensed by the number of units that are attached to the SmartEvent server.
Installing
Chapter 3

Installing Security Gateways, Security Management and Endpoint Security

In This Chapter

Introduction 15
Installation on SecurePlatform 16
Installation on Solaris or Linux 19
Installation on IPSO 21
Installation on Windows 22
Post-Installation Configuration 25
Logging In for the First Time 25
Where to Go From Here 26

Introduction

Check Point software runs on many platforms and pre-configured appliances. Each installation differs depending on the product and the platform.

There are two different deployment scenarios:

- **Standalone Deployment**: The management server (Security Management server or Multi-Domain Security Management) is installed on the same computer as the Security Gateway.
- **Distributed Deployment**: The Security gateway and the management server (Security Management server or Multi-Domain Security Management) are installed on different computers.

For more information, see Upgrading a Distributed Deployment (on page 65) or Upgrading a Standalone Deployment (on page 85). For information about supported platforms and operating systems, see the R75 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=11647).

⚠️ **Important** - If you are using a VSX deployment, you cannot upgrade your VSX Gateways or VSX clusters to R75.

To install VSX Gateways or clusters in an R75 deployment, see (http://supportcontent.checkpoint.com/documentation_download?ID=10166). For compatibility information, see (http://supportcontent.checkpoint.com/documentation_download?ID=11647).

You can manage VSX R67 using R75 SmartConsole and R75 SmartDomain Manager.

⚠️ **Note** - You must install, configure and activate the TCP/IP network protocol before you run the installation program.
Installation on SecurePlatform

In this section:

- Installing SecurePlatform Using the DVD 16
- Installing SecurePlatform using the CLI 16
- Installing Gateway & Management Features 17
- Installing Endpoint Security 18
- Completing the Installation 18

Installing SecurePlatform Using the DVD

To install on SecurePlatform using the DVD:

1. Put the installation DVD into the drive and boot the computer from the DVD.
2. When the boot screen shows, press Enter to continue. You must press Enter in 90 seconds, or the computer will try to boot from the hard drive.
3. If error messages show during the hardware compatibility scan, correct the problems and then restart the procedure from step 1.
4. When the SecurePlatform Installation screen opens, do these optional steps if necessary. Select OK to continue with the installation.
   - **Device List**: Select to open the Hardware Scan Details window, which includes options for saving the hardware scan results. This is useful for resolving hardware compatibility issues.
   - **Add Driver**: Select to install a device driver from a floppy disk. Use this option only in consultation with Technical Support.
5. In the Keyboard Selection window, select a keyboard language and then select OK.
6. From the Networking Device window, select an interface to be the management interface and then select OK.
7. In the Network Interface Configuration window, define these settings for the management interface and then select OK:
   - IP address
   - Net mask
   - Default gateway
8. In the HTTPS Server Configuration window, activate or deactivate web-based connections to the WebUI. Define an IP port (default is 443) to connect to the WebUI client. Select OK.
   - **Note**: If you are going to deploy remote access or Endpoint Security software, you must select a port other than the default value (443).
9. Select OK to format your hard drive and install SecurePlatform.
   - **Important**: This action deletes all data on your hard drive.

The installation program can run for a long time.

10. When the Complete window opens, remove the DVD and press Enter to reboot.

When the computer reboots, you can configure SecurePlatform and install Check Point Software Blades and products.

Installing SecurePlatform using the CLI

When the computer finishes rebooting, do these steps to configure SecurePlatform:

1. Log in with the user name: admin and password: admin.
2. When prompted, change and confirm the password. You can also change the user name at this time.
4. In the **Network Configuration** menu, do these steps as required:
   a) Select **Host Name**. Do the instructions on the screen to enter and see the host name.
   b) Select **Domain Name**. Do the instructions on the screen to enter and see the domain name.
   c) Select **Domain Name Servers**. Do the instructions on the screen to enter and see DNS.
   d) Select **Network Connections**. Do the instructions on the screen to configure network interfaces (connections) as required:
      (i) **Add new connection** - Add a new interface.
      (ii) **Configure connection** - Configure an existing interface.
      (iii) **Remove connection** - Delete an interface.
      (iv) **Select management connection** - Select the management interface. By default, this is the interface that you selected during installation.
      (v) **Show connection configuration** - Make sure that the network interface configuration is correct.
   e) Select **Routing**. Do the instructions on the screen to define and see the default gateway.

5. In the **Time and Date Configuration** menu, do the instructions on the screen to configure these settings:
   - Time zone
   - Date
   - Time

6. Press **n** to continue.

## Installing Gateway & Management Features

This procedure installs your Security Management Servers and related features.

1. To import a product configuration file from a TFTP server, enter **1** and do the instructions on the screen. Otherwise, press **n** to continue.
2. In the **Welcome** window, press **N** to continue.
3. Read the End User License agreement and press **Y** to accept the terms.
4. In the next window, do these steps:
   - Select **New Installation** if this is a new product installation.
   - Select **Installation Using Imported Configuration** to use the installation file imported in step 1.
   - Press **N** to continue.
5. Select the Check Point products and features to install and press **N** to continue.
6. If you are installing a gateway in distributed deployment, do these steps:
   a) Press **y** if this gateway uses a dynamically assigned IP address or **n** if it uses static IP address.
   b) Press **y** if this gateway using a Check Point cluster product or **n** if it does not.
   c) Go directly to the Completing the Installation procedure ("Completing the Installation" on page 18). Do not continue with this procedure.
7. If you selected **Security Management Server**, select one of these options:
   - Installation as a primary Security Management Server.
   - Installation as a secondary Security Management Server.
   - Installation as a Log server (without the Security Management Server component).
   Press **N** to continue.
8. In the **SmartEvent** window, select the SmartEvent components to install and press **N** to continue:
   - SmartReporter
   - SmartEvent
   - SmartEvent Correlation Unit
9. If you are also installing Endpoint Security, select an installation option and then press **N** to continue:
• Primary Endpoint Security Server.
• Secondary Endpoint Security Server.
• Connection Point.

If you selected a **Security Management Server** and an **Endpoint Security Server** in step 5, you must select **Primary Endpoint Server**.

10. If you are installing Endpoint Security, continue with the Endpoint Security installation procedures. Otherwise, go directly to the Completing the Installation procedure ("Completing the Installation" on page 18).

For Security Gateways, IP forwarding is automatically disabled and a default security policy is enforced. This default policy blocks all inbound connections, except for control connections. This policy remains in place until you install a new security policy.

### Installing Endpoint Security

If you are installing Security Management Server, do these steps:

1. Press **Enter** to scroll through and read the Endpoint Security license. Press **Y** to accept the license and continue.
2. Enter a fully qualified path to the installation directory or press **Enter** to accept the default location.
3. **In the Endpoint Security Server Type** window, select an option and then press **N** to continue:
   - **Primary Endpoint Security Server**.
   - **Secondary Endpoint Security Server**.
   - **Connection Point**.
   If you selected a **Security Management Server** and an **Endpoint Security Server**, install the Endpoint Security server as a Primary Endpoint Security server.
4. Press **Enter** to confirm your selection.
5. Press **Enter** to accept the default IP address, as defined during the initial configuration. You can enter a different IP address if necessary.
6. Enter the host name or press **Enter** to accept the default value (as defined during the initial configuration). Press **1** to confirm your selections or **2** to change them.
7. Select **Single** or **Multiple** domains. Press **1** to confirm your selections or **2** to change it.
8. Enter and confirm the master administrator password. Press **1** to confirm your selections or **2** to change it.
9. If prompted, make sure the ports 8080, 8009, 80, 443 and 2100 are available for use with Endpoint Security. If there is a port issue:
   a) Exit the installation program.
   b) Resolve all port issues. If there is an issue with port 443, try reinstalling SecurePlatform from the start. Make sure that you define a port other than 443 in the **HTTPS Server Configuration** window.
   c) Rerun the installation program and scroll through the configuration screens until you get to this step.
10. Press **Enter** to continue.
11. Continue with the Completing the Installation procedure ("Completing the Installation" on page 18).

### Completing the Installation

Do these instructions on the screen to complete the installation. The steps that you do can be different, based on the products and features that you are installing.

1. In the **Configuring Licenses and Contracts** screen, press **y** to manually enter licenses now. Press **n** to enter your licenses later (recommended) using SmartUpdate or the WebUI.
2. Enter and confirm the SIC trust activation code (Distributed deployment Security Gateways only).
3. Do the instructions on the screen to add administrators (Security Management server only).
4. Do the instructions on the screen to add GUI clients (Security Management server only).
5. For Windows installations, click **Next** on the **Certificate Authority** page.
6. Optionally, save the certificate fingerprint to a text file (Security Management server only).
7. Press **Enter** (for Windows, click **Finish**) to complete the installation and configuration.
8. Reboot the computer.

### Installation on Solaris or Linux

You install Security Management Servers on Solaris or Linux using the command line.

1. If you are installing a Security Management Server, do the instructions on the screen to configure:
   a) Licenses
   b) Administrators (name and password)
   c) GUI clients
   d) A random pool of data for cryptographic operations
   e) A Certificate authority and saving the fingerprint

2. Press **E** to complete the installation.

3. Log out and then log in again as the root administrator.

4. Run `cpstart`.

IP forwarding is automatically disabled and a default security policy is installed on the gateway. The default Security Policy blocks all inbound connections, except for control connections such as install policy operations. This policy remains in effect until you have installed the first security policy.

In this section:

- Installing Security Management servers
- Installing Endpoint Security
- Completing the Installation

### Installing Security Management servers

To install on a Linux or Solaris platform:

1. Mount the DVD on the specified subdirectory.
2. From the DVD mount point directory, run:
   ```bash
   ./UnixInstallScript
   ```
3. When the **welcome** screen opens, press **N** to continue.
4. Read and accept the terms of the **End User License Agreement**.
5. Select **New Installation** and press **N** to continue.
6. Select the products to install and press **N** to continue.
7. If you selected **Security Management Server**, select one of these options and press **N** to continue:
   - Installation as a primary Security Management Server.
   - Installation as a secondary Security Management Server.
   - Installation as a log server (without the Security Management Server component).
8. In the **SmartEvent** window, select the SmartEvent components to install and press **N** to continue:
   - SmartReporter
   - SmartEvent
   - SmartEvent Correlation Unit
9. If you are also installing Endpoint Security, do these steps:
   a) Select an installation option and then press **N** to continue:
      - Primary Endpoint Security Server.
      - Secondary Endpoint Security Server.
      - Connection Point.
If you selected a **Security Management Server** and an **Endpoint Security Server** in step 6, select **Primary Endpoint Security server**.

10. In the **Validation** window, Press **Enter** to continue.
    The installation program installs the specified products and components.

11. If you are installing Endpoint Security, continue with the Endpoint Security installation ("Installing Endpoint Security" on page 18) procedure. If not, continue to the Completing the Installation procedure ("Completing the Installation" on page 18).

### Installing Endpoint Security

If you are installing Security Management Server, do these steps:

1. Press **Enter** to scroll through and read the Endpoint Security license. Press **Y** to accept the license and continue.
2. Enter a fully qualified path to the installation directory or press **Enter** to accept the default location.
3. **In the Endpoint Security Server Type** window, select an option and then press **N** to continue:
   - **Primary Endpoint Security Server**.
   - **Secondary Endpoint Security Server**.
   - **Connection Point**.
   If you selected a **Security Management Server** and an **Endpoint Security Server**, install the Endpoint Security server as a Primary Endpoint Security server.
4. Press **Enter** to confirm your selection.
5. Press **Enter** to accept the default IP address, as defined during the initial configuration. You can enter a different IP address if necessary.
6. Enter the host name or press **Enter** to accept the default value (as defined during the initial configuration). Press **1** to confirm your selections or **2** to change them.
7. Select **Single** or **Multiple** domains. Press **1** to confirm your selections or **2** to change it.
8. Enter and confirm the master administrator password. Press **1** to confirm your selections or **2** to change it.
9. If prompted, make sure the ports 8080, 8009, 80, 443 and 2100 are available for use with Endpoint Security. If there is a port issue:
   a) Exit the installation program.
   b) Resolve all port issues. If there is an issue with port 443, try reinstalling SecurePlatform from the start. Make sure that you define a port other than 443 in the **HTTPS Server Configuration** window.
   c) Rerun the installation program and scroll through the configuration screens until you get to this step.
10. Press **Enter** to continue.
11. Continue with the Completing the Installation procedure ("Completing the Installation" on page 18).

### Completing the Installation

Do these instructions on the screen to complete the installation. The steps that you do can be different, based on the products and features that you are installing.

1. In the **Configuring Licenses and Contracts** screen, press **y** to manually enter licenses now. Press **n** to enter your licenses later (recommended) using SmartUpdate or the WebUI.
2. Enter and confirm the SIC trust activation code (Distributed deployment Security Gateways only).
3. Do the instructions on the screen to add administrators (Security Management server only).
4. Do the instructions on the screen to add GUI clients (Security Management server only).
5. For Windows installations, click **Next** on the **Certificate Authority** page.
6. Optionally, save the certificate fingerprint to a text file (Security Management server only).
7. Press **Enter** (for Windows, click **Finish**) to complete the installation and configuration.
8. Reboot the computer.
Installation on IPSO

This section gives procedures for installing R75 on an IPSO appliance.

In this section:

- Installing the R75 Package
- Initial Configuration

Installing the R75 Package

To install a new R75 package using Network Voyager:
1. Download the applicable release package for your platform to an FTP site or to your local disk.

   **Important** - Installing the incorrect package can damage your platform.

<table>
<thead>
<tr>
<th>IP Appliance Platform type</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk based</td>
<td>IPSO6_wrapper_R75.tgz (<a href="http://supportcenter.checkpoint.com/file_download?id=11773">http://supportcenter.checkpoint.com/file_download?id=11773</a>)</td>
</tr>
<tr>
<td>Flash based</td>
<td>Check_Point_R75_Security_Gateway_for_IPSO6_2.tgz (<a href="http://supportcenter.checkpoint.com/file_download?id=11772">http://supportcenter.checkpoint.com/file_download?id=11772</a>)</td>
</tr>
</tbody>
</table>

   **Note** - This package does not include CPinfo. See sk30567 (http://supportcontent.checkpoint.com/solutions?id=sk30567) for download information.

2. Log in to your appliance using Network Voyager.
3. In the Network Voyager tree, select **Configuration > System Configuration > Packages > Install Package**.
4. Upload the package file using one of these methods:
   - **Upload from an FTP site**:
     (i) In the Voyager Install Package window, select FTP.
     (ii) Enter the name or IP address of the FTP server.
     (iii) Enter the path to the directory on the FTP server where the packages are stored.
     (iv) If necessary, enter the applicable user name and password.
     (v) Click **Apply**. The names of the available packages show in the Site Listing window.
     (vi) Select the package .tgz file in the Site Listing window and click **Apply**.
     (vii) When the `<package name> downloaded to` message shows, click it and then click **Apply** again.
   - **Upload from a local disk**:
     (i) In the Voyager Install Package window, select **Upload**.
     (ii) Click **Browse** and navigate to the package .tgz file.
     (iii) Click **Apply**.
     (iv) Select the package .tgz file in the Unpack Package window and click **Apply**.
5. Click the **Click here to install/upgrade** link to continue with the installation.
6. In the **Package Installation and Upgrade** pane, select **Install** and then click **Apply**.
7. Click the **Install Package** branch in the Voyager tree to see the installation progress.
8. Go to the **Manage Packages** page.
Installation on Windows

- The R75 and Check Point CPInfo packages are automatically activated during installation (disk-based appliances only).
- Enable other packages, with the compatibility packages, as needed for your deployment.

**Important** - When you install a package using Network Voyager, this message shows:

```
Voyager environment has been updated with the latest package info.
The telnet session environment will be updated by:
logging out and logging in again the telnet session.
```

This message can be misleading. Click **Manage Packages** to verify that the package is actually installed correctly. Refresh the page periodically until you see that the installation is complete.

9. Log out of Network Voyager and then log in again.

**Initial Configuration**

Do these steps to configure your server for the first time:

1. From the IPSO command line, run `cpconfig`.
2. Read and accept the license agreement.
3. Select one of these installation types:
   - **Standalone** - Install a Security Management server and a Security Gateway on this computer. You can also install a log server.
   - **Distributed** - Install a Security Management server or a Security Gateway on this computer.
4. If you selected a Distributed installation, do the instructions on the screen to select the components to install.
5. On the **Configuring Licenses and Contracts** pane, press `n` to enter your licenses later (recommended) using SmartUpdate or the WebUI.
6. Do the instructions on the screen to add administrators and their passwords (Security Management server only).
7. Do the instructions on the screen to add GUI clients (Security Management server only).
8. Do the instructions on the screen to configure permissions.
9. Enter an administrator group name or press **Enter** to accept the default value (superuser). Do the instructions on the screen.
10. Optionally, save the certificate fingerprint to a text file (Security Management server only).
11. Press **Enter** to complete the installation and configuration.
12. Reboot the computer when prompted.
13. After you reboot, define and install a policy for this Security Management server.

**Installation on Windows**

You use the Windows GUI to install Security Gateways and Security Management server. T
Installing Gateway & Management Features

To Install R75 on a Windows platform:
1. Log in to Windows using Administrator credentials.
2. Put the installation DVD in the drive.
   The installation wizard starts automatically.
3. Click Next in the Thank you window.
4. Accept the terms of the License Agreement and click Next.
5. Select one of these installation options:
   - New installation
   - Installation using imported configuration
   Click Next.
6. If you selected Installation using imported configuration, select the location of the imported configuration file and click Next.
   a) Select an option for obtaining the latest upgrade utilities and click Next.
   b) Go to step 10.
      For more information, see Advanced Upgrade on a Windows Platform.
7. If you selected New Installation, select the installation type:
   - Typical - includes two options:
     ▪ Security Management and SmartConsole - Installs and automatically configures Security Management, SmartReporter, Correlation Unit and SmartConsole. This is the standard distributed deployment.
     ▪ Security Management, Security Gateway and SmartConsole - Installs and automatically configures Security Management, SmartReporter, Correlation Unit, Security Gateway and SmartConsole. This is the standard standalone deployment.
     Note - Both typical installation options include compatibility packages that support:
     - Check Point Security Gateway 80 Series
     - Check Point UTM-1 Edge
     - Check Point NGX R65
     - Check Point R70.x and R71.x
   - Custom - Lets you select components to install and configure.
     1. Click Next.
     2. If you selected one of the Typical options, a list of the components that will be installed shows. Click Next and go to step 10.
     3. For Custom installations, select the components to install:
        - Security Gateway
        - Security Management server
        Note - If you select the Security Management server:
        * If you select Security Management server but do not select SmartEvent and SmartReporter, Security Management Blades will be automatically installed together with Security Management.
        * If you do not select Security Management but select SmartEvent and SmartReporter Suite, Security Management will be installed and configured by default as a Log Server.
        - SmartEvent and SmartReporter
        - SmartConsole clients
        - Endpoint Security
        - Management Portal.
     4. Select a destination folder to install the components and click Next.
Installation on Windows

Note - If required version of the Microsoft.Net framework has not been installed on the target computer, the installation program installs it automatically before installing the Check Point components.

5. If prompted, select the Security Management Server type.
6. If prompted, select the SmartEvent and Reporter Suite server types.
7. If you are installing Endpoint Security, go directly to the Installing Endpoint Security section ("Installing Endpoint Security" on page 24). Otherwise, review your selections, and click Next.

Installing Endpoint Security

If you are installing Endpoint Security, do these steps. If not, go directly to the Completing the Installation section.

1. If the Endpoint Security Server Installation screen appears, click Next.
   The server type selection is done later in this procedure.
2. Select Standalone Installation or Distributed Installation:
   - Standalone Installation: Endpoint Security and the management server (Security Management server or Multi-Domain Security Management) are installed on the same computer.
   - Distributed Installation: Endpoint Security and the management server (Security Management server or Multi-Domain Security Management) are installed on different computers.
3. Review your selections, and click Next to continue.
4. Accept the license agreement and click Next to continue.
5. In the Endpoint Security Installation window, select one of these server types:
   - Primary Endpoint Security Server.
   - Secondary Endpoint Security Server.
   - Connection Point.
   If you selected a Security Management Server and an Endpoint Security Server, install the Endpoint Security server as a Primary Endpoint Security server. Click Next to continue.
6. Enter the Endpoint Security server IP address and host name, or press Enter to accept the default values.
7. Select a domain option, and Click Next to continue.
   - Single Domain: Single domain Endpoint Security installations can have only one domain segment for all administrators, user directories, and policies.
   - Multiple Domains: Multiple domain Endpoint Security installations can have multiple data segments for different administrators, user directories, and policies.
8. Enter a Master Administrator password and confirm it. The default log in name is masteradmin. Click Next to continue.
   If you are using RADIUS authentication, enter the password used by the RADIUS server for this account.
9. Review your selections, and click Next to continue.
10. Click Install to continue the installation.
11. Click Done, when the Installation completed successfully message shows.

Completing the Installation

Do these instructions on the screen to complete the installation. The steps that you do can be different, based on the products and features that you are installing.

1. In the Configuring Licenses and Contracts screen, press y to manually enter licenses now. Press n to enter your licenses later (recommended) using SmartUpdate or the WebUI.
2. Enter and confirm the SIC trust activation code (Distributed deployment Security Gateways only).
3. Do the instructions on the screen to add administrators (Security Management server only).
4. Do the instructions on the screen to add GUI clients (Security Management server only).
5. For Windows installations, click Next on the Certificate Authority page.
6. Optionally, save the certificate fingerprint to a text file (Security Management server only).
7. Press Enter (for Windows, click Finish) to complete the installation and configuration.
8. Reboot the computer.

Post-Installation Configuration

You can use the Check Point configuration tool (cpconfig) to configure settings after installation:

- **Licenses and Contracts**: Add or delete licenses for the Security Management server and Security Gateways.
- **Administrators**: Define administrators with Security Management server access permissions. These administrators must have Read/Write permissions to create the first security policy.
- **GUI Clients**: Define client computers that can connect to the Security Management server using SmartConsole clients.
- **Certificate Authority**: Starts the Internal Certificate Authority, which allows connections between the Security Management server and gateways. For Windows, you must define the name of the ICA host. You can use the default name or define your own. The ICA name must be in the host name.domain format, for example, ica.checkpoint.com.
- **Fingerprint**: Save the certificate fingerprint when you log in to SmartConsole clients for the first time.

Logging In for the First Time

You connect to the Security Management server using SmartDashboard or other SmartConsole clients. Security Management server authenticates the connection when you log in for the first time.


To log in to SmartConsole clients:
1. Open SmartDashboard or another SmartConsole client.
2. Enter the Security Management server host name or IP address.
3. Use one of these authentication steps:
   - Select **User Name** and enter an administrator name and password.
   - Select **Certificate** and then select or navigate the specified certificate.
4. Optionally, select the **Read Only** option. You cannot change settings in the read only mode. This lets you connect to the Security Management server while other administrators are connected.
5. Optionally, click the **More Options** link for more connection options.
   - **Change Password** - Lets you to change the certificate password.
   - **Session Description**: Current session description. This information shows in the SmartView Tracker Audit Mode.
   - **Use compressed connection** - Optimizes the connection to Security Management server (activated by default). For very large databases, you can deactivate this option to maximize Security Management server throughput.
   - **Always select Read Only by default** - Sets the default log mode in to Read Only. This prevents SmartDashboard from showing the last administrator and Security Management server logged in to.
   - **Demo Mode Version**: Select a release version to use with the demo mode.
6. Click **OK** to log in.
7. If necessary, manually authenticate the connection using the fingerprint generated during installation.

Note - This only occurs the first time you log in from a specific client computer.
Where to Go From Here

You have learned the basics necessary to get started. Your next step is to get more advanced knowledge of your Check Point software. Check Point documentation is available in PDF format on the Check Point DVD and the Technical Support download site (http://supportcenter.checkpoint.com).

For more technical information about Check Point products, go to SecureKnowledge. (http://supportcenter.checkpoint.com)
Chapter 4

Installing Multi-Domain Security Management

In This Chapter

Overview 27
Creating the Multi-Domain Security Management Environment 30
Using the SmartDomain Manager for the First Time 33
Where To From Here? 36

Overview

Multi-Domain Security Management is a centralized management solution for large-scale, distributed environments with many different network Domains. This best-of-breed solution is ideal for enterprises with many subsidiaries, branches, partners and networks. Multi-Domain Security Management is also an ideal solution for managed service providers, cloud computing providers, and data centers.

Centralized management gives administrators the flexibility to manage polices for many diverse entities. Security policies should be applicable to the requirements of different departments, business units, branches and partners, balanced with enterprise-wide requirements.

Basic Architecture

Multi-Domain Security Management uses tiered architecture to manage Domain network deployments.

- The Security Gateway enforces the security policy to protect network resources.
- A Domain is a network or group of networks belonging to a specified entity, such as a company, business unit, department, branch, or organization. For a cloud computing provider, one Domain can be defined for each customer.
- A Domain Management Server is a virtual Security Management Server that manages security policies and Security Gateways for a specified Domain.
- The Multi-Domain Server is a physical server that hosts the Domain Management Server databases and Multi-Domain Security Management system databases.
- The SmartDomain Manager is a management client that administrators use to manage domain security and the Multi-Domain Security Management system.
The Multi-Domain Servers and SmartDomain Manager are typically located at central **Network Operation Centers** (NOCs). Security Gateways are typically located together with protected network resources, often in another city or country.

<table>
<thead>
<tr>
<th>Callout</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>USA Development Domain</td>
</tr>
<tr>
<td>B</td>
<td>Headquarters Domain</td>
</tr>
<tr>
<td>C</td>
<td>UK Development Domain</td>
</tr>
<tr>
<td>1</td>
<td>Security Gateway</td>
</tr>
<tr>
<td>2</td>
<td>Network Operation Center</td>
</tr>
<tr>
<td>3</td>
<td>Multi-Domain Server</td>
</tr>
<tr>
<td>4A</td>
<td>USA Development Domain Management Server</td>
</tr>
<tr>
<td>4B</td>
<td>Headquarters Domain Management Server</td>
</tr>
<tr>
<td>4C</td>
<td>UK Development Domain Management Server</td>
</tr>
</tbody>
</table>

**Multi-Domain Security Management Glossary**

This glossary includes product-specific terms used in this guide.
<table>
<thead>
<tr>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Administrator</strong></td>
</tr>
<tr>
<td><strong>Global Policy</strong></td>
</tr>
<tr>
<td><strong>Global Objects</strong></td>
</tr>
<tr>
<td><strong>Internal Certificate Authority (ICA)</strong></td>
</tr>
<tr>
<td><strong>Multi-Domain Security Management</strong></td>
</tr>
<tr>
<td><strong>Domain</strong></td>
</tr>
<tr>
<td><strong>Multi-Domain Server</strong></td>
</tr>
<tr>
<td><strong>Domain Management Server</strong></td>
</tr>
<tr>
<td><strong>Multi-Domain Log Server</strong></td>
</tr>
<tr>
<td><strong>Domain Log Server</strong></td>
</tr>
<tr>
<td><strong>Primary Multi-Domain Server</strong></td>
</tr>
<tr>
<td><strong>Secondary Multi-Domain Server</strong></td>
</tr>
<tr>
<td><strong>Active Multi-Domain Server</strong></td>
</tr>
<tr>
<td><strong>Standby Multi-Domain Server</strong></td>
</tr>
<tr>
<td><strong>Active Domain Management Server</strong></td>
</tr>
<tr>
<td><strong>Standby Domain Management Server</strong></td>
</tr>
</tbody>
</table>
Creating the Multi-Domain Security Management Environment

This section explains how to provision a Multi-Domain Security Management environment.

Installation Workflow

- Setting Up Multi-Domain Security Management Networking
- Installing the Gateways
- Installing the Multi-Domain Server
- Installing SmartConsole and SmartDomain Manager Clients

Setting Up Multi-Domain Security Management Networking

The Multi-Domain Server and Domain Security Gateway computers should be ready to connect to the network. The Multi-Domain Server must have at least one interface with a routable IP address. It also must be able to query a DNS server and resolve other network components.

Make sure that you configure routing to allow IP communication between:

- Domain Management Server, Domain Log Server and their Domain Security Gateways.
- All Multi-Domain Servers in the deployment.
- The Domain Management Server and Log Servers for the same Domain.
- The Domain Management Server and its High Availability Domain Management Server peer.
- The SmartDomain Manager clients and Multi-Domain Servers.
- The SmartDomain Manager clients and Log Servers.

Installing the Gateways

Install the Network Operation Center (NOC) and Domain gateways ("Installing Security Gateways, Security Management and Endpoint Security" on page 15) using R75 DVD.

Installing the Multi-Domain Server

The next step is to install the primary Multi-Domain Server on a dedicated computer. You can install the primary Multi-Domain Server on a SecurePlatform, Linux or Solaris platform. The first Multi-Domain Server that you install and log on to is known as the Primary Multi-Domain Server.

If you are creating a multi-Multi-Domain Server deployment, repeat these steps for each secondary Multi-Domain Server.

Installing SecurePlatform

To install SecurePlatform for the primary Multi-Domain Server:

1. Put the Multi-Domain Security Management CD in the drive and boot the computer. The computer boots directly from the CD.
2. At the welcome screen, press Enter to start the installation.
   - The installation program does a hardware compatibility test.
   - If you receive an incompatibility message, select Device List to show the incompatible devices. Upgrade or replace the devices as necessary. For more compatibility information, see the R75 Release Notes.
• If it is necessary to install drivers on your computer, select **Drivers** and do the instructions on the screen.

3. In the **Keyboard Selection** window, select a keyboard language from the list.

4. If your computer has more than one interface, select the management interface in the **Networking Device** window. Typically this is `eth0`.

5. In the **Network Interface Configuration** window, enter the IP address, net mask, and default gateway IP address.

6. In the **Confirmation** window, select **OK**.

The installation program does these tasks:

- Formats the hard disk.
- Installs the packages.
- Runs post installation scripts.

The installation program runs for about 10 minutes, after which the **Installation Complete** message shows.

7. Remove the `<media>` and select **OK**. The computer reboots automatically.

### Configuring SecurePlatform

After the computer reboots, do these steps

1. Log in using `'admin'` as the user name and password.

2. When prompted, change the password.

3. In the **Welcome** screen, press `'n'` to continue.

4. On the **Network Configuration** screen, select **Host Name**.

5. Select **Set host name**, and then enter a host name for the Multi-Domain Server.

   This name cannot include spaces or special characters.

6. When prompted, enter the host IP address or press **Enter** to configure the IP address in the **Network Connections** step (recommended).

7. Press **Enter** when prompted and then press **e** to go back to the **Main** menu.

8. Select the **Network Connections** screen to configure your interfaces and network connections. Do the instructions on the screen.

   When finished, press **e** as many times as necessary and then press **n** to continue the configuration.

9. In the **Time and Date** screen, do the instructions on the screen to set the time zone, time and date.

   Select **Show date and time settings** to make sure that the date and time is correct.

10. Enter **y** to start the Multi-Domain Server installation.

### Pre-Installation Tasks - Linux

**To install the Multi-Domain Server on a Linux platform:**

1. Install and configure the Linux operating system as necessary.

2. Log in as the root user or another user with superuser privileges.

3. Insert and mount the installation CD.

4. From mount directory, go to the `linux/ pl_install` subdirectory.

5. Run `/mds_setup` to start the Multi-Domain Server installation.

### Pre-Installation Tasks - Solaris

**To prepare the Linux or Solaris Platform for installation:**

1. Install the Solaris operating system (If necessary).

2. Log in as a root user or another user with superuser privileges.

3. Insert and mount the distribution CD.

4. From the mounted directory, go to the `solaris2` directory.
5. Run `./mds_setup`, to continue with Installing and Configuring Multi-Domain Security Management.

**Multi-Domain Server Installation Procedure**

Use this procedure to install these Multi-Domain Server types:

- Primary Multi-Domain Server
- Secondary Multi-Domain Server
- Standalone log servers (Domain Log Server or Multi-Domain Log Servers)

**To Install a Multi-Domain Server:**

1. In the welcome screen, enter **yes** to continue.
2. Select the **Multi-Domain Server** type.

   **Notes:**
   - You must install the **Primary Multi-Domain Server** first.
   - You can install a Secondary Multi-Domain Server or a Multi-Domain Log Servers later.

1. When prompted, enter **yes** if you are installing a **Primary Multi-Domain Server**. If not, enter **no**.

   **Note** - You cannot change this installation setting later. You can change any data that you enter after this stage using the `mdsconfig` utility.

2. At the **Are you sure** prompt, enter **yes** to continue.
3. Enter **yes** to start the Multi-Domain Server automatically after installation.
4. After the packages install and then press **Enter** when to continue.

**Configuring the Multi-Domain Server**

The installation program continues with several configuration steps.

1. When prompted, press the space bar to scroll through the license agreement. When finished, press **y** to accept the license agreement.
2. If there is more than one interface on your Multi-Domain Server, select one interface that connects Domain Management Servers to their managed networks and gateways. You can only have one interface for this purpose.
3. At the **Configuring Licenses** prompt, enter **n** to continue using the 15 day trial license.
   
   We recommend that you get and attach your licenses when configuring Multi-Domain Security Management with the SmartDomain Manager.
4. At the **Configuring Groups** prompt, optionally assign an operating system user group with file system and command line access permissions.
   
   Press **Enter** and then press **y** to assign the **root** user group by default.
5. Press **Enter** to initialize the Certificate Authority.
6. Optionally, press **y** to save the certificate fingerprint to a file.
7. Define at least one Multi-Domain Security Management administrator.
   
   You must define the first administrator as a **Multi-Domain Security Management Superuser**. You can optionally add this administrator to a group.
   
   You can define additional administrators now. However, we recommend that you use the SmartDomain Manager to do this at a later time.
8. Do the instructions on the screen to define at least one GUI client to manage this Multi-Domain Server.
9. When prompted, press **Enter** to complete the installation.
10. Reboot the Multi-Domain Server.
Installing SmartConsole and SmartDomain Manager Clients

This section contains procedures for installing the SmartConsole and SmartDomain Manager clients on Windows platforms.

Installing SmartConsole

To install the SmartConsole clients on Windows platforms:
1. Insert the MD_DVD disk.
2. Open the Linux\windows folder.
3. Double-click the SmartConsole executable.
4. Do the instructions on the screen.

Installing the SmartDomain Manager

To install the SmartDomain Manager package:
1. Insert the MD_DVD disk.
2. Open the Linux\windows folder.
3. Double-click the Prov1Gui executable.
4. Do the instructions on the screen.

Uninstalling Multi-Domain Security Management

To uninstall a Multi-Domain Server on SecurePlatform
1. Back up the databases if you want to reinstall the Multi-Domain Server on this or another computer.
2. Reformat the hard disk or re-install a Multi-Domain Server from the DVD.

To uninstall a Multi-Domain Server on Linux or Solaris:
1. Back up the databases if you want to reinstall the Multi-Domain Server on this or another computer.
2. Run: mds_remove

To uninstall the SmartDomain Manager and SmartConsole applications:
- Use Add/Remove Programs to uninstall the clients.

Using the SmartDomain Manager for the First Time

Use the SmartDomain Manager to configure and manage the Multi-Domain Security Management deployment. Make sure that you have installed SmartDomain Manager on a trusted GUI Client. You must be an administrator with appropriate privileges (Superuser, Global Manager, or Domain Manager) to run the SmartDomain Manager.

Launching the SmartDomain Manager

To start the SmartDomain Manager:
1. Click Start > Programs > Check Point SmartConsole > SmartDomain Manager.
2. Enter your User Name and Password, or browse to your Certificate and enter the password.
3. Enter the Multi-Domain Server computer name or IP address.
   - The SmartDomain Manager connects to the Multi-Domain Server.
   - Your user name permissions are resolved.
• The SmartDomain Manager opens, displaying all network objects and menu commands that you have permission to work with.

Managing Licenses Using SmartUpdate

To manage licenses using SmartUpdate, select the **SmartUpdate** view in the SmartDomain Manager Selection Bar. If you loaded SmartUpdate, you can also right-click a Multi-Domain Server object and select **Applications > SmartUpdate** from the Options menu. Licenses for components and blades are stored in a central repository.

**To view repository contents:**
1. Select SmartUpdate from the SmartDomain Manager Main menu.
2. Select **SmartUpdate > Network Objects License & Contract > View Repository**. The repository pane shows in the SmartUpdate view.

**To add new licenses to the repository:**
1. Select SmartUpdate from the SmartDomain Manager Main menu.
2. Select **SmartUpdate > Network Objects License & Contract > Add License**.
3. Select a method for adding a license:
   - **From User Center** - Obtain a license file from the User Center.
   - **From file** - Import a license file to the repository.
   - **Manually** - Open the **Add License** window and enter licenses information manually. You can copy the license string from a file and click **Paste License** to enter the data.

You can now see the license in the repository.

**To attach a license to a component:**
1. Select SmartUpdate from the SmartDomain Manager Main menu.
2. Select **SmartUpdate > Network Objects License & Contract > Attach License**.
3. Select a license from the **Attach Licenses** window. The license shows as attached in the repository.

You can do a variety of other license management tasks using SmartUpdate. Refer to the **R75 Security Management Administration Guide** ([http://supportcontent.checkpoint.com/documentation_download?ID=11667](http://supportcontent.checkpoint.com/documentation_download?ID=11667)) for details.
Adding Licenses using the SmartDomain Manager

To add a license to a Multi-Domain Server or Multi-Domain Log Server using the SmartDomain Manager:

1. In the SmartDomain Manager, open the General View > Multi-Domain Server Contents page.
2. Double-click a Multi-Domain Server or Multi-Domain Log Server. The Multi-Domain Server Configuration window opens.
3. Open the License tab.
4. Install licenses using Fetch or Add:
   a) Click Fetch License File.
   b) In the Open window, browse to and double-click the desired license file.
   Add License Information Manually
   a) Click Add.
b) In the email message that you received from Check Point, select the entire license string (starting with `cplic putlic...` and ending with the last SKU/Feature) and copy it to the clipboard.

c) In the Add License window, click Paste License to paste the license details you have saved on the clipboard into the Add License window.

d) Click Calculate to display your Validation Code. Compare this value with the validation code that you received in your email. If validation fails, contact the Check Point licensing center, providing them with both the validation code contained in the email and the one displayed in this window.

**Demo Mode**

You can open the SmartDomain Manager in Demo mode. This mode does not require authentication or a connection to the Multi-Domain Server. Use Demo mode to experiment with different objects, views, modes and features before you create a real system. It demonstrates several pre-configured sample Domains, Domain Management Servers, Security Gateways and policies.

Operations performed in Demo mode are stored in a local database. So you can continue a Demo session from the point at which you left off in a previous session.

**Where To From Here?**

Check Point documentation provides additional information and is available in PDF format on the Check Point DVD as well as on the Check Point Support Center (http://supportcenter.checkpoint.com).

**Installing SmartEvent and SmartReporter**

The following sections present procedures for installation and initial configuration of the SmartEvent Software Blade and the SmartReporter Software Blade. The specific procedures vary according to different deployment scenarios.

**SmartEvent and SmartReporter Planning**

The SmartEvent Software Blade uses two components: a SmartEvent server, and a SmartEvent Correlation unit. The SmartReporter Software Blade uses the SmartReporter server. All three components can reside on a Security Management Server or dedicated Log server. You can also install some components on a Security Management server and some components on a dedicated Log server, to distribute the load. In a Multi-Domain Security Management deployment, the three components must be installed on one or more dedicated Log servers, and not on the Multi-Domain Security Management Multi-Domain Server.

**Standalone Deployment**

In a standalone deployment, all components of the SmartEvent and SmartReporter Software Blades are installed on a Security Management Server.

**To configure SmartEvent and SmartReporter Software Blades on a standalone Security Management Server:**

   - In Windows, you must select the Custom installation option.
2. After you complete the installation, install the SmartEvent and SmartReporter Blade license.
   - If you do not yet have a license, you will automatically receive a 15-day trial.
5. In the Management blade tab, select one or more of these Software Blades to enable them on the standalone Security Management Server:
   - SmartReporter
   - SmartEvent Server
   - SmartEvent Correlation Unit
6. Save the changes.
7. Select Policy > Install Database to install the database on the Security Management Server.
8. Run evstop and then evstart.
9. To configure SmartEvent to correlate logs, connect to the Security Management Server using the SmartEvent client.
   a) Select the Policy tab.
   b) In the navigation tree, select General Settings > Initial Settings > Correlation Units.
   c) Click Add to add the servers defined as SmartEvent Correlation Units.
   d) In the Correlation Unit window, add the log servers that contain logs for correlation. Repeat this step for each Correlation Unit.
   If Correlation Units do not appear in the list, wait until object synchronization finishes. The Status of Object Synchronization can be seen in the Overview tab.
10. If you have installed SmartReporter, connect to the Security Management Server using the SmartReporter client.
    a) In the SmartReporter client, click Management, located by default in the bottom left-hand corner of the screen,
    b) Select Consolidation > Sessions > Create New.
    c) In the New Consolidation Session window, add consolidation sessions for all log servers. If log servers do not appear in the list, wait until the Object Synchronization process finishes.
    d) Configure and schedule reports as required.
    e) Install the Event Policy by selecting Actions > Install Event Policy.

Distributed Deployment
A SmartEvent distributed deployment has SmartEvent and the Correlation Units installed on different servers.

Log Server Configuration
To configure SmartEvent on a dedicated log server:
1. install a SmartEvent license on the log server.
2. On the dedicated log server, run evconfig and follow the on-screen instructions to configure the log server to enable and configure these components:
   - SmartReporter
   - SmartEvent
   - SmartEvent Correlation Unit
3. Run evstop and then evstart.

Security Management Server Configuration
To configure the SmartEvent object:
2. If you have not yet defined a Security Management Server host network object, do so now.
4. On the General Properties page, select the Management tab, enable one or more of these Software Blades:
   - SmartReporter
   - Event Correlation - SmartEvent Server
   - Correlation Unit
   Enable other <tp_blades> as necessary.
5. Save the changes.
6. Select Policy > Install Database to install the database on all Security Management Servers.

**SmartEvent and SmartReporter Configuration**

The following steps apply to installations on new server machines. If you have previously installed these applications, you can safely skip these steps.

To configure SmartEvent and SmartReporter do one of these procedures:

If you have installed a SmartEvent server or a Correlation Unit, or both, on this log server, connect to the log server using the SmartEvent client and do the following:

1. Select the Policy tab.
2. In the navigation tree, select General Settings > Initial Settings > Correlation Units.
3. Click Add to add those servers defined as Correlation Units.
4. In the Correlation Unit window, add the log servers associated with the Correlation Unit. Repeat this step for each Correlation Unit.
   - If Correlation Units do not appear in the list, wait until object synchronization finishes. The Status of Object Synchronization can be seen in the Overview tab.

If you have installed SmartReporter on this log server, connect to the log server using the SmartReporter client and perform the following:

1. In the SmartReporter client, click Management, located by default in the bottom left-hand corner of the screen,
2. Select Consolidation > Sessions > Create New.
3. In the New Consolidation Session window, add consolidation sessions for all log servers. If log servers do not appear in the list, wait until the Object Synchronization process finishes.
4. Configure and schedule reports as required.
5. Install the Event Policy by selecting Actions > Install Event Policy.

**Multi-Domain Security Management Deployment**

In a Multi-Domain Security Management environment, these Software Blades must be on one or more dedicated Log servers, not on a Multi-Domain Server or Multi-Domain Log Server. The dedicated Log servers do not host log files, which remain on the Multi-Domain Log Server.

- SmartReporter
- SmartEvent Server
- Event Correlation

**Log Server Configuration**

To configure SmartEvent on a dedicated log server:
1. install a SmartEvent license on the log server.
2. On the dedicated log server, run `evconfig` and follow the on-screen instructions to configure the log server to enable and configure these components:
• SmartReporter
• SmartEvent
• SmartEvent Correlation Unit

3. Run `evstop` and then `evstart`.

Defining Log Servers as Global Servers

To define a log server as a Multi-Domain Security Management global object:
1. Connect to the Multi-Domain Server using the global SmartDashboard:
2. Define the dedicated log server as Global object.
3. In the **General Properties** page of the Security Management server Global object, in the **Management** tab, select the components you want to run on that server.
4. Establish SIC trust with the Multi-Domain Server.
5. Save and **Install Global Policy** an all relevant Domain Management Servers.
6. If you installed the Correlation Unit on one or more separate Log servers, perform the following steps:
   a) Create or open host network object for each log server hosting a Correlation Unit.
   b) On the **General Properties** page for each, select the **Correlation Unit** blade.
   c) Save and assign the Global Policy to all relevant Domain Management Servers.
7. If you installed a SmartEvent server and/or SmartEvent Correlation Unit on the log server, connect to the log server using the SmartEvent client.
   a) Select the **Policy** tab.
   b) In the navigation tree, select **General Settings > Initial Settings > Correlation Units**.
   c) Click **Add** to add those servers defined as Correlation Units.
   d) In the **Correlation Unit** window, add the log servers associated with the Correlation Unit. Repeat this step for each Correlation Unit.
   If Correlation Units do not appear in the list, wait until object synchronization finishes. The **Status of Object Synchronization** can be seen in the **Overview** tab.
8. If you have installed SmartReporter on this log server, connect to the log server using the SmartReporter client.
   a) In the SmartReporter client, click Management, located by default in the bottom left-hand corner of the screen,
   b) Select **Consolidation > Sessions > Create New**.
   c) In the **New Consolidation Session** window, add consolidation sessions for all log servers. If log servers do not appear in the list, wait until the Object Synchronization process finishes.
   d) Configure and schedule reports as required.
   e) Install the Event Policy by selecting **Actions > Install Event Policy**.

Defining the Reporting or SmartEvent Server as a Local Server

To define the server as a Local server:
1. Connect using SmartDashboard to the Domain Management Server that manages the dedicated log server
2. Create or open a dedicated log server object.
3. On the **General Properties** page of the Security Management server object, select the **Management** blades tab, select the components you want to run on that computer. Enable any or all of the following **Software Blades** according to your deployment:
   • SmartReporter
   • Event Correlation - SmartEvent Server
   • Correlation Unit.
4. Establish SIC with the Domain Management Server, and click OK.
5. Save changes.
6. Select Policy > Install Database and install the database on all management objects.
7. If you installed a SmartEvent server and/or a Correlation Unit on this log server, connect to the log server using the SmartEvent client.
   a) Select the Policy tab.
   b) In the navigation tree, select General Settings > Initial Settings > Correlation Units.
   c) Click Add to add those servers defined as Correlation Units.
   d) In the Correlation Unit window, add the log servers associated with the Correlation Unit. Repeat this step for each Correlation Unit.

If Correlation Units do not appear in the list, wait until object synchronization finishes. The Status of Object Synchronization can be seen in the Overview tab.
8. If you installed SmartReporter on this log server, connect to the log server using the SmartReporter client.
   a) In the SmartReporter client, click Management, located by default in the bottom left-hand corner of the screen,
   b) Select Consolidation > Sessions > Create New.
   c) In the New Consolidation Session window, add consolidation sessions for all log servers. If log servers do not appear in the list, wait until the Object Synchronization process finishes.
   d) Configure and schedule reports as required.
   e) Install the Event Policy by selecting Actions > Install Event Policy.
9. Install the Event Policy on the Correlation Units.

Installing SmartEvent Intro

The following sections present procedures for installation and initial configuration of the SmartEvent Intro Software Blade and its associated processes. The specific procedures vary according to different deployment scenarios.

SmartEvent Intro Planning

SmartEvent Intro uses two components: the SmartEvent Intro server and the Event Correlation Unit. Both components can be installed on the same or separate computers. The default configuration and recommended deployment is that each Log server is used as an Event Correlation Unit, and that the SmartEvent Intro server resides on the R75 Security Management server or dedicated R75 Log server, according to the expected load.

This table shows where to configure the components, according to deployment.

<table>
<thead>
<tr>
<th>Deployment</th>
<th>SmartEvent Intro Server</th>
<th>Event Correlation Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>All-in-one</td>
<td>Security Management server</td>
<td>Security Management server (that is also a Log server)</td>
</tr>
<tr>
<td>Basic Load 1</td>
<td>Security Management server</td>
<td>Dedicated Log server</td>
</tr>
<tr>
<td>Basic Load 2</td>
<td>Dedicated Log server</td>
<td>Security Management server (that is also a Log server)</td>
</tr>
<tr>
<td>Moderate Load/ Multi-Domain Security Management</td>
<td>Dedicated Log server</td>
<td>Same dedicated Log server</td>
</tr>
</tbody>
</table>
The Event Correlation process produces events by processing the logs from the Log server against the Event Policy. The SmartEvent Intro server runs a database that is populated by events that result from the Event Correlation process.

## Standalone Deployment

### To configure SmartEvent Intro to run on a Security Management Server:

1. Install your SmartEvent Intro Software Blade license on the Security Management Server. Within the first 15 days of installing the Security Management Server, you will automatically receive a 15-day trial.
2. Connect to the Security Management Server using SmartDashboard.
3. In the Security Management Server object properties, select SmartEvent Intro from the Software Blades Management tab.
4. If more than one of possible SmartEvent Intro blades are installed and licensed, select which mode to use from the properties of the management object > SmartEvent Intro
5. Save changes.
6. Select Policy > Install Database and install the database on your Security Management servers and Log servers.

## Distributed Deployment

### To configure SmartEvent Intro server to run on a dedicated Log server:

1. Follow the instructions to install a Log server (see "Installing Security Gateways, Security Management and Endpoint Security" on page 15), select SmartEvent and SmartReporter Suite, and select the SmartEvent and SmartEvent Correlation Unit components.
   - In Windows, you must select the Custom installation option.
2. Once you have completed the installation, install your SmartEvent Intro Software Blade license on the Security Management Server. If you do not yet have a license, you will automatically receive a 15-day trial.
3. On the dedicated Log server, configure it as SmartEvent Intro server using the following CLI commands:
   a) Run `evconfig`.
   b) Press 4 and Enter to enable SmartEvent Intro.
   c) Press 5 and Enter to enable SmartEvent Intro Event Correlator.
   d) Press 6 and Enter to save the configuration and exit `evconfig`.
   e) Run `evstop` and then `evstart`.
4. Connect with SmartDashboard to the management computer use the following steps to create a Network object for the new dedicated Log server.
   a) Right-click Network Object in the Objects Tree and select Host.
   b) Enter the name and IP address of the new server.
   c) Establish SIC with the Security Management server.
   d) In the Software Blades Management tab of the dedicated Log server object's General Properties page, select a SmartEvent Intro Software Blade.
   e) Click OK.
5. Save changes.
6. Select Policy > Install Database and install the database on all management objects.
Multi-Domain Security Management Deployment

After you install the release package on the Multi-Domain Server, you can configure your Multi-Domain Security Management environment to use SmartEvent Intro.

To configure SmartEvent Intro in a Multi-Domain Security Management Environment:

1. Follow the instructions to install a Log server (see "Installing Security Gateways, Security Management and Endpoint Security" on page 15), select **SmartEvent and SmartReporter Suite**, and select the SmartEvent and SmartEvent Correlation Unit components.
   - In Windows, you must select the **Custom** installation option.
2. After the installation completes, install a SmartEvent Intro Software Blade license on the Security Management Server.
   If you do not yet have a license, you will automatically receive a 15-day trial.
3. On the dedicated Log server, configure it as SmartEvent Intro server using the following CLI commands:
   a) Run `evconfig`.
   b) Press 4 and **Enter** to enable SmartEvent Intro.
   c) Press 5 and **Enter** to enable SmartEvent Intro Event Correlator.
   d) Press 6 and **Enter** to save the configuration and exit `evconfig`.
   e) Run `evstop` and then `evstart`.
4. Open the SmartDomain Manager and connect to the Multi-Domain Server.
5. Enable the SmartEvent Intro Software Blade for all relevant Domain Management Servers in the **Management Plug-ins** section of the Multi-Domain Security Management client.
6. Decide if the SmartEvent Intro server will be a Global server connected to the Multi-Domain Server, or a local server connected to a Domain Management Server.
   - **Global server** - Open the Global SmartDashboard for the Global Policy.
     - **Note** - All Domain Management Servers must be assigned to the Global Policy: right-click the Global Policy and click **Assign Policy**.
   - **Local server** - Open the Domain SmartDashboard for the specified Domain Management Servers.
7. Create a Network object for the new dedicated log server.
   a) Right-click **Network Object** in the Objects Tree and select **Host**.
   b) Enter the name and IP address of the new server.
   c) Establish **SIC** with the Security Management server.
   d) In the Software Blades **Management** tab of the dedicated Log server object's **General Properties** page, select **SmartEvent Intro**.
   e) Click **OK**.
8. Click **Save**.
9. (For Local server only) Select **Policy > Install Database** and install Database on all management objects.
Chapter 5

Installing Mobile Access

In This Chapter

Mobile Access Overview 43
Mobile Access Installation 43
The Mobile Access Wizard 44
Results of Enabling Mobile Access 45
Upgrading from Connectra to Mobile Access 46

Mobile Access Overview

Check Point Mobile Access blade is a simple and comprehensive remote access solution that delivers exceptional operational efficiency. It allows mobile and remote workers to connect easily and securely from any location, with any Internet device to critical resources while protecting networks and endpoint computers from threats. Combining the best of remote access technologies in a software blade provides flexible access for endpoint users and simple, streamlined deployment for IT.

This software blade option simply integrates into your existing Check Point gateway, enabling more secure and operationally efficient remote access for your endpoint users. The data transmitted by remote access is decrypted and then filtered and inspected in real time by Check Point’s award-winning gateway security services such as antivirus, intrusion prevention and web security. The Mobile Access blade also includes in-depth authentications, and the ability to check the security posture of the remote device. This further strengthens the security for remote access.

Mobile Access Installation

The Mobile Access Software Blade is only supported on machines running on the SecurePlatform Operating System. Install Mobile Access as part of the regular SecurePlatform gateway installation.

Mobile Access is pre-installed on Check Point appliances and is automatically installed when upgrading to R75 with the R75 upgrade package. In these cases, begin with step 3 below.

To install and activate the Mobile Access blade:
1. When installing R75 products during the Installation Wizard, select Mobile Access.
   If you missed step 1 in the initial installation, run sysconfig from the CLI at any time to select Mobile Access or install Mobile Access using SmartUpdate.

   Note - We do not recommend installing Mobile Access and Endpoint Security on the same machine in a standalone environment,

2. After you have finished installing the new version and have connected to the SmartDashboard from a GUI client, install policy.
The Mobile Access Wizard

The Mobile Access Wizard enables you to easily configure remote access to your network, enabling users to access an internal site remotely. Alternatively, you can configure access to a Demo application.

Essentially, the Wizard guides you through the process of:

- Creating a Web Application object
- Creating a user group, selecting an existing user group, or selecting LDAP users or groups
- Troubleshooting connectivity between the Security Gateway and the Web application
- Creating a Mobile Access rule that allows a user group to access the Web application

Step 1: Configure a Web Application

Configure a Web application that users will connect to remotely.

If you have an internal Web application, for example, an organizational intranet site or Microsoft Outlook Web Access, it is recommended to configure access to that site. Enter its URL and, optionally, a display name, which is how the application will appear in the portal, for example, Company Intranet.

Note - Domino Web Access (iNotes) applications cannot be defined as the internal Web application using the First Time Wizard.

After entering the details, you can Test connectivity between the gateway and your internal application. If the gateway cannot reach the Web application, the Wizard will list steps that you can take to enable connectivity. You can automatically accept the suggestions, making troubleshooting quick and easy. You can also choose to configure the DNS and proxy settings manually.

If you do not have an internal site, select the Demo application. The Demo application does not need any further details or connectivity tests.

Step 2: Configure Authorized Users

Configure the user or user groups that are allowed to access the Web application/s that you configured in Step 1.

Make a selection to choose which users or groups can access the configured application:

- Test user- Create a test user by entering credentials of an internal user who will be allowed to access the application.
- Users or groups from Active Directory AD.xxx.com - Define users and groups from the Active Directory that is already configured to work with your environment. This option only appears if the computer running the Wizard is a member of an Active Directory domain.
- Users or groups from other Active Directory domain - Define a new Active Directory and an account that will validate user login.

Configuring Users or Groups from an Active Directory

If you selected one of the Active Directory options above, enter a User name and Password that the Security Gateway can use to gain access into the Active Directory and validate users’ credentials. You may want to create a user account for this specific purpose.

Note - Mobile Access does not support Microsoft Active Directory 2000.

A new page opens in which you specify which users from the AD are authorized to access the application. In effect, you are creating a user group on the AD user gateway that you specify.

Under Authorized Users, select one of the following:

- Your user - allows access only to you with your AD credentials
- All users - allows access to all users defined in the Active Directory
• **Specific user(s)/group(s)** - manually enter AD users and user groups.

### The Mobile Access Wizard is Complete

A summary tells you what you have accomplished using the First Time Wizard.

1. Click **Finish** to complete the Wizard.
2. Wait while the new objects are created.
3. Click **OK** on the Security Gateway Properties window. You must install the security policy on the Security Gateway in order for your changes to take effect.

Note that the Mobile Access Wizard is only the beginning of configuring comprehensive secure remote access to internal applications. Configure a complete set of applications, access rules, and security requirements in the Mobile Access tab in SmartDashboard.

### Results of Enabling Mobile Access

When you enable the Mobile Access Software Blade, the following configuration changes happen automatically:

- **Note** - If you disable the Mobile Access blade, these changes remain in place.

#### On the Security Gateway

- Visitor Mode is enabled
- Office Mode is enabled for all users
- The SSL Network Extender client is enabled

If you used SSL Network Extender from IPSec after enabling the Mobile Access Software Blade, you must reconfigure access to SSL Network Extender from the Mobile Access Blade. Configure SSL Network Extender access as Native applications in the Mobile Access tab. It will then be accessible from the Mobile Access portal.

See the [R75 Mobile Access Administration Guide](http://supportcontent.checkpoint.com/documentation_download?ID=11673) for more information on configuring SSL Network Extender.

#### On a VPN Cluster with ClusterXL in Load Sharing

If you have clusters, the following additional Cluster settings are set:

- The Sticky Decision Function is enabled
- The Load Sharing Method becomes based on IP address

#### On a VPN Cluster with ClusterXL in High Availability

If the VPN cluster configuration is in HA Legacy mode when the Mobile Access blade is enabled, the cluster mode is automatically configured to HA New mode. The administrator should configure the cluster interfaces in the Topology tab as required for HA New mode.

The following message displays if no cluster interfaces are configured:

> The VPN Domain is not fully defined. To make the encryption work properly you must edit the interfaces topology in the Topology tab.

See the [R75 ClusterXL Administration Guide](http://supportcontent.checkpoint.com/documentation_download?ID=11659) for more information on ClusterXL modes and topology.
Upgrading from Connectra to Mobile Access

To upgrade centrally managed Connectra gateways to Mobile Access gateways, upgrade the Security Management Server and then re-install the Security Gateways. The Security Gateways will not be upgraded automatically, but should be manually reconfigured.

R62 centrally managed Connectra gateways can be upgraded to R75 from NGX R65 Management.

R66 and R66.1 centrally managed Connectra gateways can be upgraded to R75 from NGX R65 HFA 30 Management.

Standalone Connectra gateways cannot be reconfigured.

**To upgrade a centrally managed Connectra configuration:**
1. Upgrade the management server to R75.
2. Install a new Mobile Access enabled R75 Security Gateway instead of the Connectra gateway and then install the policy from the upgraded Security Management Server.
Chapter 6

Installing and Configuring DLP

This section explains how to install and perform basic configuration of the DLP Software Blade.

For information about configuring a DLP-1 Appliance as a dedicated DLP gateway, see the *R71 DLP-1 Getting Started Guide* (http://supportcontent.checkpoint.com/documentation_download?ID=10832).

DLP and Privacy

DLP captures original data that caused a rule match, including the body of the transmission and attached files. We recommend that you disclose to your users how your DLP deployment works. Tell users that transmissions that violate the data security guidelines of your organization will be stored and may be read by security personnel.

Information disclosure recommendations:

1. Disclose the privacy policy BEFORE deploying DLP.
2. Translate the most important DLP rules into guidelines and tell your users what is not allowed and will result in captured transmissions.
3. Explain that DLP scans only transmissions originating from computers inside the organization (including any source that uses organization resources, such as Remote Access or VPN connections).
4. Explain how to handle Ask User violations.
   DLP incident notifications can be sent by email (for SMTP traffic) or shown in a system tray popup from the Endpoint Security on Demand client (for SMTP, HTTP, FTP, etc).
   If the incident of the notification is in Ask User mode, the user can click the Send or Discard link in the popup of Endpoint Security on Demand to handle the incident in real-time.

   **Important** - Make your users are aware of the purpose of the Endpoint Security on Demand client: handle the DLP options directly from the popup.

   If the user exits the client, the alternative web page that provides the Ask User options may not function.

5. Explain that captured transmissions will be logged and saved, and that some may be reported to managers (Data Owners).
6. Explain that captured emails, attachments, web posts, etc. will be available for review by security personnel.
7. Explain that review of original transmissions is for organization data security alone - you are not collecting personal information. Therefore, your users do not have, nor require, the option to not have their transmissions scanned.
8. Make sure that you maintain your guidelines: do not keep or use original transmissions for any use other than review of DLP incidents and rules.
DLP Requirement Notes

Port

- **Connectivity with other components**
  Check Point Data Loss Prevention is a Software Blade. It needs connectivity to a Security Management Server and a SmartDashboard. You need a Check Point gateway for DLP, or a DLP-1 appliance. You will also probably have a protecting VPN Security Gateway in front of the DLP gateway. The environment must include a DNS.

- **Required port for dedicated DLP deployment**
  The port for DLP gateway on SecurePlatform, for the HTTP WebUI Management, is HTTPS 4434, and not 443 as is default for other Security Gateways.

DNS

The environment must include a DNS.

If you use an IP address instead of a DNS name, emails sent to users to notify of incidents will contain URLs with that IP address. Some email clients may consider URLs with IP addresses to be possible phishing emails and will then issue a warning and disable the links. To prevent this, use a DNS name, not an IP address.

Installing the DLP gateway

The DLP gateway installation process begins with the installation of SecurePlatform.

**To install on SecurePlatform using the DVD:**

1. Insert the DVD into the optical drive, and boot the computer from the DVD. After booting, the *Welcome message* appears. If you do not press *Enter* within 90 seconds, the computer boots from the hard drive. The installation program is loaded.

2. The following options are displayed:
   - **Device List**: When selected, the *Hardware Scan Details* menu displays.
   - **Add Driver**: This option is only for use in consultation with Technical Support.

3. From the *Keyboard Selection* menu, select a keyboard language and select OK.

4. From the *Network Interface Configuration* menu, define these network settings and select OK.
   - **IP address** of the management interface
   - **Net mask** and **default gateway** for the first network interface

5. Select OK to confirm that you are about to format your hard drive and install SecurePlatform with the Software Blade.

   **Important** - The formatting procedure erases all information located on your hard drives.

   The installation process can take several minutes to complete.
   When installation is complete, remove the DVD and press *Enter* to reboot.

   You can now configure SecurePlatform through the DLP WebUI or through the command line.

Configuring SecurePlatform using the WebUI

We recommend that you continue with the SecurePlatform configuration though the WebUI, especially if you are configuring the DLP gateway in Bridge Mode.

To use the WebUI, connect to the server's IP address over https (https://<ip_address>:4434). For detailed instructions, refer to the *R75 Data Loss Prevention Administration Guide* (http://supportcontent.checkpoint.com/documentation_download?ID=11661).
Configuring SecurePlatform using the CLI

You can configure the SecurePlatform basic settings through the Command Line Interface (CLI). Then you will complete the DLP initial configuration through the WebUI.

To configure SecurePlatform through the CLI:
1. Log in with the user name: admin and password: admin.
2. When prompted, change the admin password. You can also change the admin user name.
3. Run: sysconfig
   The first-time system configuration wizard starts.
   Press n to continue.
4. In the Network Configuration menu, configure these options and press n to continue:
   - Host Name
   - Domain Name
   - DNS server
   - Network Interfaces
   - Routing Configuration
5. In the Time and Date Configuration menu, configure these options and press n to continue:
   - Date
   - Time and time zone
7. After gateway R75 DLP is installed successfully, press y to reboot your machine.

You can now configure the DLP Software Blade. To do this, connect to the server's IP address over https (https://<ip_address>:4434). For detailed instructions, refer to the R75 Data Loss Prevention Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11661).

Where To From Here?

You have now performed the basic configuration of the DLP Software Blade. The next step is to obtain more advanced knowledge of your Check Point software.

- For information about configuration and deployment of DLP Gateways, see the R75 Data Loss Prevention Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11661).

Check Point documentation is available in PDF format on the Check Point DVD and the Technical Support download site (http://supportcenter.checkpoint.com).

Be sure to also use the Check Point Online Help when you are working with the Check Point SmartConsole clients.

For additional technical information about Check Point products, consult Check Point's SecureKnowledge (http://supportcenter.checkpoint.com).
Chapter 7

Installing IPS-1 Sensors

Note - To upgrade existing IPS-1 Sensors, re-install according to these instructions.

In This Chapter

Overview of IPS-1 50
Installing and Configuring IPS-1 Sensors 51
Where To From Here? 55

Overview of IPS-1

IPS-1 is an intrusion prevention system (IPS) that delivers protection from a wide-range of network threats using an IPS-1 Sensor that can be placed either on the perimeter of your network or at any location in your internal network.

Some of the benefits of IPS-1 include:

- Unified security management
- Mission-critical protection against known and unknown attacks
- Granular forensic analysis
- Flexible deployment
- Confidence Indexing

IPS-1 System Architecture

An IPS-1 deployment includes the following components:

- **IPS-1 Sensor**: A device that is used exclusively for detecting and preventing network attacks, and sends alerts to the Security Management Server. The sensor enforces “dedicated” IPS protections.

- **Security Management Server**: The central management server which contains the object database and security policies. Security policies and IPS profiles are configured on the Security Management Server and installed on the IPS-1 sensors.

- **Log Server**: Receives alert information from the Security Management Server. The Log server can be installed with the Security Management server or as a separate server.

- **SmartConsole**: Windows-based remote graphical user interface (GUI) to the Security Management server for managing IPS-1 sensors, IPS profiles and IPS protections. The SmartConsole includes a number of independent interlinked clients, primarily:
  - **SmartDashboard** for configuring protections and managing the entire IPS-1 system.
  - **SmartView Tracker** for viewing, tracking, and analyzing alerts.

IPS-1 Sensor Deployment

IPS-1 Sensors should be deployed at natural choke points according to network topology. Usually, sensors should be just within the network firewall. We do not recommend placing sensors outside the firewall.
because the sensor will not be protected by the firewall and unfiltered traffic will place a heavy load on the sensor.

Ideally, network cores should also be protected with sensors. In some cases, such as in a complex switching environment in a network core, sensors need to be used for intrusion detection in passive mode.

Sensors' monitoring interfaces are layer-3 transparent and do not have IP addresses. Each sensor has a management interface that requires an IP address that is routable to and from the Security Management Server. For enhanced security, we recommend that the management server be on a separate, out-of-band network.

**Inline Intrusion Prevention**

For intrusion prevention, sensors should be connected inline, so that all of the traffic to be monitored flows through the IPS-1 Sensor. In this configuration, sensors can drop traffic containing attacks, according to defined and configurable confidence indexing.

Inline sensors' behavior upon failure can be configured to either open, passing through all traffic; or closed, severing the traffic path.

Inline sensors can be set to Detect-Only, to avoid the possibility dropping false-positive traffic. This way you can track what the sensor would have done in prevention mode. You can fine-tune your prevention settings in Detect-only/Monitor-only mode, and later change to prevention mode.

**Passive Intrusion Detection**

The IPS-1 Sensor can be placed out of the path of network traffic, in which case it performs intrusion detection only.

For the sensor to monitor traffic, a monitoring interface of the sensor should be connected to one of the following:

- A hub's port
- A switch's SPAN (or 'mirror') port
- A network tap

A network tap has advantages over a switch's SPAN port. For example, the switch could prevent (or be unable to send) some traffic out of the SPAN port.

For information on configuring and connecting the switch or tap, see the switch's or tap's documentation.

**Installing and Configuring IPS-1 Sensors**

These instructions are for installing IPS-1 Sensor software on open servers.

The IPS-1 Sensor is installed with SecurePlatform in one installation process. You cannot reinstall the sensor without reinstalling the operating system and formatting the hard disk.

**Installing IPS-1 Sensors with SecurePlatform**

To install the IPS-1 Sensor with SecurePlatform:

1. Insert the CD from the media pack into the CD drive, and boot the machine from the CD. After booting, **Welcome to Check Point SecurePlatform** appears.
2. Press **Enter** within 90 seconds to boot from the CD. The installation program is loaded.
3. Choose **OK** to proceed with the installation. You can also use these hardware configuration options:
   - **Device List**: When selected, the **Hardware Scan Details** menu displays.
   - **Add Driver**: When selected, the **Devices** menu opens. Sometimes updated hardware is incompatible with the previous version's driver and you receive an error message during installation because the operating system could not find the appropriate hard disk driver. Alternatively, the
installation may be complete, but the hardware does not function properly. The Add Driver option enables you to add the missing driver during the installation process.

4. Select the type of hardware you are using.

If you are installing on a Check Point appliance or a legacy appliance purchased from NFR, select Appliance. If you are installing on hardware supplied by another vendor, select Open Sensor.

Sensor 1000: Select Open Sensor.

5. Choose a keyboard language. Select OK.

6. In the Networking Device window, choose the management interface and select OK.

7. In the Management Interface Configuration window, enter the management interface IP address, net mask and default gateway. Select OK.

8. Select OK to proceed with the installation.

The installation process formats your hard drive, and installs SecurePlatform operating system with the IPS-1 Sensor components. This can take several minutes to complete.

9. When installation is complete, remove the CD and press Enter to reboot.

### Configuring IPS-1 Sensors

To configure an IPS-1 Sensor:

1. Log in with the user name: admin and password: admin.

2. When prompted, change the admin password. You can also change the admin user name.

3. Run: sysconfig

   The first-time system configuration wizard starts.

   Press n to continue.

4. Read the End-user License Agreement and press y to accept it.

5. In the Network Configuration menu, configure the:
   - Host Name
   - Domain Name
   - At least one DNS server
   - Management Interface

   Press n to continue.

6. In the Time and Date Configuration menu, configure:
   - Date
   - Time and time zone

   Note - Network Time Protocol (NTP) can be configured through the command line interface after all of the installation procedures are complete. For more information, see Configuring NTP on SecurePlatform (see "Configuring NTP" on page 54).

7. Press n to continue.

8. In the Operating Mode menu, select these fields with the Enter key and choose a value.
   - Operating Mode:
     - **IDS (passive)**: intrusion detection, no prevention. Packets do not pass from one interface to another.
     - **IPS (inline, fail-closed)**: inline intrusion prevention. In fault conditions, all packets are dropped.
     - **IPS (inline, fail-open)**: inline intrusion prevention. In fault conditions, all packets are passed through.
     - **IPS Monitor-Only (inline, fail-open)**: inline bridge mode, but without actual prevention.

   For more information on sensor modes, see the R71 IPS-1 Sensor Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=10505).

   - Management Interface - displays the IP address configured in the operating system.
   - Inline Pair(s) - pairs of monitoring interfaces. Depending on your hardware, you may need to define the interface pairs that you will be using.

Select Next to proceed.
9. Enter and confirm the Activation Key for Secure Internal Communication (SIC). You will enter the activation key when you create the IPS-1 Sensor object in the SmartDashboard. SIC creates a trusted connection between the sensor and the management.

10. Enter y to start the IPS-1 Sensor processes. You can modify the sensor's settings at any time by running the `cpconfig` command.

The IPS-1 Sensor is now installed and configured.

**Post-Configuration Steps**

Once the IPS-1 Sensor has been configured, you must create the IPS-1 Sensor object in SmartDashboard. IPS-1 Sensor processes are dependent on time synchronization. You can make sure your sensors and management servers are synchronized using Network Time Protocol.

**Adding IPS-1 Sensors**

When you add a new IPS-1 Sensor object, the sensor is automatically added to the list of Enforcing Gateways and it is assigned the **IPS-1 Recommended Protection** profile. By default, the sensor is configured as **IPS-Inline** with **fail-open** bypass mode.

When adding an IPS-1 Sensor, you can also define these settings which are unique to IPS-1 Sensors:

**Working Mode**

- **IDS - Passive**: The IPS-1 Sensor is not placed in the path of traffic. Packets are processed for attack detection without any impact on the flow of network traffic.
- **IPS - Inline, Detect only**: Inline intrusion detection. Packets are forwarded through to the network before processing for attack detection. In fault conditions, all packets are allowed. Detect only mode is also useful for checking whether an IPS-mode Sensor is responsible for dropped traffic.
- **IPS - Inline, fail-open**: Inline intrusion prevention. Packets are processed for attack detection and are forwarded to the network only in accordance with protection settings. In fault conditions, all packets are allowed.
- **IPS - Inline, fail-closed**: Inline intrusion prevention. Packets are processed for attack detection and are forwarded to the network only in accordance with protection settings. In fault conditions, all packets are dropped.

**Warning** - Changing the Working Mode may stop the flow of network traffic. Make sure that your network topology is correct for the IPS-1 Sensor Working Mode that you choose.

**Topology**

By default, the IPS-1 Sensor inspects all traffic that passes through its interfaces. We recommend that you manually define the protected networks in the IPS-1 Sensor's Topology page. The Topology options are:

- **All IPs** lets the IPS-1 Sensor protections react to all traffic with the highest level of inspection. Most organizations will choose not to use this setting because it requires a high level of inspection of traffic even of traffic that does not impact the organization's security.
- **Manually defined** lets you specify the group of hosts or networks that the IPS-1 Sensor protects. This reduces the load on the sensor by focusing the sensor's resources on traffic that relates to internal networks.
- **None** does not specify a group of hosts or networks for protection. When no topology is configured, the IPS-1 Sensor inspects all traffic with a lower level of intensity. The IPS-1 Sensor will inspect traffic faster but without the high level of inspection provided by the **All IPs** and **Manually defined** settings.

**Latency Threshold**

The Latency Threshold suspends IPS inspection when the average latency of traffic passing through the sensor exceeds a specified threshold. The specified latency level will be treated as a Fail State. Then, traffic will be passed or dropped based on the Sensor bypass mode of the IPS-1 Sensor's General Properties. By default, this setting is off, but you can enable it from the IPS-1 Sensor's IPS page.
To create an IPS-1 Sensor object:
1. If there is a Security Gateway between the management server and the IPS-1 Sensor, make sure Accept IPS-1 management connections is selected in the Global Properties > Firewall page.
2. In the IPS tab, select Enforcing Gateways.
3. Click Add and choose IPS-1 Sensor.
4. Enter the properties of the IPS-1 Sensor.
5. If there is a Security Gateway between the management server and the IPS-1 Sensor, install the policy on the gateway.
6. Open the IPS-1 Sensor object and click Communication to initiate SIC.
7. Once SIC is initialized, click Close.
8. Click OK.

The IPS-1 Sensor object is created and you can now include the IPS-1 Sensor in policy installation.

**Note** - If policy installation fails when the IPS-1 Sensor is set to an IPS-Inline Working Mode, log into the sensor’s CLI and check that the interfaces are set to work as inline pairs. Refer to the R71 IPS-1 Sensor Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=10505).

### Configuring NTP

IPS-1 components rely on Network Time Protocol (NTP) to coordinate the time on each component. Use these commands to configure and manage NTP.

**ntp**

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

**ntpstop**

**Description** Stop polling the NTP server

**Syntax**

```
ntpstop
```

**ntpstart**

**Description** Start polling the NTP server

**Syntax**

```
ntpstart
```
Where To From Here?

You have now learned the basics that you need to get started. The next step is to obtain more advanced knowledge of your Check Point software.

- For information about configuration and deployment of IPS-1 Sensors, see the R71 IPS-1 Sensor Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=10505).
- For information about managing IPS profiles and protections, see the R75 IPS Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11663).

Check Point documentation is available in PDF format on the Check Point DVD and the Technical Support download site. (http://supportcenter.checkpoint.com)

Be sure to also use the Check Point Online Help when you are working with the Check Point SmartConsole clients.

For additional technical information about Check Point products, consult Check Point’s SecureKnowledge (http://supportcenter.checkpoint.com).
Upgrading
Chapter 8

Introduction to the Upgrade Process

Before you upgrade:

- For information about supported upgrade paths, see the R75 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=11647).
- Make sure that you have the latest version of this document (http://supportcontent.checkpoint.com/documentation_download?ID=11648).

In This Chapter

Contract Verification 57
Terminology 57
Upgrade Tools 58
Upgrading Successfully 58

Contract Verification

Contract verification is now an integral part of the Check Point licensing scheme. Before upgrading to the latest version, your licensing agreements are verified through the User Center.

See: Service Contract Files (on page 59) for more information.

Terminology

**Advanced Upgrade**: Installing the latest Security Management Server or Multi-Domain Server version from the distribution media on separate computer and then migrating the database from the existing Security Management Server or Multi-Domain Server. This method minimizes upgrade risks for an existing deployment.

**ClusterXL**: A software-based load sharing and high availability solution for Check Point gateway deployments. It distributes traffic between clusters of redundant gateways so that the computing capacity of multiple machines may be combined to increase total throughput. In the event that any individual gateway becomes unreachable, all connections are re-directed to a designated backup without interruption. Tight integration with Check Point's Security Management server and security gateway solutions ensures that ClusterXL deployment is a simple task for security gateway administrators.

**Distributed Deployment**: The gateway and the Security Management server are deployed on different computers.

**Standalone Deployment**: The Check Point components responsible for managing the Security Policy (the Security Management Server and the Security Gateway) are installed on the same machine.

**Gateway or Check Point Gateway**: A gateway is the software component which actively enforces the Security Policy of the organization.

**In-Place Upgrade**: Upgrading a Security Management Server or Multi-Domain Server to the latest version on the existing computer.

**SmartProvisioning**: Enables enterprises to easily scale, deploy, and manage VPNs and security for thousands of remote locations.

**Package Repository**: This is a SmartUpdate repository on the Security Management server that stores uploaded packages. These packages are then used by SmartUpdate to perform upgrades of Check Point Gateways.
**SmartLSM Security Gateway**: A Remote Office/Branch Office Gateway. (Formerly ROBO gateway)

**SmartLSM Profile** (previously ROBO Profile): An object that you define to represent properties of multiple SmartLSM Security Gateways (previously known as ROBO Gateway). Profile objects are version dependent. When you plan to upgrade SmartLSM Security Gateways to a new version, first define new Profile objects. In general, it is recommended that you keep the Profile objects of the previous versions until all SmartLSM Security Gateways of the previous version are upgraded.

**Security Policy**: A Security Policy is created by the system administrator in order to regulate the incoming and outgoing flow of communication.

**Security Management server**: The Security Management server is used by the system administrator to manage the Security Policy. The databases and policies of the organization are stored on the Security Management server, and are downloaded from time to time to the gateways.

**SmartConsole Clients**: The SmartConsole Clients are the GUI applications that are used to manage different aspects of the Security Policy. For example, *SmartView Tracker* is a GUI client used to view logs.

**SmartDashboard**: A GUI client that is used to create Security Policies.

**SmartUpdate**: A tool that enables you to centrally upgrade and manage Check Point software and licenses.

### Upgrade Tools

Various upgrade tools are provided for migration and compatibility verification of your current deployment. These tools help you successfully upgrade to R75.

The upgrade tools can be found in the R75 directory `$/FWDIR/bin/upgrade_tools`. The upgrade tools can also be downloaded from the Check Point Support site ([http://supportcenter.checkpoint.com](http://supportcenter.checkpoint.com)).

### Upgrading Successfully

**Note that:**

- Only Check Point Suite Products from version NGX R65 and above can be upgraded to R75.
- When upgrading NGX R65, only the following Plug-ins may be present: Connectra, SmartProvisioning, VSX, and Messaging Security. The presence of any other Plug-in will cause the upgrade process to fail.
- When upgrading a Security Management Server to R75, IPS profiles will remain in effect on pre-R70 gateways and can be managed from the IPS tab.
- When upgrading a Security Gateway to R75, remember to change the gateway’s object in SmartDashboard to version R75. The gateway will continue to enforce the previously configured IPS profile, but the inspection will be conducted using the new IPS inspection engine. You can apply an R75 IPS profile to the upgraded gateway at any time.

If you encounter unforeseen obstacles during the upgrade process, contact your Reseller or consult the Support Center ([http://supportcenter.checkpoint.com](http://supportcenter.checkpoint.com)).
Chapter 9

Service Contract Files

In This Chapter

Introduction 59
Working with Contract Files 59
Installing a Contract File on Security Management server 59
Installing a Contract File on a Gateway 61
Managing Contracts with SmartUpdate 63

Introduction

Before upgrading a gateway or Security Management server to R75, you need to have a valid support contract that includes software upgrade and major releases registered to your Check Point User Center account. The contract file is stored on Security Management server and downloaded to security gateways during the upgrade process. By verifying your status with the User Center, the contract file enables you to easily remain compliant with current Check Point licensing standards.

Working with Contract Files

As in all upgrade procedures, first upgrade your Security Management Server or Multi-Domain Server before upgrading the gateways. Once the management has been successfully upgraded and contains a contract file, the contract file is transferred to a gateway when the gateway is upgraded (the contract file is retrieved from the management).

Note - Multiple user accounts at the User Center are supported.

Installing a Contract File on Security Management server

The following section covers obtaining and installing the contract file for Security Management server:

- On a Windows Platform
- On SecurePlatform, Linux and Solaris
- On IPSO

On a Windows Platform

When upgrading Security Management server, the upgrade process checks to see whether a contract file is already present on the server. If not, the main options for obtaining a contract are displayed:

You can:

- Download a contracts file from the User Center
If you have Internet access and a valid user account, you may download a contract file directly from the User Center. The contract file obtained through the user center contains contract information for all of your accounts at the User Center. Contract files downloaded from the User Center match the terms of your license agreements.

a) Click Next.
b) Enter your User Account credentials.
c) If the connection succeeds but the downloaded contract file does not cover the Security Management server, a message informs you that the Security Management server is not eligible for upgrade.

However, the absence of a valid contract file will not prevent the upgrade from taking place. Once the upgrade is complete, contact your local support provider to obtain a valid contract.

### Import a local contract file

If the server does not have Internet access, then:

a) On a machine with Internet access, log in to the User Center (http://usercenter.checkpoint.com)
b) Browse to Support.
c) On the Additional Services page, in the Service Contract File Download section, click Download Now:
d) Transfer the downloaded file to the management server. After selecting Import a local contracts file, you can then browse to the location where you stored the contract file:

If the contract file does not cover the Security Management server, a message informs you that the Security Management server is not eligible for upgrade. However, the absence of a valid contract file will not prevent the upgrade from taking place. Once the upgrade is complete, contact your local support provider to obtain a valid contract.

e) Click Next to continue with the upgrade process

### Continue without contract information

Select this option if you intend to obtain and install a valid contract file at a later date. Note that at this point your gateway is not strictly eligible for an upgrade; you may be in violation of your Check Point Licensing Agreement, as shown in the final message of upgrade process. For more information, see: Managing Contracts with SmartUpdate (on page 63).

### On SecurePlatform, Linux, and Solaris

When upgrading Security Management server, the upgrade process checks to see whether a contract file is already present on the server. If not, the main options for obtaining a contract are displayed. You can:

### Download a contracts file from the User Center

If you have Internet access and a valid user account, then download a contract file directly from the User Center. This contract file conforms to the terms of your licensing agreements. If you choose to download contract information from the User Center, you are prompted to enter your:

- User name
- Password
- Proxy server address (if applicable)

If the contract file does not cover the Security Management server, a message informs you that the Security Management server is not eligible for upgrade. However, the absence of a valid contract file will not prevent the upgrade from taking place. Download a valid contract at a later date using SmartUpdate (see: Managing Contracts with SmartUpdate (on page 63)).

### Import a local contract file

If the server being upgraded does not have Internet access, then:

a) On a machine with Internet access, log in to the User Center (http://usercenter.checkpoint.com)
b) Browse to Support
c) On the Downloads page, in the Service Contract File Download section, click Download Now:
Installing a Contract File on a Gateway

The following section covers obtaining and installing the contract file for gateways:

- On a Windows Platform
- On SecurePlatform
- On IPSO

On a Windows Platform

After accepting the End User License Agreement (EULA), the upgrade process checks to see if a valid contract file is installed on the gateway. If no contract file exists, the upgrade process attempts to retrieve a contract file from the Security Management server that manages the gateway. If a contract file cannot be retrieved from Security Management server, the main options for obtaining a contract file for the gateway are displayed. You can:

- **Download a contracts file from the User Center**
  
  If you have Internet access and a valid user account, then download a contract file directly from the User Center. The contract file obtained through the user center conforms with the terms of your licensing agreements.
  
  a) Enter your User Account credentials.

  If the connection succeeds but the downloaded contract file does not cover the gateway, a no coverage message appears. However, this will not prevent the upgrade from taking place. After clicking **Next**, the upgrade process continues.

- **Import a local contract file**

On IPSO

Contract verification on IPSO is not interactive. When upgrading an IPSO Security Management server to R75, the upgrade process will check to see if there is a valid contract already present on the Security Management server. If a contract is not present, the upgrade process proceeds as normal. After successfully upgrading the gateway, the following message is displayed:

The upgrade process requires a valid contract file in order to verify that your gateway complies with Check Point licensing agreements. While the absence of a contract file does not prevent this upgrade, it is recommended that you obtain a contract file via SmartUpdate (Licenses & Contracts menu -> Update Contracts).

For further details see: http://www.checkpoint.com/ngx/upgrade/contract/

At the earliest opportunity, obtain a valid contract file from the Check Point User Center (http://supportcenter.checkpoint.com).

Installing a Contract File on a Gateway

The following section covers obtaining and installing the contract file for gateways:

d) Transfer the downloaded file to the management server. After selecting **Import a local contracts file**, enter the full path to the location where you stored the file:

If the contract file does not cover the Security Management server, a message informs you that the Security Management server is not eligible for upgrade. However, the absence of a valid contract file will not prevent the upgrade from taking place. Download a valid contract at a later date using SmartUpdate (see: Managing Contracts with SmartUpdate (on page 63).)

- **Continue without contract information**
  
  Select this option if you intend to obtain and install a valid contract file at a later date. Note that at this point your gateway is not strictly eligible for an upgrade; you may be in violation of your Check Point Licensing Agreement, as shown in the final message of the upgrade process.

  For more information, see: Managing Contracts with SmartUpdate (on page 63).
Installing a Contract File on a Gateway

If the server being upgraded does not have Internet access, then:

a) On a machine with Internet access, log in to the User Center (http://supportcenter.checkpoint.com)
b) Browse to Support
c) On the Downloads page, in the Service Contract File Download section, click Download Now:
d) Transfer the downloaded file to the gateway. After selecting Import a local contracts file, you can then browse to the location where you stored the file:
e) Click Next.

If the local contract file does not cover the gateway, a no coverage message is displayed. However, this will not prevent the upgrade from taking place. If the contract file covers the gateway, click Next to continue with the upgrade process

- Continue without contract information
Select this option if you intend to obtain and install a valid contract file at a later date. Note that at this point your gateway is not strictly eligible for an upgrade; you may be in violation of your Check Point Licensing Agreement, as shown in the final message of upgrade process.
For more information, see: Managing Contracts with SmartUpdate (on page 63).

On SecurePlatform

After accepting the End User License Agreement (EULA), the upgrade process searches for a valid contract on the gateway. If a valid contract is not located, the upgrade process attempts to retrieve the latest contract file from the Security Management server that manages the gateway. If a valid contract file is not located on the Security Management server, the main options for obtaining a contract file for the gateway are displayed. You can:

- Download a contracts file from the User Center
If you have Internet access and a valid user account, then download a contract file directly from the User Center. The contract file obtained through the user center conforms with the terms of your licensing agreements. If you choose to download contract information from the User Center, you are prompted to enter your:
  - User name
  - Password
  - Proxy server address (if applicable):
If, according to information gathered from your User Center account, your gateway is not eligible for upgrade, you can still upgrade the gateway but are advised to download a valid contract at a later date using SmartUpdate (see: Managing Contracts with SmartUpdate (on page 63) for more information on using SmartUpdate).

- Import a local contract file
If the server being upgraded does not have Internet access, then:
  a) On a machine with Internet access, log in to the User Center (http://usercenter.checkpoint.com)
  b) Browse to Support
c) On the Downloads page, in the Service Contract File Download section, click Download Now:
d) Transfer the downloaded file to the gateway. After selecting Import a local contracts file, enter the full path to the location where you stored the file:
  If the contract file does not cover the gateway, a message informs you that the gateway is not eligible for upgrade. However, the absence of a valid contract file will not prevent the upgrade from taking place. Once the upgrade is complete, contact your local support provider to obtain a valid contract.

- Continue without contract information
Select this option if you intend to obtain and install a valid contract file at a later date. Note that at this point your gateway is not strictly eligible for an upgrade; you may be in violation of your Check Point Licensing Agreement, as shown in the final message of the upgrade process.
For more information, see: Managing Contracts with SmartUpdate (on page 63).
On IPSO

Contract verification on IPSO is not interactive. When upgrading an IPSO gateway to R75, the upgrade process will check to see if there is a valid contract available on the Security Management server that manages the gateway. If none is available, the upgrade process proceeds. After successfully upgrading the gateway, the following message is displayed:

The upgrade process requires a valid contract file in order to verify that your gateway complies with Check Point licensing agreements. While the absence of a contract file does not prevent this upgrade, it is recommended that you obtain a contract file via SmartUpdate (Licenses & Contracts menu -> Update Contracts).

For further details see: http://www.checkpoint.com/ngx/upgrade/contract/

At the earliest opportunity, obtain a valid contract file from the Check Point user center.

Managing Contracts with SmartUpdate

Once you have successfully upgraded Security Management server, you can use SmartUpdate to display and manage your contracts. From the License management window, it is possible to see whether a particular license is associated with one or more contracts:

Managing Contracts

The license Repository window in SmartUpdate displays contracts as well as regular licenses:

- Clicking on a specific license shows the properties of the license:
- Clicking Show Contracts displays the contracts associated with this license:
Selecting a specific contract, then Properties displays the contract's properties, such as contract ID and expiration date as well as which licenses are covered by the contract.

Updating Contracts

Licenses & Contracts on the File menu has enhanced functionality for handling contracts:

- **Licenses & Contracts > Update Contracts**
  This option installs contract information on Security Management server. Each time you purchase a new contract, use this option to make sure the new contract is displayed in the license repository.

- **Licenses & Contracts > Get all Licenses**
  a) Collects licenses of all gateways managed by the Security Management server
  b) Updates the contract file on the server if the file on the gateway is newer
Chapter 10

Upgrading a Distributed Deployment

In This Chapter

Overview to Upgrading a Distributed Deployment 65
Using the Pre-Upgrade Verification Tool 65
Web Security License Enforcement 66
Upgrading Products on SecurePlatform 66
UTM-1 Edge Gateways Prior to Firmware Version 7.5 66
Upgrading the Security Management Server 66
Upgrading Security Gateways 71

Overview to Upgrading a Distributed Deployment

This chapter describes the process of upgrading a distributed deployment to R75. A distributed deployment consists of at least one Security Management server and one or more gateways. The Security Management server and gateway do not reside on the same physical machine. Since backward compatibility is supported, a Security Management server that has been upgraded to R75 can enforce and manage gateways from previous versions. In some cases, however, new features may not be available on earlier versions of the gateway.


Using the Pre-Upgrade Verification Tool

We recommend that you run the pre-upgrade verifier on the Security Management server source computer before export the management database. The pre-upgrade verifier does a compatibility analysis of the Security Management server database and its current configuration. A detailed report shows the steps to do before and after the upgrade.

The pre-upgrade verifier can only verify a database that is intended for import into a different major version of the Security Management server. It cannot be used on a database that is intended for import into the same major version of the Security Management server.

The pre_upgrade_verifier command

Run pre_upgrade_verifier without arguments to see its syntax and options.

Action Items

- **Errors** - Issues that must be resolved before you can continue with the upgrade. If you proceed without correcting these errors, the upgrade may fail, or you may have problems after upgrade.
- **Warnings** - Issues that are recommended to resolve before or after the upgrade.
Web Security License Enforcement

A gateway or gateway cluster requires a Web Security license if it enforces one or more of the following protections:

- Malicious Code Protector
- LDAP Injection
- SQL Injection
- Command Injection
- Directory Listing
- Error Concealment
- ASCII Only Request
- Header Rejection
- HTTP Methods

Upgrading Products on SecurePlatform

The procedure for upgrading R75 on SecurePlatform upgrades the SecurePlatform operating system as well as the specified products and Software Blades. See the Security Management Server Upgrade on SecurePlatform section for detailed procedures.

UTM-1 Edge Gateways Prior to Firmware Version 7.5

Before upgrading your deployment to R75, we recommend that you upgrade your UTM-1 Edge gateways to version 7.5 or higher. By default, Security Management server R75 is compatible with UTM-1 Edge gateways 7.5 and above.

Enabling Policy Enforcement

To enforce policies on earlier versions of UTM-1 Edge gateways, perform the following workaround:

Note - Once the workaround is complete, features new to R75 may not be available on the gateway.

1. In a text editor, open the:
   - `/var/opt/CPEdgecmp/conf/SofawareLoader.ini` file for Solaris, or
   - `c:\Program Files\CheckPoint\Edgecmp\R75\SofawareLoader.ini` file in Windows.
2. In the `[Server]` section, add the following:
   `TopologyOldFormat=1`
3. Save and close the file.

The change takes effect without running the commands `cpstop` and `cpstart`.

Upgrading the Security Management Server

This section describes how to upgrade a Security Management server to R75.
Upgrading the Security Management Server  

Upgrades can be performed incrementally so that you do not have to upgrade the Security Management server and all of the gateways at the same time. Once the Security Management server is upgraded, you can still manage gateways from the previous version, even though the gateways may not support the new features. You can upgrade the gateways at your convenience.

Use of the Pre-Upgrade verification tool can reduce the risk of incompatibility with the deployment to R75. It is used to test the current Security Management server prior to upgrading to R75. The Pre-Upgrade verification tool produces a detailed report indicating the appropriate actions that should be taken before performing an upgrade to R75 (refer to Using the Pre-Upgrade Verification Tool (on page 65)).

There are two upgrade methods available for the Security Management server:

- Upgrade your Production Security Management server
  - Perform the upgrade process on the production Security Management server (refer to the procedures in this section).

- Migrate and Upgrade to a New Security Management server
  - Perform a migration process (refer to Migrate Your Current Gateway Configuration & Upgrade) of the currently installed version to a new server, and upgrade the migrated system.

Using the Pre-Upgrade Verification Tool

We recommend that you run the pre-upgrade verifier on the Security Management server source computer before export the management database. The pre-upgrade verifier does a compatibility analysis of the Security Management server database and its current configuration. A detailed report shows the steps to do before and after the upgrade.

The pre-upgrade verifier can only verify a database that is intended for import into a different major version of the Security Management server. It cannot be used on a database that is intended for import into the same major version of the Security Management server.

Action Items

- Errors - Issues that must be resolved before you can continue with the upgrade. If you proceed without correcting these errors, the upgrade may fail, or you may have problems after upgrade.
- Warnings - Issues that are recommended to resolve before or after the upgrade.

Security Management Server Upgrade - SecurePlatform

Upgrading to R75 on a SecurePlatform operating system requires updating both the operating system and the installed software products using the CLI.

For a list of supported upgrade paths, see the R75 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=11647).

The process described in this section upgrades all of the components (Operating System and software packages) in a single upgrade process. No further upgrades are required. Refer to the R75 SecurePlatform Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11666) for additional information.

To go back to your previous configuration is required, see Reverting to Your Previous Deployment (on page 82) for details.

To upgrade SecurePlatform:
1. Insert the R75 DVD into the optical drive.
2. At the command prompt, enter `patch add cd`.
4. Enter `y` to accept the checksum calculation.
5. When prompted, create a backup image for automatic revert.

   ![Note](image) - Creating the snapshot image can take up to twenty minutes, during which Check Point products are stopped.

6. The Welcome message is displayed. Enter `n`. 

Upgrading a Distributed Deployment  
Page 67
7. Accept the license agreement, and verify your contract information.
   For more information on contracts, see: On SecurePlatform and Linux (see "On SecurePlatform" on page 62).

8. Three upgrade options are displayed: Upgrade, Export the configuration, and Perform pre-upgrade verification only.
   a) Run the pre-upgrade verification script, and follow the recommendations contained in the pre-upgrade verification results. Repeat the process until you see Your configuration is ready for upgrade.
   b) Export the configuration.
   c) Upgrade the installation.

9. Select a source for the upgrade utilities.
   Either download the most updated files from the Check Point website or use the upgrade tools contained on the DVD. The exported configuration is automatically imported during the upgrade process.

10. Open SmartUpdate and attach new licenses to the gateways.

---

**Security Management Server Upgrade - IPSO**

**Upgrade using Network Voyager**

This section gives the steps for upgrading IPSO appliances using the Network Voyager.

1. Download the applicable release package for your platform to an FTP site or to your local disk.

   Important - Installing the incorrect package can damage your platform.

<table>
<thead>
<tr>
<th>IP Appliance Platform type</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk based</td>
<td>IPSO6_wrapper_R75.tgz</td>
</tr>
<tr>
<td></td>
<td>(<a href="http://supportcenter.checkpoint.com/file_download?id=11773">http://supportcenter.checkpoint.com/file_download?id=11773</a>)</td>
</tr>
<tr>
<td>Flash based</td>
<td>Check_Point_R75_Security_Gateway_for_IPSO6_2.tgz</td>
</tr>
<tr>
<td></td>
<td>(<a href="http://supportcenter.checkpoint.com/file_download?id=11772">http://supportcenter.checkpoint.com/file_download?id=11772</a>)</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - This package does not include CPinfo. See sk30567 (<a href="http://supportcontent.checkpoint.com/solutions?id=sk30567">http://supportcontent.checkpoint.com/solutions?id=sk30567</a>) for download information.</td>
</tr>
</tbody>
</table>

2. Log in to your appliance using Network Voyager.
3. In the Network Voyager tree, select **Configuration > System Configuration > Packages > Install Package**.
4. Upload the package file using one of these methods:
   - **Upload from an FTP site:**
     1. In the Voyager **Install Package** window, select FTP.
     2. Enter the name or IP address of the FTP server.
     3. Enter the path to the directory on the FTP server where the packages are stored.
     4. If necessary, enter the applicable user name and password.
     5. Click **Apply**. The names of the available packages show in the **Site Listing** window.
     6. Select the package .tgz file in the **Site Listing** window and click **Apply**.
     7. When the <package name> downloaded to message shows, click it and then click **Apply** again.
   - **Upload from a local disk:**
     1. In the Voyager **Install Package** window, select **Upload**.
(ii) Click **Browse** and navigate to the package .tgz file.

(iii) Click **Apply**.

(iv) Select the package .tgz file in the **Unpack Package** window and click **Apply**.

5. Click the **Click here to install/upgrade** link to continue with the installation.

6. In the **Package Installation and Upgrade** pane, select **Install** and then click **Apply**.

7. Click the **Install Package** branch in the Voyager tree to see the installation progress.

8. Go to the **Manage Packages** page.
   - The R75 and Check Point CPInfo packages are automatically activated during installation (disk-based appliances only).
   - Enable other packages, with the compatibility packages, as needed for your deployment.

   **Important** - When you install a package using Network Voyager, this message shows:

   Voyager environment has been updated with the latest package info.
   The telnet session environment will be updated by: logging out and logging in again the telnet session.

   This message can be misleading. Click **Manage Packages** to verify that the package is actually installed correctly. Refresh the page periodically until you see that the installation is complete.

9. Log out of Network Voyager and then log in again.

### Upgrade using the Command Line Shell

This section gives the steps for upgrading IPSO appliances using the **clish** command line shell.

1. Download the applicable release package for your platform to an FTP site or to your local disk.

   **Important** - Installing the incorrect package can damage your platform.

<table>
<thead>
<tr>
<th>IP Appliance Platform type</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk based</td>
<td>IPSO6_wrapper_R75.tgz (<a href="http://supportcenter.checkpoint.com/file_download?id=11773">http://supportcenter.checkpoint.com/file_download?id=11773</a>)</td>
</tr>
<tr>
<td>Flash based</td>
<td>Check_Point_R75_Security_Gateway_for_IPSO6_2.tgz (<a href="http://supportcenter.checkpoint.com/file_download?id=11772">http://supportcenter.checkpoint.com/file_download?id=11772</a>)</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - This package does not include CPinfo. See sk30567 (<a href="http://supportcontent.checkpoint.com/solutions?id=sk30567">http://supportcontent.checkpoint.com/solutions?id=sk30567</a>) for download information.</td>
</tr>
</tbody>
</table>

2. Access the CLI console, and log in.

3. Type **newpkg**, and press Enter.

4. Use the FTP menu option to transfer the R75 package. Choose the option:

   - **Upgrade from an old package**.

5. Upgrade to the R75 package.

   Wait until a message informs you that the process is complete.

6. Type **reboot** and press Enter.

   The package is activated after the reboot.

7. Verify that R75 is active by running the following command:

   ```
   newpkg -q
   ```

8. Verify that R75 is the current version. Run **fw ver** on a Security Gateway or **fwm ver** on a Security Management server.
Security Management Server Upgrade on Windows Platforms

This section describes the upgrade process using the R75 DVD. It is recommended to back up your current configuration before you perform the upgrade process. For additional information, refer to: Backup and Revert for Security Gateways (on page 78). To go back to your previous configuration is required, see Reverting to Your Previous Deployment (on page 82) for details.

To perform an upgrade on a Windows platform:

1. Insert the R75 DVD.
2. If the upgrade does not start automatically, run Setup.exe from the DVD.
3. Click Next to start the installation wizard.
4. Accept the license agreement and click Next.
5. Click Next to check your license information.
6. From the Upgrade Options screen, select Upgrade and click Next.
7. Follow the support contract and upgrade utility screens. For more information on contracts, see: Installing a Contract File on Security Management server (on page 59).
8. When the pre-upgrade verification recommendation appears, select whether or not the Pre-upgrade verification tool should be executed (refer to Using the Pre-Upgrade Verification Tool). Pre-upgrade verification performs a compatibility analysis of the currently installed Security Management server and of its current configuration. A detailed report is provided, indicating appropriate actions that should be taken before and after the upgrade process. The tool can be used manually as well.
9. Indicate whether to add new products by selecting the Add new products checkbox and click Next.

   Note - When upgrading the Security Management server, SmartReporter is installed by default if it did not previously exist.

10. Depending on the components you have chosen to install, you may need to install other components. Follow the instructions.

11. The new components are installed and the Security Management server is upgraded. The progress of each component is indicated in the progress bar. Upon completion, a summary appears.

   Note - In Windows Server 2003, if Microsoft.Net framework 2.0 has not been installed on the machine, it will be installed automatically before installation of the Check Point components.

12. Follow the instructions for license management and fingerprint handling.
13. Click Finish.

Security Management Server Upgrade on Solaris

This section describes the upgrade process using the R75 DVD. It is recommended that you back up your current configuration before you perform an upgrade process. For additional information, refer to: Backup and Revert for Security Gateways (on page 78). To go back to your previous configuration is required, see Reverting to Your Previous Deployment (on page 82) for details.

To perform an upgrade on a Solaris machine in a production environment:

1. Insert the R75 DVD, and mount the DVD.
2. Run: UnixInstallScript

   The wrapper welcome message is displayed.
3. Enter n.
4. Enter y to agree to the End-user License Agreement, and verify your contract information.

   For more information on contracts, see: On SecurePlatform and Linux (see "On SecurePlatform" on page 62).
5. Select upgrade.

   (It is also possible to upgrade using an imported configuration.)
6. Enter n.
7. Select a source for the upgrade utilities.
   The R75 upgrade utilities are on the R75 DVD.
8. The pre-upgrade verification process runs automatically. View the results and follow any
   recommendations. Then, run the pre-upgrade verifier again. This message is displayed: The pre-
   Upgrade Verification was completed successfully. Your configuration is ready for upgrade.
9. To perform the upgrade, select Upgrade installed products.
   To install additional products, select Upgrade installed products and install new products. You are
   prompted to select the products from a list. Enter n.
10. Enter n to validate the products to install.
    The products are upgraded. Wait until the successful message is displayed.
11. Enter e to exit.

Security Management Server Upgrade on Linux

This section gives the steps for upgrading to R75 using the installation DVD.

To perform an in-place upgrade:
1. Insert the R75 DVD, and mount the DVD.
2. From the root directory, run: UnixInstallScript
   The wrapper welcome message is displayed.
3. Enter n.
4. Enter y to agree to the End-user License Agreement, and verify your contract information.
   For more information on contracts, see: On SecurePlatform and Linux (see “On SecurePlatform” on
   page 62).
5. Select upgrade.
6. Enter n.
7. Select a source for the upgrade utilities.
   Although the R65 upgrade utilities are on the R75 DVD, it is recommended to download the latest tools
   from the Check Point website:
8. The pre-upgrade verification process runs automatically. View the results and follow any
   recommendations. Then, run the pre-upgrade verifier again. This message is displayed: The pre-
   Upgrade Verification was completed successfully. Your configuration is ready for upgrade.
9. To perform the upgrade, specify Upgrade installed products.
   To install new products, select Upgrade installed products and install new products, select the
   products, and enter n.
10. Enter n to validate the products to install.
    The products are upgraded.
11. Enter e to exit.

Upgrading Security Gateways

You can upgrade Security Gateways using one of these methods:

- **SmartUpdate**: Centrally upgrade and manage Check Point software and licenses from a SmartConsole
  client.
- **Local Upgrade**: Do a local upgrade on the Security Gateway itself.
Upgrading a Cluster Deployment

You can use one of these methods to upgrade a cluster deployment:

- **Minimal Effort Upgrade**: Select this option if you have a period of time during which network downtime is allowed. The minimal effort method is much simpler because the clusters are upgraded as gateways and therefore can be upgraded as individual gateways.

- **Zero Downtime**: Select this option if network activity is required during the upgrade process. The zero downtime method assures both inbound and outbound network connectivity at all times during the upgrade. There is always at least one active member that handles traffic.

For more details, refer to Upgrading ClusterXL Deployments (on page 99).

Upgrading Gateways using SmartUpdate

SmartUpdate upgrades gateways and other OPSEC products from a central management client. This makes sure that the latest software versions are deployed throughout the network. SmartUpdate uses a simple point and click interface to do these management tasks.

The R75 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=11647) includes supported upgrade paths and supported platforms information.

**To upgrade SecurePlatform using a DVD:**

1. Log in to SecurePlatform (expert mode is not necessary).
2. Apply the SecurePlatform R75 upgrade package: `# patch add cd`
3. Select the SecurePlatform upgrade package (`CPspupgrade_<version_number>.tgz`)
4. Enter `y` to accept the MD5 checksum calculation.
5. When prompted, create a backup image for automatic revert.

   A Safe Upgrade will be done. Safe Upgrade automatically takes a snapshot of the entire system so that the entire system (operating system and installed products) can be restored if something goes wrong during the Upgrade process (for example, hardware incompatibility). If the Upgrade process detects a malfunction, it automatically reverts to the Safe Upgrade image.

   When the Upgrade process is complete, upon reboot you are given the option to manually start the SecurePlatform operating system using the upgraded version image or using the image created prior to the Upgrade process.

6. After you complete the upgrade process, do the following:
   a) Using SmartDashboard, log in to the R75 Security Management server that controls the upgraded gateway.
   b) Open the gateway object properties window for the upgraded gateway and change the version to R75.
   c) Do Install Policy on the upgraded gateway.

**SmartUpdate Options**

SmartUpdate is the primary tool used for upgrading Check Point gateways. The following features and tools are available in SmartUpdate:

- **Upgrade All Packages**: This feature allows you to upgrade all packages installed on a gateway. For IPSO and SecurePlatform, this feature also allows you to upgrade your operating system as a part of your upgrade. The SmartUpdate “Upgrade all Packages” option supports HFAs, i.e., it will suggest upgrading the gateway with the latest HFA if a HFA package is available in the Package Repository. “Upgrade All” is the recommended method. In addition, there is an advanced method to install (distribute) packages one by one.

- **Add Package to Repository**: SmartUpdate provides three “helper” tools for adding packages to the Package Repository:

- **From CD/DVD**: Adds a package from the Check Point DVD.
- **From File**: Adds a package that you have stored locally.
- **From Download Center**: Adds a package from the Check Point Download Center.
Upgrading Security Gateways

- **Get Check Point Gateway Data**: This tool updates SmartUpdate with the current Check Point or OPSEC third-party packages installed on a specific gateway or for your entire enterprise.

- **Check for Updates**: This feature, available from the SmartDashboard Tools menu, locates the latest HFA on the Check Point Download Center, and adds it to the Package Repository.

**Configuring the Security Management Server for SmartUpdate**

To configure the Security Management server for SmartUpdate:

1. Install the latest version of SmartConsole, including SmartUpdate.
2. Define the remote Check Point gateways in SmartDashboard (for a new Security Management server installation).
3. Verify that your Security Management server contains the correct license to use SmartUpdate.
4. Verify that the Administrator SmartUpdate permissions (as defined in the cpconfig configuration tool) are Read/Write.
5. To enable SmartUpdate connections to the gateways, make sure that Policy Global Properties > FireWall > Firewall Implied Rules > Accept SmartUpdate Connections (SmartUpdate) is selected. By default, it is selected.

**Add Packages to the Package Repository**

Use SmartUpdate to add packages to and delete packages from the Package Repository:

- directly from the Check Point Download Center website (Packages > Add > From Download Center),
- by adding them from the Check Point DVD (Packages > Add > From CD/DVD),
- by importing a file (Packages > Add > From File).

When adding the package to the Package Repository, the package file is transferred to the Security Management server. When the Operation Status window opens, you can verify the success of the operation. The Package Repository is then updated to show the new package object.

**Gateway Upgrade Process Using SmartUpdate**

To update a gateway using SmartUpdate:

1. From SmartUpdate > Packages > Upgrade All Packages select one or more gateways and click Continue.
   - The Upgrade All Packages window opens, and in the Upgrade Verification list you can see which gateways can or cannot be upgraded.
     - To see a list of which packages will be installed on the gateways that can be upgraded, select the gateway and click the Details button.
     - For an explanation as to why a gateway cannot be upgraded, select the relevant gateway and click the Details button.
2. From the list provided, select the gateways that can be upgraded and click Upgrade.

   **Note** - The Allow reboot... option (selected by default) is required in order to activate the newly installed packages.

The Operation Status pane opens and shows the progress of the installation. Each operation is represented by a single entry. Double click the entry to open the Operation Details window, which shows the operation history.

The following operations are performed during the installation process:

- The Check Point Remote Installation Daemon connects to the Check Point gateway.
- Verification for sufficient disk space.
- Verification of the package dependencies.
- The package is transferred to the gateway if it is not already there.
- The package is installed on the gateway.
- Enforcement policies are compiled for the new version.
- The gateway is rebooted if the Allow Reboot option was selected and the package requires it.
The gateway version is updated in SmartDashboard.
The installed packages are updated in SmartUpdate.

Gateway Upgrade on SecurePlatform

Upgrading to R75 on SecurePlatform operating system requires updating both operating system and software products installed. SecurePlatform users should follow the relevant SecurePlatform upgrade process.

For a list of supported upgrade paths, refer to the *R75 Release Notes* (http://supportcontent.checkpoint.com/documentation_download?ID=11647).

The process described in this section upgrades all components (Operating System and software packages) in a single upgrade process. No further upgrades are required. The single upgrade package contains all necessary software items. For more details, refer to the *R75 SecurePlatform Administration Guide* (http://supportcontent.checkpoint.com/documentation_download?ID=11666).

**Important** - Before upgrading a SecurePlatform gateway to R70 or higher from NGX R65 with HFA 40 or HFA 50, you must follow the instructions in sk43247 (http://supportcontent.checkpoint.com/solutions?id=sk43247).

If you need to revert to your previous configuration, refer to *Reverting to Your Previous Deployment* (on page 82).

Upgrading SecurePlatform Using a DVD

This section describes how to upgrade SecurePlatform using an optical drive.

**To upgrade SecurePlatform using a DVD:**
1. Log in to SecurePlatform (*expert* mode is not necessary).
2. Apply the SecurePlatform R75 upgrade package: `# patch add cd`
3. Select the SecurePlatform upgrade package (`CPspupgrade_<version_number>.tgz`)
4. Enter `y` to accept the MD5 checksum calculation.
5. When prompted, create a backup image for automatic revert.

A Safe Upgrade will be performed. Safe Upgrade automatically takes a snapshot of the entire system so that the entire system (operating system and installed products) can be restored if something goes wrong during the Upgrade process (for example, hardware incompatibility). If the Upgrade process detects a malfunction, it automatically reverts to the Safe Upgrade image.

When the Upgrade process is complete, upon reboot you are given the option to manually start the SecurePlatform operating system using the upgraded version image or using the image created prior to the Upgrade process.

6. After you complete the upgrade process, do the following:
   a) Using SmartDashboard, log in to the R75 Security Management server that controls the upgraded gateway.
   b) Open the gateway object properties window for the upgraded gateway and change the version to R75.
   c) Perform Install Policy on the upgraded gateway.

Gateway Upgrade on a UTM-1/Power-1 Appliance

Upgrading to R75 can only be done using the WebUI.

**To upgrade your appliance using the WebUI:**
1. Download an upgrade package from the Check Point User Center.
2. Select the upgrade package file.
3. Click *Upload upgrade package to appliance*.
   The *Upload Package to Appliance* window opens.
4. Browse to the upgrade (.tgz) file and select it.
5. Click Upload and wait until the package uploads
6. Click **Start Upgrade**.
7. Before the upgrade begins, an image is created of the system and is used to revert to in the event the
upgrade is not successful. The **Save an Image before Upgrade** page, displays the image information.
8. Click **Next**.
9. In the **Safe Upgrade** section, select **Safe upgrade** to require a successful login after the upgrade is
complete. If no login takes place within the configured amount of time, the system will revert to the
saved image.
   Click **Next**.
10. The **Current Upgrade File on Appliance** section displays the information of the current upgrade.
    To begin the upgrade, click **Start**.

### Gateway Upgrade on an IP Appliance

Use the procedures in this section to:
- Add the new version of IPSO (also known as an IPSO image)
- Add the R75 release package
- Add other packages

These procedures do not remove the existing images, packages, or your configuration information. If you
add a new version, you can revert to the earlier versions stored on the platform. When you revert, your IPSO
configuration information is not affected.

You can add IPSO images, R75 and other packages to the IP Appliance with Network Voyager or with the
CLI shell.

When you add an IPSO image, the IPSO boot manager is upgraded automatically if your system does not
have the boot manager for the image you are adding based network element management application. Use
a console to perform the initial configuration.

### Adding and Activating an R75 Package Using Network Voyager

To install and activate an R75 package using Network Voyager:
1. Download the applicable release package for your platform to an FTP site or to your local disk.

   **Important** - Installing the incorrect package can damage your platform.

<table>
<thead>
<tr>
<th>IP Appliance Platform type</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk based</td>
<td>IPSO6_wrapper_R75.tgz (<a href="http://supportcenter.checkpoint.com/file_download?id=11773">http://supportcenter.checkpoint.com/file_download?id=11773</a>)</td>
</tr>
<tr>
<td>Flash based</td>
<td>Check_Point_R75_Security_Gateway_for_IPSO6_2.tgz (<a href="http://supportcenter.checkpoint.com/file_download?id=11772">http://supportcenter.checkpoint.com/file_download?id=11772</a>)</td>
</tr>
</tbody>
</table>

   **Note** - This package does not include CPinfo. See sk30567 ([http://supportcontent.checkpoint.com/solutions?id=sk30567](http://supportcontent.checkpoint.com/solutions?id=sk30567)) for download information.

2. Enter Network Voyager,
3. Choose **Configuration > System configuration > Packages > Install Packages**
4. Choose the remote location of the package.
   - **FTP** to upload from an FTP server
   - **Upload** to upload from a local machine
5. For FTP, enter the FTP site location and credentials.
6. For both FTP and Upload method, choose the package.
7. Click **Save**.
8. Click the link to upgrade the package.
9. In the Package Installation and Upgrade window, select Upgrade, and select the package to Upgrade From.
10. Click Apply.
   The upgrade begins.
11. To monitor progress, click the Install package link. The upgrade log is shown.
12. When an "Installation Completed" message appears, click Save.
   Reboot the system.
   After the reboot, R75 will be active.
13. To verify that R75 is active, run the CLI command: `newpkg -q`

Adding and Activating an R75 Package Using the CLI Shell

To install and activate the R75 package using the CLI shell:

1. Download the applicable release package for your platform to an FTP site or to your local disk.
   **Important** - Installing the incorrect package can damage your platform.

<table>
<thead>
<tr>
<th>IP Appliance Platform type</th>
<th>Package</th>
</tr>
</thead>
</table>
   | Disk based                | IPSO6_wrapper_R75.tgz (
   |                           | **Note** - This package does not include CPinfo. See sk30567 ( [http://supportcontent.checkpoint.com/solutions?id=sk30567](http://supportcontent.checkpoint.com/solutions?id=sk30567) ) for download information. |

   2. Access the CLI console, and log in.
   3. Type `newpkg`, and press Enter.
   4. Use the FTP menu option to transfer the R75 package. Choose the option:
      Upgrade from an old package.
   5. Upgrade to the R75 package.
      Wait until a message informs you that the process is complete.
   6. Type `reboot` and press Enter.
      The package is activated after the reboot.
   7. Verify that R75 is active by running the following command `newpkg -q`.
   8. Verify that R75 is the current version. Run `fw ver` on a Security Gateway or `fwm ver` on a Security Management server.

Updating the Security Gateway Version in SmartDashboard

At this point the IP Appliance enforces the Initial Policy which does not allow http connections. It is therefore not possible to connect via Network Voyager. To enforce the Security Policy and make it possible to connect to the IP Appliance via Network Voyager, install the Security Policy (that allows http) via SmartDashboard.

To install the Policy on the IP Appliance:

1. Log in to the R75 SmartDashboard that controls the Security Management Server that manages the IP Appliance.
2. Edit the Check Point Security Gateway object of the IP Appliance.
4. Install the Policy.
Gateway Upgrade Process on a Windows Platform

This section describes the upgrade process using the R75 Installation DVD.

To upgrade a gateway in a Windows platform:
1. Insert the R75 DVD.
2. If the upgrade does not start automatically, run Setup.exe from the DVD.
3. Click Next to start the installation wizard.
4. Accept the license agreement and click Next.
5. Click Next to check your license information.
6. Select one of the license options and click Next.
7. To add Check Point products that were not installed previously, select Install additional Check Point products and click Next.
8. Select the new products to install.
9. A list of the products that will be upgraded or installed. Click Next to start the installation.
10. When the installation is finished, click Next to continue.
11. In Licenses and Contracts, select a licensing option and click Next.
12. In Secure Internal Communication, verify the SIC details and click Next.
13. In Clustering, select whether this Security Gateway is part of a cluster.
14. Click Finish to close the installation wizard.

When the upgrade process is complete:
1. Using SmartDashboard, log in to the R75 Security Management server that controls the upgraded gateway.
2. Open the gateway object properties window that represents the upgraded gateway and change the version to R75.
3. Do Install Policy on the upgraded gateway.

If need to revert to your previous configuration, refer to Reverting to Your Previous Deployment (on page 82) for details.
Chapter 11
Backup and Revert for Security Gateways

In This Chapter

Introduction 78
Backing Up Your Current Deployment 78
Restoring a Deployment 79
SecurePlatform Backup and Restore Commands 79
SecurePlatform Snapshot Image Management 81
Reverting to Your Previous Deployment 82

Introduction

Before you perform an upgrade process, you should back up your current configuration. The purpose of the backup process is to back up the entire configuration, and to restore it if necessary, for example, in the event that the upgrade process is unsuccessful.

To back up your configuration, use the Export utility tool of the version for which you are creating a backup file. The backup file contains your current system configuration (for example, objects, rules, and users) and can be used to restore your previous configuration if the upgrade process fails. The restoration procedure restores the configuration in effect when the backup procedure was executed.

Note - Operating system level configurations (for example, network configuration) are not exported.

If you are performing an upgrade process on SecurePlatform, you do not have to back up your configuration using the Export utility. SecurePlatform provides the option of backing up your configuration during the Upgrade process.

Backing Up Your Current Deployment

To back up your current deployment:
1. In the original Security Management server, insert the product DVD for the version you are backing up.
2. Select the Export option in the installation wizard, or use the Export tool located in the relevant operating system directory on the product DVD.

Once the Export utility process is complete, the configuration file is created in the chosen destination path in a tar gzip format (.tgz).

Important - The configuration file (.tgz) contains your product configuration. It is highly recommended to delete it after completing the import process.
Restoring a Deployment

To restore a deployment:
1. Copy the exported.tgz file to the target Security Management server.
2. In the Security Management server, insert the product DVD for the version being restored.
3. Using the available options, perform an installation using an imported configuration file.

SecurePlatform Backup and Restore Commands

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

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

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

The restore utility is used for restoring SecurePlatform settings and/or product configurations from backup files.

Expert permissions are required to perform the backup and restore procedures.

Backup

This command is used to back up the system configuration. You can also copy backup files to a number of SCP and TFTP servers for improved backup robustness. The backup command, when run by itself without any additional flags, uses default backup settings and performs a local backup.

Syntax

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

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>Enables VPN log backup (By default, VPN logs are not backed up.)</td>
</tr>
<tr>
<td>--purge DAYS</td>
<td>Deletes old backups from previous backup attempts</td>
</tr>
</tbody>
</table>
SecurePlatform Backup and Restore Commands

### Backup and Revert for Security Gateways

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| [-sche[d <hh:mm <m
DayOfMonth> | <w
DaysOfWeek>] | off] | Schedule interval at which backup is to take place |
|                            | • On - specify time and day of week, or day of month                  |
|                            | • Off - disable schedule                                              |
| --tftp <ServerIP> [-path <Path>] | List of IP addresses of TFTP servers, on which the configuration is to be backed up, and optionally the filename |
| --scp <ServerIP> <User name> <Password>[-path <Path>] | List of IP addresses of SCP servers, on which the configuration is to be backed up, the user name and password used to access the SCP server, and optionally the filename |
| --file [-path <Path>] | When the backup is performed locally, specify an optional 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;Server IP&gt; [Filename]</td>
<td>IP address of TFTP server, from which the configuration is restored, and the filename</td>
</tr>
<tr>
<td>--scp &lt;Server IP&gt; &lt;User name&gt; &lt;Password&gt; [Filename]</td>
<td>IP address of SCP server, from which the configuration is restored, the user name 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>


### Restore

This command is used to restore the system configuration.

**Syntax**

```
restore [-h] [-d][|--tftp <Server IP> <Filename>] | |
|--scp <Server IP> <User name> <Password>
<Filename>] | |
|--file <Filename>] |
```
SecurePlatform Snapshot Image Management

SecurePlatform provides the option of backing up the entire SecurePlatform operating system and all of its products using the `snapshot` command.

A snapshot of the system can be taken manually using the `snapshot` command or automatically during an upgrade procedure using the SafeUpgrade option.

Having a snapshot of the entire operating system enables you to restore SecurePlatform if needed. Similar to Backup and Restore, the Snapshot and Revert features ensure easy maintenance and management, even if a situation arises that demands that you undo an upgrade and revert to a previous deployment.

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

Note - The `snapshot` and `revert` commands are relevant only for reverting R75 to a previous version on SecurePlatform. If you are using another platform, see Reverting to Your Previous Deployment (on page 82).

### Snapshot

This command creates an image of SecurePlatform. The `snapshot` command, run by itself without any additional flags, uses the default backup settings and creates a local snapshot.

#### Syntax

```
```

### Revert

This command restores SecurePlatform from a snapshot file, reverting the machine to a previous deployment. The `revert` command, run by itself without any additional flags, uses default backup settings, and reboots the system from a local snapshot.

```
```

### Revert Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>obtain usage</td>
</tr>
<tr>
<td>-d</td>
<td>debug flag</td>
</tr>
</tbody>
</table>

---

Backup and Revert for Security Gateways   Page 81
Reverting to Your Previous Deployment

To revert to a version that was active before it was upgraded to R75, perform the procedures described in this section, according to the platform you have. This will uninstall the last active version only, and leave the previously installed version as the now-active version.

To an Earlier Version on SecurePlatform

To revert to a prior software version (R70 or R6X) on SecurePlatform:
1. Before upgrading to the newer version, take a snapshot (on page 81).
2. Copy the snapshot file from /var/CPsnapshot/snapshots to an external server.
3. Reinstall the machine with the relevant software (R70 or R6X).
4. Copy the snapshot file taken in step 1 above to /var/CPsnapshot/snapshots using TFTP, FTP or SCP server.
5. Use the Revert (on page 81) command to restore your configuration.

To an Earlier Version on an IP Appliance

You can revert to an earlier version that is compatible with IPSO version 6.2, such as R70 or R71.

To revert to an earlier version on an IP appliance using Voyager:
1. Go to Configuration > System Configuration > Packages > Manage Packages.
2. Clear the Enable checkbox for the current package, Check Point R75 and click Apply.
3. Click the link Click to check the status of the operation. There is no check in the checkbox.
4. Click the Enable checkbox for the version you would like to revert to and click Apply.
5. Click the link Click to check the status of the operation. There is no check in the checkbox. The installation starts.
6. Upon completion, a success message appears.
7. Save the configuration. At the bottom of the page, click Save.
8. Reboot the appliance.

To revert to an earlier version on an IP appliance using the CLI:
1. At the CLI command prompt type clish.

Note - The clish shell cannot be used on a system that was previously accessed by Network Voyager or another user, because the system is locked. To unlock the system, run the command set config-lock on override.
2. **Type** `show package active`

3. To set the active package to inactive, **type**
   ```
   set package name <directory_name> off
   ```
   **For example:**
   ```
   set package name /opt/CPsuite-R71 off
   ```

4. **To revert to a previous package,** **type**
   ```
   set package name <directory_name> on
   ```
   **For example:**
   ```
   set package name /opt/CPsuite-R65 on
   ```

5. Upon completion of the installation, a success message appears.

6. Reboot the appliance.

---

**To an Earlier Version on a Windows Platform**

To revert to a prior software version on a Windows platform:

1. In Add/Remove Programs, select **Check Point <product> R75**.
2. Click **Remove**.

   The latest version is uninstalled, and the previous version is active.

---

**To an Earlier Version on a Solaris Platform**

To revert to a prior software version on a Solaris platform:

1. For each installed package, other than CPSuite, run the command:
   ```
   pkgrm <file>-R75.
   ```
2. Run the command: `pkgrm CPsuite-R75`.

   The latest version is uninstalled, and the previous version is active.

---

**To an Earlier Version on a Linux Platform**

To revert to a prior software version on a Linux platform:

1. To view a list of all the installed packages, run:
   ```
   rpm -qa | grep CP
   ```
2. For each installed package, other than CPSuite, run the command:
   ```
   rpm -e <file>-R75-00.
   ```
3. Run the command: `rpm -e CPsuite-R75-00`.

   The latest version is uninstalled, and the previous version is active.

---

**ICA Considerations**

Once the Revert process is complete, certificates issued during the use of R75 remain valid. While these certificates are valid, they cannot be processed by the Internal CA.

**To resume management of older certificates after the Revert process:**

1. **Back up the InternalCA.NDB and ICA.crl files** (located in the `$FWDIR/conf` directory) and all `*.crl` files (located in the `$FWDIR/conf/crl` directory) from the version prior to R75 to a suitable location.
2. **Copy the R75 InternalCA.NDB, ICA.crl and the `*.crl` files** (located in the `$FWDIR/conf` directory) from the current R75 version and use them to overwrite the files in the location specified in the `$FWDIR/conf` directory).
Note - If the Upgrade process was performed on a machine that runs a different operating system than the original machine, the InternalCA.NDB file must be converted after it is copied to the reverted environment. To do this, run the cpca_dbutil d2u command line from the reverted environment.

3. Once the Revert process is complete, use the ICA Management Tool to review certificates created using R75 in the reverted environment. For example, the subject to which a specific certificate was issued may no longer exist. In such a case, you may want to revoke the specific certificate.

For additional information, refer to The Internal Certificate Authority (ICA) and the ICA Management Tool chapters in the R75 Security Management Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11667).
Chapter 12

Upgrading a Standalone Deployment

In This Chapter

Introduction 85
Pre-Upgrade Considerations 85
Standalone Security Gateway Upgrade on a Windows Platform 86
Standalone Security Gateway Upgrade on SecurePlatform 87
Standalone Gateway Upgrade on an IPSO Platform 88
Standalone Upgrade on a UTM-1/Power-1 Appliance 88

Introduction

This chapter describes the process of upgrading a standalone deployment to R75. A standalone deployment consists of the Security Management server and gateway installed on the same system. Since backward compatibility is supported, a Security Management server that has been upgraded to R75 can enforce and manage gateways from previous versions. In some cases, however, new features may not be available on earlier versions of the gateway. For more information, see Compatibility Tables.

Note - R75 cannot manage gateway versions NG, NG FP1, or NG FP2.

Pre-Upgrade Considerations

Upgrading Products on a SecurePlatform Operating System

Upgrading to R75 on a SecurePlatform operating system requires upgrading both the operating system and the installed software products.

To upgrade products installed on SecurePlatform, refer to Standalone Security Gateway Upgrade on SecurePlatform (on page 87).

This process upgrades all the installed components (Operating System and software packages) in a single upgrade process. No further upgrades are required.

Reverting to Your Previous Software Version

Before you perform an upgrade process you should back up your current SecurePlatform configuration. The purpose of the backup process is to back up the entire SecurePlatform configuration, and to restore it if necessary, for example, in the event that the Upgrade process is unsuccessful.

Important - For all operating systems except SecurePlatform, an R75 upgrade cannot be reverted to its previous version, once it is complete.
To back up your configuration, use the SecurePlatform snapshot and revert commands (for additional information, refer to SecurePlatform Backup and Restore Commands (on page 79)).

**Using the Pre-Upgrade Verification Tool**

We recommend that you run the pre-upgrade verifier on the Security Management server source computer before export the management database. The pre-upgrade verifier does a compatibility analysis of the Security Management server database and its current configuration. A detailed report shows the steps to do before and after the upgrade.

The pre-upgrade verifier can only verify a database that is intended for import into a different major version of the Security Management server. It cannot be used on a database that is intended for import into the same major version of the Security Management server.

**Action Items**

- **Errors** - Issues that must be resolved before you can continue with the upgrade. If you proceed without correcting these errors, the upgrade may fail, or you may have problems after upgrade.
- **Warnings** - Issues that are recommended to resolve before or after the upgrade.

**Standalone Security Gateway Upgrade on a Windows Platform**

It is recommended that before you perform an upgrade process, you should back up your current configuration, in case the upgrade process is unsuccessful. For additional information, refer to Backing Up Your Current Deployment (on page 78).

⚠️ **Important** - For all operating systems except SecurePlatform, an R75 upgrade cannot be reverted to its previous version once it is complete.

**To perform an upgrade on a Windows platform:**

1. Insert the R75 DVD into the optical drive.
2. Execute the Installation package.
3. Agree to the EULA and verify your contract information.
   For more information on contracts, On a Windows Platform (on page 61).
4. From the **Upgrade Options** screen, select **Upgrade**.
5. When the pre-upgrade verification recommendation appears, select whether or not the Pre-upgrade verification tool should be executed (refer to Using the Pre-Upgrade Verification Tool). Pre-upgrade verification performs a compatibility analysis of the currently installed gateway and its current configuration. A detailed report is provided, indicating appropriate actions that should be taken before and after the upgrade process. The tool can be used manually as well.
6. From the **Upgrade Options** screen, select **Upgrade** again.
   The Pre-Upgrade Verification runs again.
7. Reboot when prompted.

**Uninstalling Packages**

Uninstall Check Point packages on the Windows platform using the Add/Remove applet in the Control Panel. Check Point packages need to be uninstalled in the opposite order to which they were installed. Since CPsuite is the first package installed, it should be the last package uninstalled.
Standalone Security Gateway Upgrade on SecurePlatform

Upgrading to R75 on a SecurePlatform operating system requires updating both the operating system and the installed software products.

For a list of supported upgrade paths, see the R75 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=11647).

The process described in this section upgrades all of the components (Operating System and software packages) in a single upgrade process. No further upgrades are required. The single upgrade package contains all necessary software items.

**Important** - For all operating systems except SecurePlatform, an R75 upgrade cannot be reverted to its previous version once it is complete.

**To perform an upgrade on a SecurePlatform server:**

1. Insert R75 DVD into the optical drive.
2. At the command prompt, enter `patch add cd`.
3. Select **SecurePlatform R75 Upgrade Package** (CPspupgrade_<version_number>.tgz).
4. Enter `y` to accept the checksum calculation.
5. When prompted, create a backup image for automatic revert.
   - **Note** - Creating the snapshot image can take up to twenty minutes, during which time Check Point products are stopped.
6. The **welcome** message is displayed. Enter `n`.
7. Accept the license agreement, and verifying your contract information.
   - For more information on contracts, On SecurePlatform and Linux (see "On SecurePlatform" on page 62).
8. Three upgrade options are displayed:
   - Upgrade
   - Export the configuration
   - Perform pre-upgrade verification only
     - (i) Run the pre-upgrade verification script, and follow the recommendations contained in the pre-upgrade verification results. Repeat the process until you see **Your configuration is ready for upgrade**.
     - (ii) Export the configuration.
     - (iii) Upgrade the installation.
9. Enter `c` to agree to the license upgrade.
   - The license upgrade process also handles gateway licenses in the SmartUpdate license repository. Select one of the following:
     - Enter [L] to view the licenses installed on your machine.
     - Enter [C] to check if currently installed licenses have been upgraded.
     - Enter [S] to simulate the license upgrade.
     - Enter [U] to perform the license upgrade, or generate a license file that can be used to upgrade licenses on a machine with no Internet access to the User Center.
     - Enter [O] to perform the license upgrade on a license file that was generated on machine with no Internet access to the User Center.
     - Enter [Q] to quit.
10. Select a source for the upgrade utilities
    - Either download the most updated files from the Check Point website or use the upgrade tools contained on the DVD. The exported configuration is automatically imported during the upgrade process.
11. Open SmartUpdate and attach the new licenses to the gateways.
Uninstalling Packages

Check Point packages need to be uninstalled in the opposite order to which they were installed. Since CPsuite is the first package installed, it should be the last package uninstalled.

Run the `rpm -qa <package name>` to view a list of the installed packages.

Standalone Gateway Upgrade on an IPSO Platform

To upgrade a standalone gateway on an IP Appliance, IPSO platform, follow the procedure for upgrading a gateway. However, ignore all instructions that apply only to flash-based IP Appliances, because a standalone gateway includes a Security Management Server, and a flash-based IP Appliance cannot be used as a Security Management Server. See Gateway Upgrade on an IPSO Platform ("Gateway Upgrade on an IP Appliance" on page 75).

Standalone Upgrade on a UTM-1/Power-1 Appliance

Upgrading to R75 can only be done using the WebUI.

To upgrade your appliance using the WebUI:
1. Download an upgrade package, as directed.
2. Select the upgrade package file.
3. Click Upload upgrade package to appliance.
   The Upload Package to Appliance window opens.
4. Browse to the upgrade (tgz) file and select it.
5. Click Upload and wait until the package uploads
6. Click Start Upgrade.
7. Before the upgrade begins, an image is created of the system and is used to revert to in the event the upgrade is not successful. The Save an Image before Upgrade page, displays the image information. Click Next.
8. In the Safe Upgrade section, select Safe upgrade to require a successful login after the upgrade is complete. If no login takes place within the configured amount of time, the system will revert to the saved image. Click Next.
9. The Current Upgrade File on Appliance section displays the information of the current upgrade.
10. To begin the upgrade, click Start..

Uninstalling Packages

Check Point packages need to be uninstalled in the opposite order to which they were installed. For example, since CPsuite is the first package installed, it should be the last package uninstalled.

Run the `rpm -e <package name>` to view a list of the installed packages.
Chapter 13

Advanced Security Management Server Upgrade and Database Migration

In This Chapter

Overview .......................................................... 89
Upgrade Workflow .............................................. 90
Using the Pre-Upgrade Verification Tool .............. 97
Migrate Command Reference ............................... 98

Overview

This chapter gives a description of the basic upgrade workflow and the detailed procedures for different platforms and upgrade scenarios.

Using advanced upgrade, you install R75 on a different computer. This is typically a clean installation, but you can also use another existing server. You then migrate the management databases from the existing (source) computer to the new (target) computer using the migrate command or the installation DVD.

You can do an advanced upgrade on primary and secondary Security Management servers. Advanced upgrade has these advantages:

- Prevents unnecessary down time during the upgrade.
- Lets you test the new version before you use it.
- Lets you move your Security Management server to a different platform.

Important -

- The set of products installed on the target computer must be equal to or greater than the set of products installed on the source.
- The version of the Security Management server on the target must be equal to or greater than the version of the Security Management server on the source.
- The target computer can be a different platform.
- The advanced upgrade procedure does not automatically migrate the SmartReporter to the target computer. Use the SmartReporter database migration procedure (see "SmartReporter Advanced Upgrade" on page 96) to do this.
- The advanced upgrade procedure does not automatically migrate the SmartEvent management database to the target computer.
Before Advanced Upgrade

After Advanced Upgrade

<table>
<thead>
<tr>
<th>Key</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Source computer</td>
<td>1</td>
<td>Target R75 computer connected to network</td>
</tr>
<tr>
<td>2</td>
<td>Management database migration path</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>R75 target computer, not connected to the network</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Supported Upgrade Paths, Platforms and Products**

If upgrading to R75, ensure that the upgrade from the version on the source computer is a supported. For a list of supported upgrade paths, platforms and products, see the R75 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=11647).

**Upgrade Workflow**

This section includes a procedural overview for advanced upgrades and continues with detailed procedures for each platform. Also included are special procedures for:

- Upgrading a secondary Security Management server
- Migrating to a computer with a different IP address
- Advance upgrade for deployments using SmartReporter

**Advanced Upgrade Workflow**

1. Prepare Source for Export
2. Install New Version on Target
3. Export Databases From Source
4. Import Databases to Target
5. Test Target Deployment
6. Connect Target to Network
In this section:

- General Workflow
- Platform-Specific Procedures
- Upgrading a Secondary Security Management Server
- Migrating to a Computer with a Different IP Address
- SmartReporter Advanced Upgrade

**General Workflow**

**Do these steps on the source computer:**

1. Make sure to read the R75 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=11647) to make sure that your upgrade path is supported.

2. Use one of these ways to get the R75 migration tools:
   - Download the R75 migration tools from the Support Center (https://support.checkpoint.com). This is the best way to make sure that you get the most recent version. In the Support Center:
     - (i) Search for "R75 migration tools".
     - (ii) Filter by target version.
     - (iii) Filter by target operating system.
   - OR
   - If source and target machines are the same platform, copy $FWDIR/bin/upgrade_tools on Unix platforms or %FWDIR%\bin\upgrade_tools on the Windows platform from the target computer to the source computer. You need to install R75 on the target computer before doing this.

   **Note:**
   - Copy the migration tools to a directory of your choice, such as /var/tmp.
   - Do not overwrite existing tools.

3. Run `fw logswitch` to close the SmartView Tracker log files (optional). Only closed logs are migrated.

4. Do not do this step for standalone deployments: Close all Check Point GUI clients that are connected to the Security Management server. Alternatively, you can run the `cpstop` command on the source computer.

   **Important**: If you don't close the GUI clients or run `cpstop`, the exported management database can become corrupted.

5. Run the `pre_upgrade_verifier` command (see "Using the Pre-Upgrade Verification Tool" on page 65).

6. Correct all errors before continuing.

7. Do the platform-specific export procedure (see "Platform-Specific Procedures" on page 92) to create the management database export file.

8. If SmartReporter is installed on the source computer, export the SmartReporter management database (see “SmartReporter Advanced Upgrade” on page 96).

**Do these steps on the target computer:**

1. Install the R75 Security Management server or a standalone deployment (see "Installing Security Gateways, Security Management and Endpoint Security" on page 15) on the target computer. Configure as required.

2. Get the most updated R75 migration tools for the target platform (recommended) or use the installed migration tools in $FWDIR/bin/upgrade_tools on Unix platforms or %FWDIR%\bin\upgrade_tools on Windows.

3. Do the platform-specific import procedure (see "Platform-Specific Procedures" on page 92) to import the management database from the source computer to the target.
4. If SmartReporter is installed on the source computer, import the SmartReporter management database (see "Importing the SmartReporter Management Database" on page 97).

5. Test the target installation.

6. Disconnect the source computer from the network.

7. Connect the target computer to the network.

Licenses are related to the Security Management server IP address. We recommend that you keep the same IP address for the target Security Management server. If you are using a different IP address, see Migration to a New Machine with a Different IP Address (see "Migrating to a Computer with a Different IP Address" on page 95).

Platform-Specific Procedures

This section includes the platform-specific procedures for exporting and importing the Security Management Server database files. These procedures are only part of the general procedure (see "General Workflow" on page 91) for advanced upgrades.

In this section:

- Advanced Upgrade on SecurePlatform
- Advanced Upgrade on Linux or Solaris Platforms
- Advanced Upgrade on the IPSO Platform
- Advanced Upgrade on the Windows Platform

Advanced Upgrade on SecurePlatform

This section gives detailed procedures for importing and exporting the Security Management Server database on SecurePlatform.

In this section

- Exporting the Management Database using the Command Line
- Exporting the Management Database using the Graphical Interface from the DVD
- Importing the Management Database

Exporting the Management Database using the Command Line

To create a management database export file on the source computer:

1. Log in to the expert mode.
2. Get the R75 migration tools.
3. Run:
   
   ```
   <path to migration tools directory>/migrate export <exported database name>.tgz.
   ```

4. Do the instructions shown on the screen. This creates the `<exported database name>.tgz` file.

Exporting the Management Database using the Graphical Interface from the DVD

To create a management database export file on source SecurePlatform computer using the installation DVD:

1. Insert the R75 DVD into source computer drive.
2. At the command prompt, run:
   
   ```
   patch add cd
   ```

4. Enter y to confirm the checksum calculation.
5. You are prompted to create a backup image for automatic revert. There is no need to create a backup image now because exporting the management database does not change the system.
Note - Creating a snapshot image can take up to twenty minutes, during which time Check Point products are stopped.

7. Press Y to accept the license agreement.
9. Select a source for the upgrade utilities. We recommend that you select Download the most updated files from the Check Point website to get the latest files. You can also select Use the upgrade tools contained on the CD. Press N to continue.
10. If the Pre-Upgrade Verification fails, correct the errors and restart this procedure from the step 2. Otherwise, press N to continue.
11. In the Export window, press N to continue. The management database is saved in /var/tmp/cpexport.tgz.
12. Press E to exit the installation program.

Importing the Management Database

To import the management database file to the target computer:
1. Log in to the expert mode.
2. Copy the management database file that you exported from the source computer to a directory of your choice on the target computer.
3. Run:
   `<path to migration tools directory>/migrate import <exported database name>.tgz`.
4. Do the instructions on the screen to import the management database.

Advanced Upgrade on Linux or Solaris Platforms

This section gives detailed procedures for importing and exporting the Security Management Server database on Linux and Solaris platforms.

In this section:

Exporting the Management Database using the Command Line

To create a management database export file on the source computer:
1. Get the R75 migration tools.
2. Run:
   `<path to migration tools directory>/migrate export <exported database name>.tgz`.
3. Do the instructions shown on the screen. This creates the `<exported database name>.tgz` file.

Importing the Management Database

To import the management database to the target computer:
1. Copy the management database file that you exported from the source computer to a directory of your choice on the target computer.
2. Run:
   `<path to migration tools directory>/migrate import <exported database name>.tgz`.
3. Do the instructions on the screen to import the management database.
Advanced Upgrade on the IPSO Platform

This section gives detailed procedures for importing and exporting the Security Management Server database on IPSO appliances. Export using the installation DVD is not supported for this platform.

In this section:

- Exporting the Database
- Importing the Database

Exporting the Database

To create a management database export file on the source computer:

1. Get the R75 migration tools.
2. Run:
   `<path to migration tools directory>/migrate export <exported database name>.tgz`.
3. Do the instructions shown on the screen. This creates the `<exported database name>.tgz` file.

Importing the Database

To import the management database file to the target computer:

1. Copy the management database file that you exported from the source computer to a directory of your choice on the target computer.
2. Run:
   `<path to migration tools directory>/migrate import <exported database name>.tgz`.
3. Do the instructions on the screen to import the management database.

Advanced Upgrade on the Windows Platform

This section gives detailed procedures for importing and exporting the Security Management server database on the Windows platform.

In this section

- Exporting the Management Database using the Command Line
- Exporting the Management Database using the Graphical Interface from the DVD
- Importing the Management Database

Exporting the Management Database using the Command Line

To create a management database export file:

1. Get the R75 migration tools.
2. From the Windows command prompt, run:
   `<path to migration tools directory>\migrate.exe export <exported database name>.tgz`.
3. Do the instructions shown on the screen. This creates the `<exported database name>.tgz` file.

Exporting the Management Database using the Graphical Interface from the DVD

To export the management database file:

1. Log in to Windows using Administrator credentials.
2. Insert the R75 DVD in the optical drive.
   If the wizard does not start automatically, run `setup.exe` from the DVD.
3. Click Next in the Thank you window.
4. Accept the terms of the License Agreement and click Next.
5. Select Export.
6. Use one of these options to get the upgrade utilities.
   - Download the most recent upgrade utilities from the Check Point download center (https://support.checkpoint.com).
   - Use the upgrade utilities that you downloaded to your local disk.
   - Use the upgrade utilities on the DVD.
7. If there are pre-upgrade verification errors, correct them and start this procedure again from step 3. Otherwise, click Next to continue.
8. Enter path and management database export file name. The default is: c:\temp\cp_db_configuration.tgz.
9. When the export completes, click OK.

Importing the Management Database

To import the management database file to the target computer:
1. Copy the management database file that you exported from the source computer to a directory of your choice on the target computer.
2. From the Windows command prompt, run:
   <path to migration tools directory>\migrate.exe import <exported database name>.tgz.
3. Do the instructions on the screen to import the management database.

Upgrading a Secondary Security Management Server

To do an advanced upgrade for a Secondary Security Management server, use this workflow:
1. Export the management database file from the primary Security Management server.
   If the primary Security Management server is not available, convert the secondary Security Management server to a primary Security Management server.
2. Install a new primary Security Management server.
3. Import the management database file to the new Primary Security Management server.

Migrating to a Computer with a Different IP Address

Licenses are related to the Security Management server IP addresses. When migrating your current Security Management server, we recommend that you use the same IP address for the target computer.

These sections show the procedures for using a different IP address for your target Security Management server.

Before Migrating Your Source Security Management Server

Do these steps on the source computer before migrating:
1. Create a new host object in SmartDashboard with the IP address of a target Security Management server.
2. Define a firewall rule that allows this new Security Management server to connect to Security Gateways using these services:
   - FW1 (TCP 256)
   - CPD (TCP 18191)
   - FW1_CPRID (TCP 18208)
   The source is the host object created in step 1 and the destination is any. This rule must be the first rule in the Rule Base.
3. Install the new security policy on all gateways.
After Migrating the Security Management Server

Do these steps on the target computer after migrating:
1. Update the Security Management server licenses with the new IP address. If central licenses are in use, they must also be updated with the new IP Address.
2. Run cpstart
3. Connect to the new IP address with SmartDashboard.
4. Remove the host object and rule that you created before the migration.
5. On the target Security Management server, update the primary Security Management server object to make the IP Address and topology match the new configuration.
6. On the DNS, map the target Security Management server host name to the new IP address.

SmartReporter Advanced Upgrade

The Security Management server advanced upgrade does not automatically migrate the SmartReporter management database from the source computer to the target. If you have SmartReporter installed on the source machine, you must do several additional steps to migrate this management database to the target computer.

In this section:
- Exporting the Management Database
- Importing the SmartReporter Management Database
- Completing the SmartReporter Upgrade

Exporting the Management Database

To create the SmartReporter management database export file on the source computer, do these steps:
1. Run cpstop.
2. Find and open the MySQL configuration file using a text editor:
   - On SecurePlatform, Linux and Solaris platforms, the configuration file is: $RTDIR/Database/conf/my.cnf.
   - On Windows platforms, the configuration file is: %RTDIR%\Database\conf\my.ini
   Use this file to locate directory names for use in the next steps.
3. Go to the directory specified by the datadir=<xxx> parameter in the MySQL configuration file.
4. Delete the contents of the directory specified in the innodb_log_group_home_dir= <xxx> setting.
5. Create the SmartReporter management database export file. Assign the name datadir.tgz to this file.
   a) Go to the directory specified by the datadir= <xxx> parameter in the MySQL configuration file.
   b) Use the gtar -zcvf datadir.tgz command to create an archive file containing all files in the directories specified by these parameters.
      - datadir= <xxx>
      - innodb_data_file_path= <xxx>
6. Backup these items to a different device (USB drive, CD, FTP server, network location, etc.):
   - The datadir export file (datadir.tgz).
   - The MySQL configuration file (my.cnf or my.ini). You must change the suffix on the backup device from .cnf or .ini to .old. This suffix is required by the import scripts.
   - Company logo image files located in the $RTDIR/bin (%RTDIR%\bin on Windows) directory.
   - Custom distribution scripts located in $RTDIR/DistributionScripts (%RTDIR%\DistributionScripts on Windows).
   - The evr_addon_export script file located in $RTDIR/conf.
Importing the SmartReporter Management Database

Do these steps on the target computer:
1. If you have not already done so, install R75 (see "Installing Security Gateways, Security Management and Endpoint Security" on page 15) and SmartReporter, on the target computer.
2. Run cpstop.
3. Copy the my.cnf.old (my.ini.old for Windows) to the $RTDIR/Database/conf/ (%RTDIR%\Database\conf for Windows) directory.
4. Copy these files from the backup device to the target computer:
   - The SmartReporter management database export file (datadir.tgz) to the one of these paths:
     - SecurePlatform, Linux or Solaris: $RTDIR/bin
     - Windows: %RTDIR%\bin
   - Company logo image files to the $RTDIR/bin (%RTDIR%\bin on Windows) directory.
   - Custom distribution scripts to the $RTDIR/DistributionScripts (%RTDIR%\DistributionScripts on Windows) directory.
   - The evr_addon_export script file to the $RTDIR/conf (%RTDIR%\conf for Windows) directory.

Completing the SmartReporter Upgrade

Do these steps to complete the SmartReporter upgrade:
1. Run:
   EVR_DB_Upgrade -mysql "<absolute path to file>/<SmartReporter database export file>.tgz"
   For example, if datadir.tgz is located in /opt/CPrt-R75/bin, run:
   EVR_DB_Upgrade -mysql "/opt/CPrt-R75/bin/datadir.tgz"
2. If you are not using the default directory paths, change these fields in the MySQL configuration file to match the locations of these directories:
   datadir=
   innodb_log_group_home_dir=
   innodb_data_file_path=
3. Run cpstart

Using the Pre-Upgrade Verification Tool

We recommend that you run the pre-upgrade verifier on the Security Management server source computer before export the management database. The pre-upgrade verifier does a compatibility analysis of the Security Management server database and its current configuration. A detailed report shows the steps to do before and after the upgrade.

The pre-upgrade verifier can only verify a database that is intended for import into a different major version of the Security Management server. It cannot be used on a database that is intended for import into the same major version of the Security Management server.

The pre_upgrade_verifier command

Run pre_upgrade_verifier without arguments to see its syntax and options.

Action Items

- **Errors** - Issues that must be resolved before you can continue with the upgrade. If you proceed without correcting these errors, the upgrade may fail, or you may have problems after upgrade.
- **Warnings** - Issues that are recommended to resolve before or after the upgrade.
### migrate

**Description**  

```
migrate <ACTION> [OPTIONS] <FILE>
```

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTION</td>
<td></td>
<td>Required parameter. Specify one of the following:</td>
</tr>
<tr>
<td></td>
<td>export</td>
<td>Exports a management database. Before exporting, close all SmartConsole clients or run <code>cpstop</code> on the Security Management server.</td>
</tr>
<tr>
<td></td>
<td>import</td>
<td>Imports a management database.</td>
</tr>
<tr>
<td>OPTIONS</td>
<td></td>
<td>Optional parameters:</td>
</tr>
<tr>
<td></td>
<td>-l</td>
<td>Export or import SmartView Tracker logs. Only closed logs are exported. Use the <code>fw logswitch</code> command to close the logs before you do the import.</td>
</tr>
</tbody>
</table>
|           | -n    | Run silently (non-interactive) using the default options for each setting.  
**Important note:** If you export a management database using the `-n` argument to a directory containing a file with the same name, it will be overwritten without prompting.  
If you run `migrate import` using this option, the `migrate` command runs `cpstop` to stop the Security Management server before importing.  
`cpstop` does not run before an export operation. |
| FILE      |       | A required parameter.  
The name of the archive file that contains the Security Management server database. The path to the archive must exist.  
Run the migrate command using the absolute path to the command or a relative path from the current directory. |
Chapter 14

Upgrading ClusterXL Deployments

In This Chapter

<table>
<thead>
<tr>
<th>Tools for Gateway Upgrades</th>
<th>99</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning a Cluster Upgrade</td>
<td>99</td>
</tr>
<tr>
<td>Minimal Effort Upgrade on a ClusterXL Cluster</td>
<td>100</td>
</tr>
<tr>
<td>Zero Downtime Upgrade on a ClusterXL Cluster</td>
<td>100</td>
</tr>
<tr>
<td>Full Connectivity Upgrade on a ClusterXL Cluster</td>
<td>102</td>
</tr>
</tbody>
</table>

Tools for Gateway Upgrades

SmartUpdate has these tools for upgrading gateways:

- **SmartUpdate Upgrade All Packages Feature**: This feature allows you to upgrade all packages installed on a gateway. For IPSO and SecurePlatform, this feature also allows you to upgrade your Operating System as a part of your upgrade.

- **SmartUpdate Add Package to Repository**: SmartUpdate provides three tools for adding packages to the Package Repository:
  - From CD/DVD: Adds a package from the Check Point DVD.
  - From File: Adds a package that you have stored locally.
  - From Download Center: Adds a package from the Check Point Download Center.

- **SmartUpdate Get Check Point Gateway Data**: This tool updates SmartUpdate with the current Check Point or OPSEC third party packages installed on a specific gateway or throughout your entire enterprise.

Planning a Cluster Upgrade

When upgrading ClusterXL, the following options are available to you:

- **Minimal Effort Upgrade**: Select this option if you have a period of time during which network downtime is allowed. The minimal effort method is much simpler because the clusters are upgraded as gateways and therefore can be upgraded as individual gateways.

- **Zero Downtime**: Select this option if network activity is required during the upgrade process. The zero downtime method assures both inbound and outbound network connectivity at all time during the upgrade. There is always at least one active member that handles traffic.

- **Full Connectivity Upgrade**: Choose this option if your gateway needs to remain active and your connections must be maintained. Full Connectivity Upgrade with Zero Down Time assures both inbound and outbound network connectivity at all time during the upgrade. There is always at least one active member that handles traffic and open connections are maintained during the upgrade.

  **Note** - Full Connectivity Upgrade is supported between minor versions only. For further information, refer to Full Connectivity Upgrade on a ClusterXL Cluster (on page 102) and the R75 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=1647).
Permanent Kernel Global Variables

When upgrading each cluster member, verify that changes to permanent kernel global variables are not lost (see: sk26202). For example, if `fwha_mac_magic` and `fwha_mac_forward_magic` were set to values other than the default values, then verify these values remain unchanged after the upgrade.

Ready State During Cluster Upgrade/Rollback Operations

When cluster members of different versions are present on the same synchronization network, cluster members of the previous version become active while cluster members of the new (upgraded) version remain in a special state called Ready. In this state, the cluster members with the new version do not process any traffic destined for the cluster IP address. This behavior is the expected behavior during the upgrade process.

To avoid such behavior during an upgrade or rollback, physically or using `ifconfig`, disconnect the cluster interfaces and the synchronization network of that cluster member before beginning.

Upgrading OPSEC Certified Third-Party Cluster Products

- When upgrading IP appliance clusters (VRRP and IP Clusters), follow either one of the available procedures (that is, zero downtime or minimal effort).
- When upgrading other third-party clustering products, it is recommended that you use the minimal effort procedure.
  Zero downtime upgrade is not supported using the regular procedure. The third party may supply an alternative upgrade procedure to achieve a zero downtime upgrade.
- For a complete understanding of the upgrade procedure, refer to the third-party vendor documentation before performing the upgrade process.

Minimal Effort Upgrade on a ClusterXL Cluster

If you choose to perform a Minimal Effort Upgrade, meaning you can afford to have a period of time during which network downtime is allowed, each cluster member is treated as an individual gateway. In other words, each cluster member can be upgraded in the same way as you would upgrade an individual gateway member. For additional instructions, refer to Upgrading a Distributed Deployment (on page 65).

Zero Downtime Upgrade on a ClusterXL Cluster

Supported Modes

Zero Downtime is supported on all modes of ClusterXL, including IPSO's IP clustering and VRRP. For additional third-party clustering solutions, consult your third-party solution's guide.

To perform a zero downtime upgrade, first upgrade all but one of the cluster members.

To upgrade all but one of the cluster members:

1. To avoid possible problems with switches around the cluster, it is recommended to switch the CCP protocol to Broadcast mode on all cluster members. Run `cphaconf set_ccp broadcast` on all cluster members.
Note - cphaconf set_ccp starts working immediately. It does not require a reboot, and it will survive the reboot. If you want to switch the CCP protocol back to Multicast mode on all cluster members after the upgrade, then run cphaconf set_ccp multicast on all cluster members.

2. Suppose that cluster member A is the active member, and members B and C are standby members. In Load Sharing mode, randomly choose one of the cluster members to upgrade last. Ensure that the previously upgraded NGX licenses are attached to members B and C.

3. Attach the previously upgraded licenses to all cluster members (A, B and C) as follows:
   - On the SmartConsole GUI machine, open SmartUpdate, and connect to the Security Management server. The updated licenses are displayed as Assigned.
   - Use the Attach assigned licenses option to Attach the Assigned licenses to the cluster members.

4. Upgrade cluster members B and C in one of the following ways:
   - Using SmartUpdate
   - In Place

When the upgrade of B and C is complete, reboot both of them.

If you are running SmartUpdate, skip to step 7. SmartUpdate compiles and installs an updated policy on the new member, once it is rebooted.

5. Installing the policy:

Be aware that policy installation on the old Check Point gateway may cut connections for services that do not survive the policy installation.

This can be avoided by configuring the Check Point Gateway > Advanced > Connection Persistence tab to either Keep all connections or Keep data connections. For complete instructions, click the help button in the Connection Persistence tab.

   Note - Do not change any cluster parameters from the current policy at this time. For example, if the cluster is running in New High Availability mode, do not change it to Load Sharing. Changes can be made after the upgrade process is complete.

6. If you are upgrading from a previous version, perform the following steps:
   a) From the Policy Installation window, clear the For Gateway Clusters, install on all the members, if it fails do not install at all option located under the Install on each selected Module independently option.
   b) Install the security policy on the cluster.

The policy will be successfully installed on cluster members B and C, and will fail on member A.

7. Using the cphaprob stat command (executed on a cluster member), verify that the status of cluster member A is Active or Active Attention. The remaining cluster members will have a Ready status. The status Active Attention is given if member A’s synchronization interface reports that its outbound status is down, because it is no longer communicating with other cluster members.

8. Execute the cphastop command on cluster member A. Machines B and/or C start to process traffic (depending on whether this is a Load Sharing or High Availability configuration).

9. It is recommended that you do not install a new policy on the cluster until the last member has been upgraded. If you must install a new policy, perform the following steps:
   a) Run cpstop on the old Check Point gateway.
   b) Run fw ctl set int fwha_conf_immediate 1 on all new Check Point gateways.
   c) Install the policy.

   Note - It is recommended that you minimize the time in which cluster members are running different versions.

To upgrade the final cluster member:

1. Upgrade cluster member A by either:
   - Using SmartUpdate
   - In Place
2. Reboot cluster member A.
3. Run `cphaconf set CCP multicast` followed by `cphastart` on all cluster members. This returns the cluster control protocol to multicast (instead of broadcast).
   This step can be skipped if you prefer to remain working with the cluster control protocol in the broadcast mode.

**Full Connectivity Upgrade on a ClusterXL Cluster**

ClusterXL clusters can be upgraded while at the same time maintaining full connectivity between the cluster members.

**Understanding a Full Connectivity Upgrade**

The Full Connectivity Upgrade (FCU) method assures that synchronization is possible from old to new cluster members without losing connectivity. A full connectivity upgrade is only supported from R75 to a future minor version that specifically supports FCU.

Connections that have been opened on the old cluster member will continue to "live" on the new cluster member.

In discussing connectivity, cluster members are divided into two categories:

- **New Members (NMs):** Cluster members that have already been upgraded. NMs are in the "non-active" state.
- **Old Members (OMs):** Cluster members that have not yet been upgraded. These cluster members are in an "active state" and carry all the traffic.

**Supported Modes**

FCU is supported on all modes of ClusterXL, including IPSO's IP clustering and VRRP. Legacy High Availability is not supported in FCU. For other third-party support, refer to the third-party documentation.

**Full Connectivity Upgrade Prerequisites**

Verify that the new member (NM) and the old member (OM) contain the same firewall policy and product installation. During the upgrade, do not change the policy from the last policy installed on the Check Point Gateway prior to its upgrade. Make sure that the upgraded version is at least NGX or higher.

**Full Connectivity Upgrade Limitations**

- This upgrade procedure is equivalent to a failover in a cluster where both members are of the same version. Therefore, whatever would not normally survive failover, will not survive a Full Connectivity Upgrade. This includes:
  - Security servers and services that are marked as non-synced
  - Local connections
  - TCP connections that are TCP streamed
  - The exact same products must be installed on the OM and on the NM.

Verify the installed products by running the command `fw ctl conn` on both cluster members.

An example output on the NM:
Full Connectivity Upgrade on a ClusterXL Cluster

Registered connections modules:

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Newconn</th>
<th>Packet</th>
<th>End</th>
<th>Reload</th>
<th>Dup</th>
</tr>
</thead>
<tbody>
<tr>
<td>0:</td>
<td>Accounting</td>
<td>00000000</td>
<td>00000000</td>
<td>d08ff920</td>
<td>00000000</td>
<td></td>
</tr>
<tr>
<td>Special</td>
<td>d08fed58</td>
<td>d0976098</td>
<td>00000000</td>
<td>00000000</td>
<td>00000000</td>
<td></td>
</tr>
<tr>
<td>1:</td>
<td>Authentication</td>
<td>d0975e7c</td>
<td>00000000</td>
<td>00000000</td>
<td>d0955370</td>
<td>00000000</td>
</tr>
<tr>
<td>Special</td>
<td>d095520</td>
<td>d0976114</td>
<td>00000000</td>
<td>00000000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:</td>
<td>NAT</td>
<td>00000000</td>
<td>00000000</td>
<td>d0955370</td>
<td>00000000</td>
<td></td>
</tr>
<tr>
<td>Special</td>
<td>d095520</td>
<td>d0976114</td>
<td>00000000</td>
<td>00000000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:</td>
<td>SeqVerifier</td>
<td>d091e670</td>
<td>00000000</td>
<td>00000000</td>
<td>d091e114</td>
<td></td>
</tr>
<tr>
<td>Special</td>
<td>d091e708</td>
<td>d091e708</td>
<td>00000000</td>
<td>00000000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6:</td>
<td>Tcpstreaming</td>
<td>d0913da8</td>
<td>00000000</td>
<td>d09732d8</td>
<td>00000000</td>
<td></td>
</tr>
<tr>
<td>None</td>
<td>VPN</td>
<td>00000000</td>
<td>00000000</td>
<td>d155a8d0</td>
<td>00000000</td>
<td></td>
</tr>
<tr>
<td>Special</td>
<td>d1553e48</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Verify that the list of Check Point Gateway names is the same for both cluster members.

- All the Gateway configuration parameters should have the same values on the NM and the OM. The same rule applies to any other local configurations you may have set.
  
  For example, having the attribute `block_new_conns` with different values on the NM and on the OM might cause the FCU to fail since gateway behavior cannot be changed during the upgrade.

- A cluster that performs static NAT using the gateway's automatic proxy ARP feature requires special considerations: `cpstop` the old Check Point Gateway right after running `cphastop`. Run `cphastop` as part of the upgrade procedure described in Zero Downtime Upgrade on a ClusterXL Cluster (on page 100). Otherwise, some of the connections that rely on proxy ARP may fail and cause other connections that rely on proxy ARP not to open until the upgrade process completes. Note that running `cpstop` on the old Check Point Gateway rules out the option to roll back to the OM while maintaining all live connections that were originally created on the OM.

Performing a Full Connectivity Upgrade

The procedure for updating a cluster with full connectivity varies according to the number of members in the cluster.

To upgrade a cluster with two members:

Follow the steps outlined in Zero Downtime Upgrade on a ClusterXL Cluster (on page 100). Before you run `cphastop` as described in the Supported Modes (on page 100) section, run the following command on the upgraded member:

```
fw fcu <other member ip on sync network>
```

(e.g. `fw fcu 172.16.0.1`).

Then continue with step 8 of Supported Modes (on page 100).

To upgrade a cluster with three or more members:

Choose one of the following two methods:

1. Upgrade the two NMs, following the steps outlined in Zero Downtime Upgrade on a ClusterXL Cluster (on page 100). Before you get to step 8 of Supported Modes (on page 102) (executing `cphastop`), run the following command on all the upgraded members: `fw fcu <other member ip on sync network>` then continue with step 8 of Supported Modes (on page 102) on the single OM.

   or

2. First upgrade only one member, following the steps outlined in Zero Downtime Upgrade on a ClusterXL Cluster (on page 100). Before you get to step 8 of Supported Modes (on page 102) (executing `cphastop`), run the following command on all the upgraded members: `fw fcu <other member ip on sync network>`. Then continue with step 8 of Supported Modes (on page 102) on all remaining OMs.

For more than three members, divide the upgrade of your members so that the active cluster members can handle the amount of traffic during the upgrade.

![Note - cphastop can also be executed from the Cluster object in the SmartConsole. Once cphastop is executed, do not run cpstart or cphastart again or reboot the machine.](image)


**Monitoring the Full Connectivity Upgrade**

*Displaying Upgrade Statistics (cphaprob fcustat)*

```
cphaprob fcustat displays statistical information regarding the upgrade process. Run this command on
the new member. Typical output looks like this:

<table>
<thead>
<tr>
<th>During FCU</th>
<th>yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of connection modules........</td>
<td>23</td>
</tr>
<tr>
<td>Connection module map (remote --&gt;local)</td>
<td></td>
</tr>
<tr>
<td>0 --&gt; 0 (Accounting)</td>
<td></td>
</tr>
<tr>
<td>1 --&gt; 1 (Authentication)</td>
<td></td>
</tr>
<tr>
<td>2 --&gt; 3 (NAT)</td>
<td></td>
</tr>
<tr>
<td>3 --&gt; 4 (SeqVerifier)</td>
<td></td>
</tr>
<tr>
<td>4 --&gt; 5 (SynDefender)</td>
<td></td>
</tr>
<tr>
<td>5 --&gt; 6 (Tcpstreaming)</td>
<td></td>
</tr>
<tr>
<td>6 --&gt; 7 (VPN)</td>
<td></td>
</tr>
<tr>
<td>Table id map (remote-&gt;local)........</td>
<td></td>
</tr>
<tr>
<td>78 --&gt; 0x98EFFD0 (sip_state)</td>
<td></td>
</tr>
<tr>
<td>8158 --&gt; 0x9872070 (connections)</td>
<td></td>
</tr>
</tbody>
</table>

Global handlers  ................. none

```

The command output includes the following parameters:

**During FCU:** This should be "yes" only after running the `fw fcu` command and before running `cphastop`
on the final OM. In all other cases it should be "no".

**Number of connection modules:** Safe to ignore.

**Connection module map:** The output reveals a translation map from the OM to the NM. For additional
information, refer to Full Connectivity Upgrade Limitations (see "Supported Modes" on page 102).

**Table id map:** This shows the mapping between the gateway's kernel table indices on the OM and on the
NM. Having a translation is not mandatory.

**Table handlers:** This should include a `sip_state` and connection table handlers. In a security gateway
configuration, a VPN handler should also be included.

**Global handlers:** Reserved for future use.

*Display the Connections Table (fw tab -t connections -u [-s])*  

This command displays the "connection" table. If everything was synchronized correctly the number of
entries in this table and the content itself should be approximately the same in the old and new cluster
members. This is an approximation because during time that you run the command on the old and new
members, new connections may have been created or old connections were deleted.

**Note** - Not all connections are synchronized. For example, local
connections and services that are marked as non-synchronized.

**Options**

- `-t` - table
- `-u` - unlimited entries
- `-s` - (optional) summary of the number of connections

For further information on the `fw tab -t connections` command, refer to the "Command Line Interface"
Book.
Making Adjustments After Checking the Connection Table

It is safe to run the `fw fcu` command more than once. Be sure to run both `cpstop` and `cpstart` on the NM before re-running the `fw fcu` command. The reason for running `cpstop` and `cpstart` is that the table handlers that deal with the upgrade are only created during policy installation (`cpstart` installs policy).
Chapter 15

Upgrading SmartEvent and SmartReporter

In This Chapter

Overview of Upgrading SmartEvent and SmartReporter 106
Upgrading SmartReporter 106
Upgrading SmartEvent 108

Overview of Upgrading SmartEvent and SmartReporter

You can upgrade these product versions to R75 if the original product version is:

- SmartReporter of version R56 (known as Eventia Reporter) or higher
- SmartEvent of version 1.0 (known as Eventia Analyzer) or higher.

Upgrading SmartReporter

During the upgrade procedure, the MySQL4 database is upgraded to MySQL5. Due to a more efficient way of handling the data, this upgrade results in a smaller sized database, as shown on the management view > database maintenance > Database capacity details.

For Standalone Deployments

A Standalone Deployment upgrade is a previous SmartReporter version that is installed on a Security Management Server.

To upgrade SmartReporter in a Standalone Deployment:

Windows Platform

1. Login as an administrator and double-click on the setup file.
2. Agree to the License Agreement and click Forward.
3. Select Upgrade and click Forward.
4. Do the instructions on the screen. The instructions are different according to your platform and deployment type.
5. Indicate whether to add new products by selecting the Add new products option and click Forward. A list of the products that will be upgraded appears. Click Forward. Depending on the components that you have chosen to install, you may need to take additional steps (such as installing other components and/or license management).
6. Verify the default directory, or browse to new location in which SmartReporter will be installed.
7. Verify the default directory, or browse to new location in which the output files created by the SmartReporter output will be generated.
Click **Next** and reboot the computer to complete the installation.

8. Launch SmartDashboard.

9. Install the Security Policy, (**Policy > Install**) or install the database (**Policy > Install Database**) to make SmartReporter fully functional.

### Solaris and Linux Platform

1. Mount the DVD on the relevant subdirectory.
2. In the mounted directory, run the script: `UnixInstallScript`
3. Read the End-User License Agreement (EULA) and if you accept click **Yes**.
4. Select **Upgrade** and click **Forward**.
5. Do the instructions on the screen. The instructions are different according to your platform and deployment type.
6. Indicate whether to add new products by selecting the **Add new products** option and click **Forward**. A list of the products that will be upgraded appears. Click **Forward**. Depending on the components that you have chosen to install, you may need to take additional steps (such as installing other components and/or license management).
7. Verify the default directory, or browse to new location in which SmartReporter will be installed.
8. Verify the default directory, or browse to new location in which the output files created by the SmartReporter output will be generated.
   Click **Next** and reboot the computer to complete the installation.

9. Launch SmartDashboard.

10. Install the Security Policy, (**Policy > Install**) or install the database (**Policy > Install Database**) to make SmartReporter fully functional.

### SecurePlatform

1. After you install SecurePlatform from the DVD, select the SmartReporter product from `cpconfig` or from the SecurePlatform Web GUI.
2. Select **Upgrade** and click **Forward**.
3. Do the instructions on the screen. The instructions are different according to your platform and deployment type.
4. Indicate whether to add new products by selecting the **Add new products** option and click **Forward**. A list of the products that will be upgraded appears. Click **Forward**. Depending on the components that you have chosen to install, you may need to take additional steps (such as installing other components and/or license management).
5. Verify the default directory, or browse to new location in which SmartReporter will be installed.
6. Verify the default directory, or browse to new location in which the output files created by the SmartReporter output will be generated.
   Click **Next** and reboot the computer to complete the installation.

7. Launch SmartDashboard.

8. Install the Security Policy, (**Policy > Install**) or install the database (**Policy > Install Database**) to make SmartReporter fully functional.

### For Distributed Deployments

A Distributed Deployment upgrade refers to a previous SmartReporter version installed on a dedicated computer and a SmartReporter Add-on installed on a Security Management server or Multi-Domain Server (for versions prior to R63).

To upgrade SmartReporter in a distributed deployment, install R75 on the old SmartReporter Server and migrate the previous add-on from the Security Management server to the SmartReporter.

### Upgrade SmartReporter to the new R75

1. Before upgrading, open the SmartReporter client.
2. Go to Management > Consolidation > Sessions and stop all consolidations sessions by selecting Stop > Terminate. Verify that all the consolidation sessions have a Stopped status before closing SmartReporter.

3. Run cpstop and wait till the mysql and log Consolidator processes stop.

4. Install R75 on the previous SmartReporter Server.

**Migrate the Add-on to the SmartReporter Server**

To migrate the add-on to the SmartReporter Server:

1. Run cpstop on both the target machine (SmartReporter) and the original machine (the Add-on machine).

2. Copy the script evr_addon_export from the directory $RTDIR/conf in the SmartReporter Server to the Multi-Domain Server.

3. Invoke evr_addon_export on the Security Management Server or Multi-Domain Server. This generates a file called evr_addon_tables.tgz in the same location as evr_addon_export.

4. Copy evr_addon_tables.tgz to the $RTDIR/bin directory on the target SmartReporter server.

5. On the SmartReporter Server run svr_install --import evr_addon_tables.tgz.

6. Run cpstart on both the target and original machine.

7. Open the SmartReporter client and start the Consolidation Sessions, if necessary.

Note - After upgrading SmartReporter, the GUI client must be defined on the SmartReporter Server. To do this run cpconfig and select GUI Clients.

Note - After upgrading SmartReporter in a Multi-Domain Security Management environment, select Domains that initiate synchronization with the Domain Management Server of the selected Domain. To do this select Tools > Domain Activation in the SmartReporter client, select the relevant Domains, and click OK.

**Advanced SmartReporter Upgrade**

**Enabling SmartEvent after Upgrading SmartReporter**

After upgrading SmartReporter from a previous version, only the SmartReporter components will be enabled. To enable the SmartEvent components (analyzer or correlation unit) as well, run:

1. cpstop

2. evconfig
   - While running evconfig, enable the SmartEvent Server or the Correlation Unit.

3. cpstart

**Upgrading SmartEvent**

The process consists of:

- Upgrading SmartEvent to R75
- Verifying that the events database has been successfully moved to its new location
- Enabling SmartReporter (optional)
Upgrading SmartEvent to R75

SmartEvent can be upgraded to R75:

- **Directly** from version NGX R63
- **Indirectly** from any version prior to NGX R63
  
  a) To upgrade from version 1.0: first upgrade to version 2.0, then upgrade to R63, and then to R65.
  
  b) To upgrade from version 2.0: first upgrade to R63 then to R65

**Prerequisites**

Before upgrading to SmartEvent R75, note the path to the current database file:

$RTDIR/events_db/events.sql, where $RTDIR is a variable that contains the path of the previous SmartEvent installation.

**Upgrading SmartEvent on SecurePlatform**

1. Insert the R75 DVD into the optical drive and run `patch add cd`.
2. Confirm the Multi-Domain Server checksum.
3. Select whether to create a backup image for automatic revert (recommended).
4. Read and accept the license agreement.
5. Select **Upgrade**.
6. Download or import a service contract file, or choose to continue without one.
7. Select a source for the R75 upgrade utilities.
8. Select **Upgrade Installed Products**.
9. Validate the products in the products list.
10. Reboot once the upgrade is complete.

**Upgrading SmartEvent on a Windows Platform**

1. Insert the R75 DVD into the optical drive.
2. Read and accept the license agreement.
3. Select an upgrade option.
4. Download or import a service contract file, or choose to continue without one.
5. If necessary, upgrade your license.
6. Select a source for the R75 upgrade utilities.
7. Perform the pre-upgrade verification check.
8. Optionally install additional Check Point products.
9. Validate the products in the products list.
10. Decide whether to copy log files now or manually copy them later.
11. Select a destination location.
12. Once the upgrade has completed, reboot.

**Upgrading SmartEvent on Solaris and Linux**

1. Insert the R75 installation DVD into the optical drive.
2. Run: `UnixInstallScript`.
3. Read and accept the license agreement.
4. Select the upgrade option.
5. Download or import a service contract file, or choose to continue without one.
6. Select a source for the R75 upgrade utilities.
7. Select to upgrade installed products.
8. Validate the products in the products list.
9. Once upgrade has completed, login again to the root account.
10. Run `cpstart` to activate the installed products.

**Enabling SmartReporter**

After upgrading SmartEvent from a previous version, only the SmartEvent components (Analyzer or Correlation Unit) will be enabled. To enable SmartReporter, run:

1. `cpstop`
2. `evconfig`
3. `Enable SmartReporter`
4. `cpstart`
Chapter 16

Upgrading Multi-Domain Security Management

This section covers upgrading Multi-Domain Security Management to R75

In This Chapter

- Multi-Domain Security Management Upgrade Overview: 111
- Upgrade Multi-Domain Security Management Tools: 111
- Upgrade Best Practices: 118
- Upgrading a High Availability Deployment: 123
- Restarting Domain Management Servers: 125
- Restoring Your Original Environment: 126
- Changing the Multi-Domain Server IP Address and External Interface: 126
- IPS with Multi-Domain Security Management: 127

Multi-Domain Security Management Upgrade Overview

The direct upgrade of the Multi-Domain Server to R75 is supported from the following versions:

<table>
<thead>
<tr>
<th>Release</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGX</td>
<td>R65</td>
</tr>
<tr>
<td></td>
<td>R70.x</td>
</tr>
<tr>
<td></td>
<td>R71.x</td>
</tr>
</tbody>
</table>

The latest supported platform data is always available in the R75 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=11647).

Upgrade Multi-Domain Security Management Tools

This section describes the different upgrade and migrate utilities, and explains when and how each of them is used.

Pre-Upgrade Verifiers and Correction Utilities

Before performing the upgrade the Multi-Domain Security Management upgrade script, mds_setup, runs a list of pre-upgrade utilities. The utilities search for well-known upgrade problems that might be present in your existing installation. The output of the utilities is also saved to a log file. Three types of messages are generated by the pre-upgrade utilities:
• **Action items before the upgrade:** These include errors and warnings. Errors have to be repaired before the upgrade. Warnings are left for the user to check and conclude whether they should be fixed or not. In some cases, it is suggested that fixing utilities should be run during the pre-upgrade check, but in most cases the fixes are done manually from SmartDashboard. An example of an error to be fixed before the upgrade is when an invalid policy name is found in your existing installation. In this case, you must rename the policy.

• **Action items after the upgrade:** These include errors and warnings, which are to be handled after the upgrade.

• **Information messages:** This section includes items to be noted. For example, when a specific object type that is no longer supported is found in your database and is converted during the upgrade process, a message indicates that this change is going to occur.

### Installation Script

The `mds_setup` installation script installs Multi-Domain Security Management on non-SecurePlatform platforms.

Note - When installing Multi-Domain Server on SecurePlatform, the installation is done with using the SecurePlatform installer on the DVD. Do not run the `mds_setup` script directly. See Upgrade Best Practices (on page 118).

#### To run `mds_setup`:

1. Mount the DVD to the specified subdirectory.
2. Change the directory to the mounted directory.
3. Browse to the Solaris or the Linux directory.
4. Run the installation script: `./mds_setup`.

When `mds_setup` is executed, it first checks for an existing installation of Multi-Domain Server:

• If no such installation exists, `mds_setup` asks you to confirm a fresh installation of Multi-Domain Server.

• If a previous version of Multi-Domain Server is detected, you are prompted to select an option:
  ▪ Pre-Upgrade Verification Only
  ▪ Upgrade
  ▪ Export
  ▪ Backup

5. After the installation completes successfully, exit all shell sessions and then open a new shell to set the new environment.

### Pre-Upgrade Verification Only

Pre-Upgrade Verification Only enables you to run pre-upgrade verification without upgrading your existing installation. No fixing utilities are executed. Use this option at least once before you upgrade. It provides you with a full report on upgrade issues, some of which should be handled before the upgrade.

You must run the pre-upgrade verification on all Multi-Domain Server computers. If the verification detects problems, you need to perform the required corrections and then synchronize all Multi-Domain Servers.

### Upgrade

When the upgrade option is used, `mds_setup` runs the Pre-Upgrade Verifier and if no errors are found, the upgrade process proceeds. In case of errors, `mds_setup` stops the installation until all the errors are fixed. In some cases, `mds_setup` suggests automatically fixing the problem using a fixing utility. Fixing utilities that affect the existing installation can also be run from the command line. You can choose to stop the installation and run the fixing utility from the command line. There are two important things to remember after changing your existing installation:

1. Verify your changes in the existing installation before you upgrade.
2. Synchronize global policies as follows:
Upgrade Multi-Domain Security Management Tools

a) In the Global SmartDashboard, select **Management High Availability** from the **Policy** menu.
b) Click **Synchronize**.
c) If you make any changes to global policies, reassign the global policies to affected Domains.
d) Synchronize databases between Domain Management Servers in High Availability mode.
e) Install the database on Log Servers.

**Backup**

Before doing an upgrade, back up your Multi-Domain Server. The backup option from `mds_setup` runs the `mds_backup` process (refer to `mds_backup`). Backup is also used for replication of your Multi-Domain Server to another machine. Manual operations are necessary if you are switching IP addresses or network interface names (see “Changing the Multi-Domain Server IP Address and External Interface” on page 126).

**Container2MultiDomain**

In versions prior to Multi-Domain Security Management R75, you had the option of dividing functionality between two physical Multi-Domain Server platforms:

- Multi-Domain Server Containers hosted the Domain Management Server (formerly CMA) databases.
- Multi-Domain Server Managers hosted the system and Global Object databases.

The current version no longer uses this architecture. All Multi-Domain Servers host all management databases.

Versions R75 and later use a different licensing model. All converted Multi-Domain Servers must have the appropriate new licenses.

Check Point developed the **Container2MultiDomain** utility to help administrators convert their old Multi-Domain Server Containers to the new single platform architecture.

- You can still use your old Multi-Domain Server Containers in a R75 deployment without conversion. Appropriate licenses are required.
- You must attach the appropriate R75 licenses to the upgraded Multi-Domain Server Container before using the **Container2MultiDomain** utility.
- **Container2MultiDomain** is applicable only to versions R75 and later.
- You can only use **Container2MultiDomain** if all of these conditions are true:
  - The Multi-Domain Server must have a license that includes the CPSB-GLBP or CPSB-BASE blades.
  - The Multi-Domain Server must be a Container.
  - The Multi-Domain Server must be running.
- You must restart all Multi-Domain Servers in your deployment after using **Container2MultiDomain**. You do not need to restart your Domain Management Servers.

**Running Container2MultiDomain**

After upgrading an old Multi-Domain Server Container, this message shows to remind you that you can use `Container2MultiDomain` to do the conversion.

The installation has indicated that this server is a Container MDS. When converting this server to a Multi-Domain Server, after logging in again to the shell, please add the required Software Blade.

Run the `Container2MultiDomain` utility and follow the instructions.

Converting a Multi-Domain Server is optional.

**To use the utility:**

1. Run `Container2MultiDomain` from the Multi-Domain Server command line.
2. When this message opens, enter yes.
This utility will convert a Container MDS to a Multi-Domain Server. Please make sure the server is up before continuing.

Would you like to continue [yes/no] ? yes

3. This message opens when the process completes.

This server will be converted from a Container MDS to a Multi-Domain Server.
Registry has been updated.
mdss::sight Updated Successfully
Multi-Domain Server database has been updated.
Please restart ALL the Multi-Domain Servers in your environment for changes to take effect.

Export

The `mds setup Export` option extracts the database and configuration settings from a Multi-Domain Server and its associated Domain Management Servers. It then stores this data in a single tgz file. You can import this tgz file to a newly installed Multi-Domain Server.

In a High Availability deployment, you must export the primary Multi-Domain Server. If the target Multi-Domain Server uses a different leading IP address than the source server, you must change the Multi-Domain Server IP address and the external interface (see "Changing the Multi-Domain Server IP Address and External Interface" on page 126).

You can include the log files in the exported tgz file. These log files are likely to be very large.

migrate export

The `migrate export` command exports the content of a single Domain Management Server or Security Management Server database into a tgz archive file. This archive file serves as the source for the migration tools described below. The `migrate` utility is included on the Multi-Domain Security Management distribution DVD.

To install the `migrate` utility:

1. Locate the `pl_upgrade_tools.tgz` archive file in the `upgrade_tools` subdirectory under the relevant operating system parent directory.
2. Extract the contents of the archive into a folder on the source computer (the computer hosting the Domain Management Server or Security Management Server).

Installation example:

```
# gtar xvfz /mnt/cdrom/upgrade_tools/solaris2/pl_upgrade_tools.tgz /var/opt/export_tools
```

*Note* - Before migrating, all objects representing the secondary management should be deleted from the primary Security Management server.

The database to import is the database belonging to the primary Domain Management Server/Security Management server. Before importing, verify that the database has been synchronized.

Also perform these steps if you want to migrate your current High Availability environment to a Domain Management Server High Availability on a different Multi-Domain Server. Then, continue with a High Availability deployment (see the High Availability chapter in the R75 Multi-Domain Security Management Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11683)).

**Usage**

To export the management database, run:

```
<fully qualified path to command>migrate export [-l] <output file>
```
The optional `-l` flag includes closed log files from the source Domain Management Server in the output archive.

- The `migrate` command works on the current Domain Management Server. You must use the `mdsenv <Domain Management Server name>` command to set environment to the current Domain Management Server (or to the Multi-Domain Server environment for the global policy) before you run the `migrate` command.
- The output file must be specified with the fully qualified path. Make sure there is sufficient disk space for the output file.
- Do a "log switch" immediately before you export the Domain Management Server to export the log files.

**Example**

```
# cd /var/opt/export_tools
# mdsenv dms1
# migrate export -l /var/opt/dms1_exported.tgz
```

**cma_migrate**

The `cma_migrate` command imports an existing Domain Management Server management database into a Multi-Domain Server. If the imported Domain Management Server is from a version earlier than that of the Multi-Domain Server, the upgrade process occurs automatically during the import.

You must run `cma_migrate` to import Domain Management Servers exported using the `migrate export` command. Copy the exported management database archive file to target Multi-Domain Server prior to using the `cma_migrate` command. Bear in mind that the source and target platforms may be different. Supported source platform include: Solaris, Linux, Windows, SecurePlatform or IPSO.

Before running `cma_migrate`, create a new Domain and a new Domain Management Server. Do not start the Domain Management Server.

If you are migrating a Domain Management Server to a new Domain Management Server with a different IP address, see (see "Migrating to a Computer with a Different IP Address" on page 95).

**Usage**

```
cma_migrate <source management tgz archive> <target Domain Management Server FWDIR directory>
```

**Example**

```
cma_migrate /tmp/exported_smc.tgz /opt/CPmds-r71/domains/dms2/CPsuite-R71/fw1
```

The first argument `<source management tgz archive>` specifies the path, on the Multi-Domain Server, to the source management data as obtained by the migrate utility. The second argument `<target Domain Management Server FWDIR directory>` is the FWDIR of the newly created Domain Management Server.

**Note** - To run the `cma_migrate` utility from the SmartDomain Manager, right-click a Domain Management Server and select Import Domain Management Server from the options menu. You can also run `mdscmd migratecma` to import files to a Domain Management Server.
Additional Information

When running `cma_migrate`, pre-upgrade verification takes place. If no errors are found, then the migration continues. If errors are found, certain modifications must be implemented on the original Security Management server, after which you must re-export the source.

Certificate Authority Information

The original Certificate Authority and `putkey` information is maintained when using `cma_migrate`. This means that the Security Management server that was migrated using `cma_migrate` should not re-generate certificates to gateways and SIC should continue to work with gateways. However, if the IP of the Domain Management Server is different than that of the original management, then `putkey` should be repeated between the Domain Management Server and entities that connect to it using `putkey` information. Use `putkey -n` to re-establish trust. For additional information on `putkey`, refer to the Check Point Command Line Interface documentation.

If your intent is to split a Domain Management Server into two or more Domain Management Servers, reinitialize their Internal Certificate Authority so that only one of the new Domain Management Servers employs the original ICA:

**To reinitialize a Domain Management Server Internal Certificate Authority:**

1. Run: `mdsstop_customer <Domain Management Server NAME>`
2. Run: `mdsenv <Domain Management Server NAME>`
3. Remove the current Internal Certificate Authority by executing the `fwm sic reset` command. This may require some preparation that is described in detail from the command prompt and also in the Secure Knowledge solution sk17197.
4. Create a new Internal Certificate Authority by executing: `mdsconfig -ca <Domain Management Server NAME> <Domain Management Server IP>`
5. Run the command: `mdsstart_customer <Domain Management Server NAME>`

For further information, refer to SK17197 ([http://supportcontent.checkpoint.com/solutions?id=sk17197](http://supportcontent.checkpoint.com/solutions?id=sk17197)).

Resolving Issues with IKE Certificates

When migrating a management database that contains a gateway object that takes part in a VPN tunnel with an externally managed third-party gateway, an issue with the IKE certificates arises. After migration, when such a gateway presents its IKE certificate to its peer, the peer gateway uses the FQDN of the certificate to retrieve the host name and IP address of the Certificate Authority that issued the certificate. If the IKE certificate was issued by a Check Point Internal CA, the FQDN will contain the host name of the original management. In this case, the peer gateway will try to contact the original management for the CRL information, and failing to do so will not accept the certificate.

There are two ways to resolve this issue:

- Update the DNS server on the peer side to resolve the host name of the original management to the IP address of the relevant Domain Management Server.
- Revoke the IKE certificate for the gateway(s) and create a new one. The new certificate will contain the FQDN of the Domain Management Server.

**migrate_global_policies**

The `migrate_global_policies` command imports (and upgrades, if necessary) a global policies database from one Multi-Domain Server to another.

If the global policy database on the target Multi-Domain Server contains policies that are assigned to Domains, the `migrate_global_policies` command stops. This is to make sure that the Global Policy used by those Domains is not deleted.

Note - When executing the `migrate_global_policies` utility, the Multi-Domain Server will be stopped. The Domain Management Server can remain up and running.
**Usage**

```
mds_backup [-g -b {-d <target dir name>} -v -h]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-g</code></td>
<td>Executes without prompting to disconnect GUI clients.</td>
</tr>
<tr>
<td><code>-b</code></td>
<td>Batch mode - executes without asking anything (<code>-g</code> is implied).</td>
</tr>
<tr>
<td><code>-d</code></td>
<td>Specifies a directory store for the backup file. When not specified, the backup file is stored in the current directory. You cannot store the backup file in any location inside the product root directory tree.</td>
</tr>
</tbody>
</table>

```mds_backup <path to exported Multi-Domain Server tgz archive>
```

- `<path to exported Multi-Domain Server tgz archive>`: specifies the fully qualified path to the archive file created by the `migrate export` command.

**Note** - `migrate_global_policies` is blocked if there are global policies assigned to Domains. Do not assign any Global Policy to Domains before you run `migrate_global_policies`.

---

**Backup and Restore**

The purpose of the backup/restore utility is to back up a whole Multi-Domain Server, including all the Domain Management Servers that it maintains, and to restore it when necessary. The restoration procedure brings the Multi-Domain Server to the state it was when the backup procedure was executed. The backup saves both user data and binaries.

**Note** - Backup and restore cannot be used to move the Multi-Domain Server installation between platforms.

Restoration can be performed on the original machine or, if your intention is to upgrade by replicating your Multi-Domain Server for testing purposes, to another machine. When performing a restoration to another machine, if the machine's IP address or interface has changed, refer to Changing the Multi-Domain Server IP Address and External Interface (on page 126) for instructions on how to adjust the restored Multi-Domain Server to the new machine.

During backup, you can view data but cannot make changes. If the Multi-Domain Security Management system consists of several Multi-Domain Servers, the backup procedure takes place manually on all the Multi-Domain Servers concurrently. Likewise, when the restoration procedure takes place, it should be performed on all Multi-Domain Servers concurrently.

**mds_backup**

The `mds_backup` command backs up binaries and data from your Multi-Domain Server to the working directory. This command requires Superuser privileges.

```
mds_backup executes the gtar command on product root directories containing data and binaries, and backs up all files except those specified in mds_exclude.dat ($MDSDIR/conf) file. The collected information is stored in a single .tgz file. This .tgz file name consists of the backup date and time, which is saved in the current working directory. For example: 13Sep2002-141437.mdsbk.tgz
```

**To perform a backup:**

1. Execute `mds_backup` from any location outside the product directory tree to be backed up. This becomes the working directory.
2. Upon completion of the backup process, copy the backup .tgz file, together with the `mds_restore`, `gtar` and `gzip` command files, to your external backup location.

**Usage**

```
mds_backup [-g -b {-d <target dir name>} -v -h]
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-g</code></td>
<td>Executes without prompting to disconnect GUI clients.</td>
</tr>
<tr>
<td><code>-b</code></td>
<td>Batch mode - executes without asking anything (<code>-g</code> is implied).</td>
</tr>
<tr>
<td><code>-d</code></td>
<td>Specifies a directory store for the backup file. When not specified, the backup file is stored in the current directory. You cannot store the backup file in any location inside the product root directory tree.</td>
</tr>
</tbody>
</table>
Upgrade Best Practices

In-Place Upgrade

The in-place upgrade process takes place on the existing Multi-Domain Server machine. The Multi-Domain Server with all Domain Management Servers are upgraded during a single upgrade process.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-v</td>
<td>Verbose mode - lists all files to be backed up, but do not perform the backup operation.</td>
</tr>
<tr>
<td>-l</td>
<td>Exclude logs from the backup.</td>
</tr>
<tr>
<td>-h</td>
<td>Help - displays help text.</td>
</tr>
</tbody>
</table>

**Comments**

When using the -g or -b options, make sure that no GUI clients or SmartReporter servers are connected. Otherwise, the backup file may contain inconsistencies due to database changes made during the backup process.

It is important not to run mds_backup from any of the directories that will be backed up. For example, when backing up a Multi-Domain Server, do not run mds_backup from /opt/CPmds-R70 since it is a circular reference (backing up directory that you need to write into).

Active log files are not backed up, in order to avoid read-during-write inconsistencies. It is recommended to perform a log switch prior to the backup procedure.

**Further Info.**

The Multi-Domain Server configuration can be backed up without backing up the log files. Such a backup will usually be significantly smaller in size than a full backup with logs. To back up without log files, add the following line to the file $MDSDIR/conf/mds_exclude.dat:

```
log/*
```

**mds_restore**

**Description**

Restores a Multi-Domain Server that was previously backed up with mds_backup. For correct operation, mds_restore should be restored onto a clean Multi-Domain Server installation.

**Usage**

```
./mds_restore <backup file>
```

**Note**

- The mds_restore command must use the script that was created in the directory into which the backup file was created.

---

Upgrade Best Practices

In-Place Upgrade

The in-place upgrade process takes place on the existing Multi-Domain Server machine. The Multi-Domain Server with all Domain Management Servers are upgraded during a single upgrade process.

1. Run the Pre-upgrade verification only option from mds_setup. In a multi-Multi-Domain Server environment, perform this step on all Multi-Domain Servers (refer to Upgrading in a Multi-Multi-Domain Server Environment ("Upgrading a High Availability Deployment" on page 123) for details).
2. Make the changes required by the pre-upgrade verification, and if you have High Availability, perform the required synchronizations.
3. Test your changes as follows:
   a) Assign the global policy
   b) Install policies to Domain Management Servers
   c) Verify logging using SmartView Tracker
   d) View status using the SmartDomain Manager or SmartView Monitor
4. Back up your system either by selecting the backup options in mds_setup or by running mds_backup.

---

Note - When upgrading Multi-Domain Security Management, all SmartUpdate packages on the Multi-Domain Server (excluding SofaWare firmware packages) are deleted from the SmartUpdate Repository.
5. Perform the in-place upgrade.
   - For Solaris or Linux, use `mds_setup`. See Installation Script (on page 112).
   - For SecurePlatform, run `patch add cd`. See Upgrading to R75 on SecurePlatform (on page 119).
6. Run `Container2MultiDomain`.

### Upgrading to R75 on SecurePlatform

This section describes how to upgrade SecurePlatform with the DVD.

**To perform an upgrade on SecurePlatform:**

1. Log in to SecurePlatform (expert mode is not necessary).
2. Apply the SecurePlatform upgrade package:
   ```
   # patch add cd.
   ```
3. You are prompted to verify the MD5 checksum.
4. Answer the following question:
   - **Do you want to create a backup image for automatic revert? Yes/No**
     - If you select **Yes**, a Safe Upgrade is performed.

   Safe Upgrade automatically takes a snapshot of the entire system so that the entire system (operating system and installed products) can be restored if something goes wrong during the Upgrade process (for example, hardware incompatibility). If the Upgrade process detects a malfunction, it automatically reverts to the Safe Upgrade image.

   When the Upgrade process is complete, upon reboot you are given the option to start the SecurePlatform operating system using the upgraded version image or using the image prior to the Upgrade process.

### Exporting and Importing a Multi-Domain Server

You can upgrade to the current version by replicating a deployment from existing (source) Multi-Domain Servers to target Multi-Domain Servers. This process combines a simplified methodology for upgrading a Multi-Domain Security Management deployment with the ability to thoroughly test the deployment prior to implementation.

Use the `mds_setup` command, with the Export option, to extract database and configuration settings from a Multi-Domain Server, together with its Domain Management Servers, and then stores this data in a single tgz file. If you are working with a high availability deployment, you must export the primary Multi-Domain Server.

Use the `MDS_import` command to import the contents of a saved tgz file to a separate, newly installed Multi-Domain Server.

These commands export and import the following information:

- Global Multi-Domain Server database
- All Domain Management Servers
- GUI Clients
- Administrators and permissions
- Licenses
- Log files (optional)

### Planning the Upgrade

Prior to initiating the upgrade process, consider the following points:

- Verify that the target Multi-Domain Server meets the minimum hardware and operating system requirements and is configured identically to the source Multi-Domain Server.
- If the target Multi-Domain Server uses a different leading IP address than the source Multi-Domain Server, you must change the Multi-Domain Server IP address and the external interface (see "Changing the Multi-Domain Server IP Address and External Interface" on page 126).
You must upgrade all Multi-Domain Servers in your deployment, including high availability and load sharing members.

The target Multi-Domain Server should be on an isolated network segment so the gateways associated with the source Multi-Domain Server are not affected until the process is complete and fully tested.

The `mds_import` command supports upgrades from the following versions:
- R65
- R70.x
- R71.x

Once you begin the export process from your source Multi-Domain Server, avoid making any configuration changes on that Multi-Domain Server. Changes made subsequent to the export will not be included in the tgz file. You will need to make any such changes manually on the target after completing the upgrade.

**Exporting a Multi-Domain Server deployment**

To export a Multi-Domain Server to a tgz file:
1. Backup the source Multi-Domain Server.
2. On the source Multi-Domain Server, run the `mds_setup` command.
3. Select the Export option.
4. Follow the instructions on the screen.
5. When prompted, choose whether or not you wish to save the log files to the tgz file.

   **Note**: Exporting the log files may significantly increase the tgz file size and the time required to complete the upgrade.

**Importing a Multi-Domain Server deployment**

To import a Multi-Domain Server deployment onto a target machine:
1. Perform a clean Multi-Domain Server installation on the target machine, according to the instructions for your specific platform.
2. Copy the appropriate exported tgz file from the source Multi-Domain Server to the new target Multi-Domain Server. The tgz file conforms to the following naming convention: `exported_mds_<time & date stamp>.tgz`
3. Run the `mds_import` command on the target Multi-Domain Server. Follow the instructions on the screen.
4. Run `mdsstart` on the target Multi-Domain Server.
5. Test to confirm that the replication has been successful:
   a) Start the Multi-Domain Server.
   b) Verify that all Domain Management Servers are running and that you can connect to the Multi-Domain Server using the SmartDomain Manager and Global SmartDashboard.
   c) Connect to the Domain Management Servers using SmartDashboard.

**Replicate and Upgrade**

Choose this type of upgrade if you intend to change hardware as part of the upgrade process or if you want to test the upgrade process first. The existing Multi-Domain Server installation is copied to another machine (referred to as the target machine) by using the `mds_backup` and `mds_restore` commands.

To perform the Replicate and Upgrade process:
1. Back up your existing Multi-Domain Server. This can be done by running `mds_backup` or by running `mds_setup` and selecting the Backup option.
2. Install a fresh Multi-Domain Server on the target machine.
   To restore your existing Multi-Domain Server, first install a fresh Multi-Domain Server on the target machine that is the exact same version as your existing Multi-Domain Server.
Note - The target machine should be on an isolated network segment so that gateways connected to the original Multi-Domain Server are not affected until you switch to the target machine.

3. Restore the Multi-Domain Server on the target machine. Copy the files created by the backup process to the target machine and run `mds_restore`.

4. If your target machine and the source machine have different IP addresses, follow the steps listed in IP Address Change (on page 126) to adjust the restored Multi-Domain Server to the new IP address. If your target machine and the source machine have different interface names (e.g. `hme0` and `hme1`), follow the steps listed in Interface Change (on page 126) to adjust the restored Multi-Domain Server to the new interface name.

5. Test to confirm that the replication has been successful:
   a) Start the Multi-Domain Server.
   b) Verify that all Domain Management Servers are running and that you can connect to the Multi-Domain Server with SmartDomain Manager and Global SmartDashboard.
   c) Connect to Domain Management Servers using SmartDashboard.

6. Upgrade your Multi-Domain Server. Stop the Multi-Domain Server on the target machine and employ an In-Place Upgrade (for additional information, refer to In-Place Upgrade (on page 118)).

7. Run `Container2MultiDomain`.

8. Start the Multi-Domain Server.

### Gradual Upgrade to Another Computer

In a gradual upgrade, Domain Management Servers are transferred to another current version Multi-Domain Server one Domain Management Server at a time.

In a gradual upgrade, the following information is not retained:

- **Multi-Domain Security Management Administrators**
  
  **To do:** Redefine and reassign to Domains after the upgrade.

- **Multi-Domain Security Management SmartConsole Clients**
  
  **To do:** Redefine and reassign to Domains after the upgrade.

- **Policy assignment to Domains**
  
  **To do:** Assign policies to Domains after the upgrade.

- **Global Communities statuses.**
  
  **To do:** execute the command:

  ```
  mdsenv; fwm mds rebuild_global_communities_status all
  ```

**To perform a gradual upgrade:**

1. Install the Multi-Domain Server on the target machine.

2. On the target Multi-Domain Server, create a Domain and Domain Management Server. Do not start the Domain Management Server.

3. Use the `migrate export` command to export the Domain Management Server database into a .tgz file and transfer the file from the source machine to the destination machine. For additional information, refer to `migrate export` (on page 114). This process transfers the licenses for the Domain Management Server.

4. Use `cma_migrate` to import the Domain Management Server. For additional information, refer to `cma_migrate` (on page 115).

5. Start the Domain Management Server and run:

   ```
   mdsenv
   mdsstart
   ```

6. Use `migrate_global_policies` to import the global policies.

### Gradual Upgrade with Global VPN Communities

The gradual upgrade process for a Multi-Domain Server using Global VPN Communities is not fundamentally different from the gradual upgrade process described above, with the following exceptions:
1. Global VPN community setup involves the Global database and the Domain Management Servers that are managing gateways participating in the global communities. When gradually upgrading a GVC environment, split the upgrade into two parts:
   - one for all Domain Management Servers that do not participate in the Global VPN Community
   - one for Domain Management Servers that do participate with the Global VPN Community

2. If some of your Domain Management Servers have already been migrated and some have not and you would like to use the Global Policy, make sure that it does not contain gateways of non-existing Domains. To test for non-existing Domains, assign this Global Policy to a Domain. If the assignment operation fails and the error message lists problematic gateways, you have at least one non-existing Domain. If this occurs:
   a) Run the where used query from the Global SmartDashboard > Manage > Network Objects > Actions to identify where the problematic gateways are used in the Global Policy. Review the result set, and edit or delete list items as necessary. Make sure that no problematic gateways are in use.
   b) The gateways must be disabled from global use:
      (i) From the General View, right-click a gateway and select Disable Global Use.
      (ii) If the globally used gateway refers to a gateway of a Domain that was not migrated, you can remove the gateway from the global database by issuing a command line command. First, make sure that the Global SmartDashboard is not running, and then execute the command:
          mdsenv; remove_globally_used_gw <Global name of the gateway>

3. When issuing the command: migrate_global_policies where the existing Global Policy contains Global Communities, the resulting Global Policy contains:
   - Global gateways from the existing database
   - Global gateways from the migrated database
   As a result of the migration, the Global Communities are overridden by the migrated database.

4. The gradual upgrade does not restore the Global Communities statuses, therefore, if either the existing or the migrated Global Policy contains Global Communities, reset the statuses from the command line with the Multi-Domain Server started.
   mdsenv; fwm mds rebuild_global_communities_status all

---

**Migrating from Security Management to Domain Management Server**

This section describes how to migrate the management part of a standalone gateway to a Domain Management Server, and then manage the standalone gateway (as a gateway only) from the Domain Management Server.

**Note** - If you want the option to later undo the separation process, back up the standalone gateway before migrating.

Before migrating the management part of the standalone gateway to the target Domain Management Server, some adjustments are required:

1. Make sure that the target Domain Management Server IP address can communicate with all gateways.
2. Add an object representing the Domain Management Server (name and IP address) and define it as a Secondary Security Management server.
3. Install policy on all managed gateways.
4. Delete all objects or access rules created in steps 1 and 2.
5. If the standalone gateway already has Check Point Security Gateway installed:
   - Clear the Firewall option in the Check Point Products section of the gateway object. You may have to first remove it from the Install On column of your Rule Base (and then add it again).
   - If the standalone gateway participates in a VPN community, in the IPSec VPN tab, remove it from the community and erase its certificate. Note these changes in order to undo them after the migration.
6. Save and close SmartDashboard. Do not install policy.
7. To migrate the management database to the Domain Management Server, run:

```
<fully qualified path to the command location> migrate export [-l] <output file>
```

See migrate export (on page 114) for details.

8. Create a new Domain Management Server on the Multi-Domain Server, but do not start it.

9. Migrate the exported database into the Domain Management Server. Use the `cma_migrate` command or the import operation from the SmartDomain Manager, specifying as an argument the database location you specified in step 7.

![Warning icon] Important - Do not use the `migrate_assist` command (or any other method not described in this step) to migrate a management database. The `migrate_assist` command is obsolete.

10. To configure the Domain Management Server after migration, start it and launch SmartDashboard.

11. In SmartDashboard, under **Network Objects**, locate:
   - An object with the Name and IP address of the Domain Management Server primary management object (migrated). Previous references to the standalone management object now refer to this object.
   - An object for each gateway managed previously by Security Management.

12. Edit the Primary Management Object and remove all interfaces (**Network Object > Topology > Remove**).

13. Create an object representing the gateway on the standalone machine (from **New > Check Point > Gateway**), and:
   - Assign a Name and IP address for the gateway.
   - Select the appropriate Check Point version.
   - Select the appropriate Check Point Products you have installed.
   - If the object previously belonged to a VPN Community, add it back.
   - Do not initialize communication.

14. Run Domain Management Server on the primary management object and, in each location, consider changing to the new gateway object.

15. Install the policy on all gateways, except for the standalone gateway. You may see warning messages about this gateway because it is not yet configured. These messages can be safely ignored.

16. Uninstall the standalone gateway.

17. Install a gateway only on the previous standalone machine.

18. From the Domain Management Server SmartDashboard, edit the gateway object and establish trust with that gateway.

19. On the same object, define the gateway’s topology.

20. Install the policy on the gateway.

## Upgrading a High Availability Deployment

High Availability deployments give redundancy at the Multi-Domain Server and/or the Domain Management Server level. In general, High Availability helps to reduce down-time during an upgrade.

This section includes instructions for doing an upgrade in a High Availability deployment. Specifically, it explains the order of upgrade and synchronization issues.

### Pre-Upgrade Verification and Tools

Run the pre-upgrade verification on all Multi-Domain Servers before upgrading any Multi-Domain Servers. Select the **Pre-Upgrade Verification Only** option from `mds_setup` (for additional information, refer to Pre-Upgrade Verifiers and Fixing Utilities (see "Pre-Upgrade Verifiers and Correction Utilities" on page 111)). Upgrade the primary Multi-Domain Server only after you have fixed all errors and reviewed all warnings for all Multi-Domain Servers.
Upgrading a High Availability Deployment

Overview

Multi-Domain Security Management High Availability gives uninterrupted management redundancy for all Domains. Multi-Domain Security Management High Availability operates at these levels:

- **Multi-Domain Server High Availability** - Multiple Multi-Domain Servers are, by default, automatically synchronized with each other. You can connect to any Multi-Domain Server to do Domain management tasks. One Multi-Domain Server is designated as the **Active** Multi-Domain Server. Other Multi-Domain Servers are designated as **Standby** Multi-Domain Servers.

  You can only do Global policy and global object management tasks using the active Multi-Domain Server. In the event that the active Multi-Domain Server is unavailable, you must change one of the standby Multi-Domain Servers to active.

- **Domain Management Server High Availability** - Multiple Domain Management Servers give Active/Standby redundancy for Domain management. One Domain Management Server for each Domain is **Active**. The other, fully synchronized Domain Management Servers for that Domain, are standbys. In the event that the Active Domain Management Server becomes unavailable, you must change one of the standby Domain Management Servers to active.

You can also use ClusterXL to give High Availability redundancy to your Domain Security Gateways. You use SmartDashboard to configure and manage Security Gateway High Availability for Domain Management Servers.

  **Note** - The current version supports multiple Domain Management Servers for each Domain.

Multi-Domain Server High Availability

Multi-Domain Servers can only communicate and synchronize with other Multi-Domain Servers running the same version. If your deployment has more than one Multi-Domain Server, do these steps:

1. Upgrade the primary Multi-Domain Server.
2. Upgrade the other Multi-Domain Servers.

During the upgrade process, we recommend that you do not use any of the Multi-Domain Servers to make changes to the databases. This can cause inconsistent synchronization between Multi-Domain Servers.

  **Note** - You must upgrade your Multi-Domain Log Servers to the same version as the Multi-Domain Servers.

Updating Multi-Domain Servers and Domain Management Servers

1. Do pre-upgrade verification for all Multi-Domain Servers.
2. If a change to the global database is necessary, synchronize all other Multi-Domain Servers immediately after making these changes. You need only do this step on one Multi-Domain Server. The synchronization process will automatically make these changes for all other Multi-Domain Servers.
3. If these global database changes affect a global policy that has been assigned to any Domain, you must re-assign the global policy to all affected Domains.
4. If the verification process finds any Domain Management Server level errors (for example, gateways that are no longer supported by the new version), do these steps:
   a) Make the required changes on the Active Domain Management Server.
   b) Synchronize the Active Domain Management Server with all Standby Domain Management Servers.
   c) If your Domain contains Log Servers, do these steps.
      i) In the Domain SmartDashboard, select **Policy > Install Database** to manually install the new database.
      ii) Select all Log Servers.
Make sure that the change to the Domain Log Server is successful.

**Note** - When synchronizing, make sure that you have only one active Multi-Domain Server and one active Domain Management Server for each Domain.

Make the necessary changes to the active Multi-Domain Server and Domain Management Server and then synchronize them to the standby.

---

**Updating Objects in the Domain Management Server Databases**

After updating the Multi-Domain Servers and Domain Management Servers, you must update the objects in all Domain Management Server databases. This is necessary because the upgrade process does not automatically update the object versions attribute in the databases. In this case, when using SmartDashboard to connect to a Domain Management Server after the upgrade, the standby Domain Management Servers and Log Servers continue to show the previous version.

To update all Domain Management Server and Domain Log Server objects, do these steps on all Multi-Domain Servers:

1. Run `mdsstat` to make sure that all Domain Management Servers are running. If any Domain Management Servers are down, resolve the issue and run `mds_startcustomerver` to start the Domain Management Server.
2. Run `mdserv` to go to the top level context.
3. Run:
   ```bash
   $MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL
   ```
   Alternatively, you can update one Domain Management Server or Domain Log Server at a time by using this command:
   ```bash
   T$MDSDIR/scripts/Multi-Domain Server_fix_cmas_clms_version -c ALL -n <Multi-Domain Log Server/Multi-Domain Server name>
   ```
4. Synchronize all standby Domain Management Servers.

---

**Managing Domain Management Servers During the Upgrade Process**

The best practice is to avoid making any changes to Domain Management Server databases during the upgrade process. If your business model cannot support management down-time during the upgrade, you can continue to manage Domain Management Servers during the upgrade process.

However, this creates a risk of inconsistent Domain Management Server database content between instances on different Multi-Domain Servers. The synchronization process cannot resolve these inconsistencies.

After successfully upgrading one Multi-Domain Server, you can set its Domain Management Servers to Active while you upgrade the others. Synchronization between the Domain Management Servers occurs after all Multi-Domain Servers are upgraded.

If, during the upgrade process, you make changes to the Domain Management Server database using different Multi-Domain Servers, the contents of the two (or more) databases will be different. Because you cannot synchronize these database, some of these changes will be lost. The Domain Management Server High Availability status appears as Collision.

You must decide which database version to retain and synchronize it to the other Domain Management Servers. You then must re-enter the lost changes to the synchronized database.

---

**Restarting Domain Management Servers**

After completing the upgrade process, start Domain Management Servers with this command:
Restoring Your Original Environment

Before the Upgrade

Pre-upgrade utilities are an integral part of the upgrade process. In some cases, you are required to change your database before the actual upgrade can take place or the Pre-Upgrade Verifier suggests you execute utilities that perform the required changes automatically. Even if you decide to restore your original environment, keep the changes you made as a result of the pre-upgrade verification.

Prepare a backup of your current configuration using the mds_backup utility from the currently installed version. Prepare a backup as the first step of the upgrade process and prepare a second backup right after the Pre-Upgrade Verifier successfully completes with no further suggestions.

Restoring Your Original Environment

To restore your original environment:

1. Remove the new installation:
   a) If the installation finished successfully, execute the mds_remove utility from the new version. This restores your original environment just before the upgrade, after the pre-upgrade verification stage.
   b) If the installation stopped or failed before its completion, manually remove the new software packages. It may be easier for you to remove all Check Point installed packages and perform a fresh installation of the original version.

2. Do a clean install on the Multi-Domain Server, with the instructions appropriate for your platform.

3. Run mds_restore using the backup files.

Changing the Multi-Domain Server IP Address and External Interface

IP Address Change

If your target machine and the source machine have different IP addresses, follow the steps listed below it to change the restored Multi-Domain Server to the new IP address.

To change the IP address:

1. Stop the Multi-Domain Server by running mdsstop.
2. Change the IP address in $MDSDIR/conf/LeadingIP file to the new IP address.
3. Edit the $MDSDIR/conf/mdsdb/mdss.C file. Find the Multi-Domain Server object that has the source Multi-Domain Server IP address and change its IP address to the new IP address. Do not change the Multi-Domain Server name.
4. Install a new license on the target Multi-Domain Server with the new Multi-Domain Server IP address.
5. For multiple Multi-Domain Server environments, repeat steps 1 to 4 for each Multi-Domain Server that has a changed IP address.

Interface Change

If your target machine and the source machine have different interface names (e.g., hme0 and hme1), follow the steps listed below to adjust the restored Multi-Domain Server to the new interface name.
To change the interface:
1. Change the interface name in file $MDSDIR/conf/external.if to the new interface name.
2. For each Domain Management Server, replace the interface name in $FWDIR/conf/vip_index.conf.

IPS with Multi-Domain Security Management

- When upgrading to R75, the previous Domain IPS configuration is overridden when you first assign a Global Policy.
  We recommend that you save each Domain policy, so that you can restore the settings after the upgrade. To do so, go to the Domain Configuration window > Assign Global Policy tab, and enable Create database version.
- Customers upgrading to the current version should note that the IPS subscription has changed.
- All Domains subscribed to IPS are automatically assigned to an "Exclusive" subscription
- "Override" and "Merge" subscriptions are no longer supported.
Chapter 17

Upgrading SmartLSM Security (ROBO) Gateways

In This Chapter

Planning the ROBO Gateway Upgrade 128
ROBO Gateway Upgrade Package to SmartUpdate Repository 128
License Upgrade for a Security Gateway ROBO Gateway 129
Upgrading a ROBO Gateway Using SmartProvisioning 129
Using the Command Line Interface 131

Planning the ROBO Gateway Upgrade

When you upgrade your Security Management server, it is recommended to upgrade the ROBO gateways managed by SmartProvisioning so that they are compatible with the latest features and functionalities. This chapter describes how to upgrade your ROBO gateways.

The general workflow for upgrading ROBO gateways comprises the following steps:

1. For Security Gateway ROBO gateways, in SmartDashboard, define new SmartLSM Profile objects for the new version and install the respective policies on these objects. This Install Policy operation only compiles the policy, it does not send it to any gateway. The compiled policy is automatically fetched later by the relevant ROBO gateways, following their upgrade.

2. Add the upgrade package to the SmartUpdate package repository.
   For additional information, refer to ROBO Gateway Upgrade Package to SmartUpdate Repository (on page 128).

3. Upgrade your ROBO Gateways in one of the following ways:
   - Using SmartProvisioning (refer to Upgrading a ROBO Gateway Using SmartProvisioning (on page 129))
   - Using the SmartLSM Command Line Interface
     (refer to Upgrading a Security Gateway ROBO Gateway Using the SmartLSM cli (see "Upgrading a Security Gateway ROBO Gateway Using LSMcli" on page 132)).

When upgrading Security Gateway ROBO gateways, the upgrade process removes the initial Plug & Play license from your gateway. Trying to perform a remote upgrade on a gateway without a valid NGX license will succeed, but this gateway will not be able to load the correct policy after the upgrade. Make sure that all gateways have valid permanent NG and NGX licenses installed before the upgrade.

ROBO Gateway Upgrade Package to SmartUpdate Repository

Once you have launched SmartUpdate, add the packages needed for the upgrade to the SmartUpdate package repository. UTM-1 Edge Firmware packages are added the same way.

License Upgrade for a Security Gateway

ROBO Gateway

The general workflow for upgrading ROBO gateway licenses to N70 comprises the following steps:
1. Upgrade the software on the ROBO Gateway, as described in Upgrading a ROBO Gateway Using SmartProvisioning (on page 129).
2. Use SmartProvisioning to Attach the upgraded licenses to each ROBO Gateway, one ROBO at a time.

Using SmartProvisioning to Attach the Upgraded Licenses

To attach the upgraded licenses:
1. Open SmartProvisioning.
2. For each ROBO Gateway, open the Edit Security Gateway ROBO Gateway window, and select the Licenses tab. All licenses that are attached to this ROBO gateway are shown. If the license upgrade succeeded, the window will report that: There are un-attached licenses that are assigned to this ROBO.
3. Add those licenses that are assigned to this ROBO from the SmartLSM License Repository to the Licenses window. You can do this by performing one of the following two options. The first way is easier:
   - Click Add these licenses to the list.
   - Click Add, and then select those licenses that are assigned to this ROBO. The added assigned licenses are shown grayed-out because they are not yet attached.
4. Click OK to attach the Assigned Licenses to this ROBO. The Licenses window shows that the license is Attached.
5. Repeat from step 2 for each ROBO gateway.

License Upgrade on Multiple ROBO Gateways

You can use scripting to upgrade licenses on multiple ROBO gateways. For additional information, refer to Example: License Upgrade on Multiple ROBO Gateways (on page 134).

Upgrading a ROBO Gateway Using SmartProvisioning

Upgrading a Security Gateway ROBO Gateway

There are two methods for upgrading a Security Gateway, the Full Upgrade and the Specific Install.

Full Upgrade

This method automatically performs all the required checks and actions for you. When it successfully completes, the upgraded ROBO Gateway is ready for use. This is the recommended method to upgrade Security Gateway ROBO Gateways.

To perform a full upgrade:
1. From SmartProvisioning, select the line representing the Security Gateway ROBO Gateway to be upgraded.
2. Select Actions > Packages > Upgrade All Packages. This selection can also be done through the right-click menu, or the Upgrade All Packages icon in the toolbar. The upgrade process begins with a verification stage, checking which version is currently installed on the gateway and whether the required packages exist in your Package Repository. When it completes, a Verification Details window opens, showing you the verification results.
3. Select **Change to a new Profile after upgrade**, and select the appropriate new SmartLSM Profile from the list.
4. Select **Allow reboot if required**.
5. Click the **Continue** button.

The Upgrade process begins. Its stages and completion status can be seen in the **Action Status** pane, at the bottom of SmartLSM. The entire progress report can be seen at any time by viewing the **Action History** (right-click on the respective line in the **Action Status** pane, and select **Action History**).

**Specific Installation**

This method can be used to install a specific product on a ROBO Gateway.

**To perform a specific installation:**

1. From **SmartLSM**, select the line representing the Security Gateway ROBO gateway you want to upgrade.
2. Select **Actions > Packages > Get Gateway Data** to fetch information about Packages currently installed on the Security Gateway ROBO gateway.
3. Select **Actions > Packages > Distribute Package**... or right-click menu, and select **Distribute Package**..., or click the icon in the toolbar.

The **Distribute Package** window opens. This window displays the relevant packages from the Package Repository that can be installed on your Security Gateway.

4. In the **Distribute Package** window, select the package you want to install. You can then select one of the following actions:
   - Distribute and install packages
   - Only distribute packages (install later)
   - Install previously distributed packages
5. The **Allow Reboot if required** option should be selected only when upgrading VPN-1. If you do not select this option, manually reboot the gateway from its console. The gateway is rebooted after the package installation is completed.

   **Note** - If you are doing a step-by-step upgrade, do not select **Allow Reboot if required**.

6. If the operating system is SecurePlatform, you can select **Backup image for automatic revert**, in case the installation does not succeed.
7. The option **Change to a new profile after install** lets you select the SmartLSM Profile that will be assigned to the package upon installation. When upgrading the Security Gateway ROBO gateway, you must provide a suitable SmartLSM Profile from the target version. If you are installing a package that does not require changing the SmartLSM Profile of the Security Gateway ROBO gateway, this field remains disabled.
8. Click the **Start** button.
9. The Install process begins. Its stages and completion status can be seen in the **Action Status** pane, at the bottom of SmartLSM. The whole progress report can be seen at any time by viewing the **Action History** (right-click on the respective line in the **Action Status** pane, and select **Action History**).

   **Note** - You can verify if the installation will succeed before actually upgrading the ROBO Gateway by choosing **Actions > Packages > Verify Installation**.

**Upgrading a UTM-1 Edge ROBO Gateway**

**To upgrade the gateway:**

1. From **SmartLSM**, select the line representing the UTM-1 Edge ROBO gateway you want to upgrade, and choose **Edit > Edit ROBO gateway**... This selection can also be done through the right-click menu, or the Edit ROBO gateway icon in the toolbar, or by double-clicking the ROBO line.
2. Select the **Firmware** tab.
3. Select the **Use the following firmware** option, select the desired firmware from the list, and click **OK**. The UTM-1 Edge ROBO gateway fetches and installs the new firmware the next time it automatically checks for updates. In order for the firmware upgrade to take effect immediately, restart the ROBO Gateway by selecting **Actions > Restart gateway**.

### Upgrading a Security Gateway ROBO Gateway In Place

You can upgrade a ROBO gateway In Place (from the ROBO gateway's console), just like an In Place upgrade of a regular gateway. Following the upgrade, update the new version on the SmartLSM side, and select a new SmartLSM Profile for the gateway.

**To upgrade a gateway In Place:**

1. From **SmartLSM**, select the line representing the Security Gateway ROBO gateway you just upgraded, and select **Edit > Edit ROBO gateway**... or right-click the Edit ROBO gateway icon in the toolbar, or double-click the ROBO line. The **Edit** window opens in the **General** tab.
2. From the **Version** menu, select the new version of the upgraded gateway.
3. From the **Profile** menu, select a new SmartLSM Profile for the upgraded gateway.
4. Click **OK** to close the window.
5. The policy and properties of the new SmartLSM Profile are applied on the ROBO Gateway the next time it automatically checks for updates. In order for the SmartLSM Profile change to take effect immediately, restart the ROBO Gateway by selecting **Actions > Restart Gateway**.

### Using the Command Line Interface

#### SmartLSM Upgrade Tools

**LSMcli**

The **LSM Command Line Interface (LSMcli)** is an alternative to SmartLSM. **LSMcli** provides the ability to perform SmartLSM operations from a command line or through a script. It also enables you to upgrade a ROBO Gateway. When used in scripts it allows you to perform batch upgrades.

The **LSMcli** tool is contained in the management installation package on the Security Management server machine. It can be run on your Security Management server, or it can be copied to and run on another host with the same operating system. The host does not need to be a Check Point-installed machine, but it must be:

- Defined on the Security Management server as a GUI Client.
- Use the same Operating System as the Security Management server.
- Reachable through the network from the Security Management server.

For general usage and help, type the command **LSMcli --help**.

The LSMcli command line arguments are fully described in the **Command Line Reference** chapter of the **R75 Smart Provisioning Administration Guide** ([http://supportcontent.checkpoint.com/documentation_download?ID=11671](http://supportcontent.checkpoint.com/documentation_download?ID=11671)). A partial list of arguments is shown in the table below, which lists only the arguments that are important for performing upgrades.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>(Optional) Run the command with debug output.</td>
</tr>
<tr>
<td>Server</td>
<td>The IP or host name of the Security Management server.</td>
</tr>
<tr>
<td>User</td>
<td>The user name and password of a Security Management Server Administrator.</td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>ROBO</td>
<td>The name of the ROBO Gateway to be upgraded.</td>
</tr>
</tbody>
</table>
### Using the Command Line Interface

#### Upgrading SmartLSM Security (ROBO) Gateways

<table>
<thead>
<tr>
<th>Argument</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-F Firmware</td>
<td>The firmware version of the UTM-1 Edge ROBO Gateway.</td>
</tr>
<tr>
<td>-P Profile</td>
<td>(Optional) The SmartLSM Profile name the ROBO Gateway will be mapped to after a successful upgrade. &lt;br&gt; You must specify the new SmartLSM Profile when upgrading the VPN-1 version. This is not necessary when installing Hotfixes or other packages.</td>
</tr>
<tr>
<td>boot</td>
<td>(Optional) Use this option only when upgrading VPN-1. If you do not use this option, manually reboot the gateway from its console.</td>
</tr>
<tr>
<td>-DoNotDistribute</td>
<td>(Optional) Install previously distributed packages.</td>
</tr>
<tr>
<td>Product Vendor Version SP</td>
<td>To view the list of packages available in the repository, use the <code>ShowRepository LSMcli</code> command. &lt;br&gt; (Command usage is described in the R75 SmartProvisioning Administration Guide (<a href="http://supportcontent.checkpoint.com/documentation/download?ID=11671">http://supportcontent.checkpoint.com/documentation/download?ID=11671</a>)).</td>
</tr>
<tr>
<td>-KeepDOs</td>
<td>To add the dynamic objects in the LSMcli command to the existing list of dynamic objects.</td>
</tr>
</tbody>
</table>

### Export

The `export` tool is located in your SmartLSM application, under **File > Export to File**. Use this tool to export a ROBO Gateway's properties into a text file that you can turn into a script in order to perform batch upgrades.

### Upgrading a Security Gateway ROBO Gateway Using LSMcli

For descriptions of the command line arguments for the following commands, refer to the table above.
To verify that a Full Upgrade of a ROBO Gateway will succeed, execute:
LSMcli [-d] <Server> <User> <Password> VerifyUpgrade <ROBO>

To perform a Full Upgrade of a ROBO gateway, execute:
LSMcli [-d] <Server> <User> <Password> Upgrade <ROBO> [-P=Profile] [-boot]

To see which product packages are available in your package repository, execute:
LSMcli [-d] <Server> <User> <Password> ShowRepository

To verify that a Specific Install on a ROBO gateway will succeed, execute:
LSMcli [-d] <Server> <User> <Password> VerifyInstall <ROBO> <Product> <Vendor> <Version> <SP>

To perform a Specific Install on a ROBO gateway, execute:

To only distribute a package, execute:
LSMcli [-d] <Server> <User> <Password> Distribute <ROBO> <Product> <Vendor> <Version> <SP>

To view a list of packages that can be installed on a specific ROBO gateway, execute:
LSMcli [-d] <Server> <User> <Password> GetCandidates <ROBO>

To get data about a specific ROBO gateway, execute:
LSMcli [-d] <Server> <User> <Password> GetInfo <ROBO>

Note - It is recommended to use the Full Upgrade method to upgrade Security Gateway ROBO Gateways.

Example: Upgrading a Single Security Gateway ROBO Gateway
% LSMcli MyServer John mypassword VerifyUpgrade ROBO17
% LSMcli MyServer John mypassword Upgrade ROBO17 -P=MyNewProfile

Where:
MyServer = the name of my Security Management server.
John = the administrator's name.
mypassword = the administrator's password.
VerifyUpgrade = the Full Upgrade verification command.
Upgrade = the Full Upgrade command.
ROBO17 = the Security Gateway ROBO Gateway to be upgraded.
MyNewProfile = the new SmartLSM Profile that ROBO17 will be mapped to after the upgrade.

Upgrading a UTM-1 Edge ROBO Gateway Using LSMcli
For descriptions of the command line arguments for the following commands, refer to Table 15-1.
To see which product packages are available in your package repository, execute:

```
LSMcli [-d] <Server> <User> <Password> ShowRepository
```

To upgrade a UTM-1 Edge ROBO gateway, execute:

```
LSMcli [-d] <Server> <User> <Password> ModifyROBO VPN1Edge
<ROBO> [-P=Profile] [-F=Firmwarename]
```

If you want the firmware update to take effect immediately, execute:

```
LSMcli [-d] <Server> <User> <Password> Restart <ROBO>
```

**Example: Upgrading a Single UTM-1 Edge ROBO Gateway**

```
% LSMcli MyServer John mypassword ModifyROBO VPN1Edge
  ROBO101 -P=EdgeNewProfile -F=4.0.23
% LSMcli MyServer John mypassword Restart ROBO101
```

Where:

- **MyServer** = the name of your Security Management server.
- **John** = the administrator's name.
- **mypassword** = the administrator's password.
- **ModifyROBO VPN1Edge** = the command to modify a property on a UTM-1 Edge ROBO gateway.
- **ROBO101** = the Edge ROBO Gateway to be upgraded.
- **EdgeNewProfile** = the new SmartLSM Profile that ROBO101 will be mapped to after the upgrade (optional).
- **4.0.23** = the name of the new Firmware package.
- **Restart** = the command to restart the gateway.

**Using the LSMcli in Scripts**

Scripting can be very handy when you want to upgrade multiple ROBO Gateways in batches.

**Example: Using the LSM CLI to write a script to upgrade multiple ROBO Gateways**

Create the following script and run it:

```
LSMcli MyServer John mypassword Upgrade ROBO17 -P=MyNewProfile
LSMcli MyServer John mypassword Upgrade ROBO18 -P=MyNewProfile
LSMcli MyServer John mypassword Upgrade ROBO19 -P=MyOtherProfile
```

**Example: License Upgrade on Multiple ROBO Gateways**

To upgrade licenses on multiple ROBO Gateways, create a script that runs the LSMcli command with the AttachAssignedLicenses option on all ROBO Gateways. The AttachAssignedLicenses option is equivalent to attaching licenses as described in Using SmartProvisioning to Attach the Upgraded Licenses (on page 129) in SmartLSM.

Run:

```
LSMcli [-d] <Server> <User> <Password>
AttachAssignedLicenses VPN1 <ROBO>
```

For example:
<table>
<thead>
<tr>
<th>LSMcli MyServer John mypassword AttachAssignedLicenses VPN1 ROBO17</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSMcli MyServer John mypassword AttachAssignedLicenses VPN1 ROBO18</td>
</tr>
<tr>
<td>LSMcli MyServer John mypassword AttachAssignedLicenses VPN1 ROBO19</td>
</tr>
</tbody>
</table>
Index

A
Action Items • 64, 66, 85, 96
Add Packages to the Package Repository • 72
Adding and Activating an R75 Package Using Network Voyager • 74
Adding and Activating an R75 Package Using the CLI Shell • 75
Adding IPS-1 Sensors • 52
Adding Licenses using the SmartDomain Manager • 34
Additional Information • 114
Advanced Security Management Server Upgrade and Database Migration • 88
Advanced SmartReporter Upgrade • 107
Advanced Upgrade on Linux or Solaris Platforms • 92
Advanced Upgrade on SecurePlatform • 91
Advanced Upgrade on the IPSO Platform • 93
Advanced Upgrade on the Windows Platform • 93
After Migrating the Security Management Server • 95

B
Backing Up Your Current Deployment • 77
Backup • 78, 112
Backup and Restore • 116
Backup and Revert for Security Gateways • 77
Backup Parameters • 78
Basic Architecture • 26
Before Migrating Your Source Security Management Server • 94
Before the Upgrade • 125

C
Certificate Authority Information • 115
Changing the Multi-Domain Server IP Address and External Interface • 125
cma_migrate • 114
Compatibility Tables • 12
Completing the Installation • 18, 20, 24
Completing the SmartReporter Upgrade • 96
Configuring IPS-1 Sensors • 51
Configuring NTP • 53
Configuring SecurePlatform • 30
Configuring SecurePlatform using the CLI • 48
Configuring SecurePlatform using the WebUI • 47
Configuring the Multi-Domain Server • 31
Configuring the Security Management Server for SmartUpdate • 72
Container2MultiDomain • 112
Contract Verification • 56
Creating the Multi-Domain Security Management Environment • 29

D
Defining Log Servers as Global Servers • 38
Defining the Reporting or SmartEvent Server as a Local Server • 38
Demo Mode • 35
Display the Connections Table (fw tab -t connections -u [-s]) • 103
Displaying Upgrade Statistics (cphaprob fcustat) • 103
Distributed Deployment • 36, 40
DLP and Privacy • 46
DLP Requirement Notes • 47
Downloading R75 • 10

E
Enabling Policy Enforcement • 65
Enabling SmartEvent after Upgrading SmartReporter • 107
Enabling SmartReporter • 109
Example • 114
License Upgrade on Multiple ROBO Gateways • 133
Upgrading a Single Security Gateway ROBO Gateway • 132
Upgrading a Single UTM-1 Edge ROBO Gateway • 133
Using the LSM CLI to write a script to upgrade multiple ROBO Gateways • 133
Export • 113, 131
Exporting a Multi-Domain Server deployment • 119
Exporting and Importing a Multi-Domain Server • 118
Exporting the Database • 93
Exporting the Management Database • 95
Exporting the Management Database using the Command Line • 91, 92, 93
Exporting the Management Database using the Graphical Interface from the DVD • 91, 93

F
For Distributed Deployments • 106
For New Check Point Customers • 9
For Standalone Deployments • 105
Full Connectivity Upgrade Limitations • 101
Full Connectivity Upgrade on a ClusterXL Cluster • 101
Full Connectivity Upgrade Prerequisites • 101
Full Upgrade • 128

G
Gateway Upgrade on a UTM-1/Power-1 Appliance • 73
Gateway Upgrade on an IP Appliance • 74
Gateway Upgrade on SecurePlatform • 73
Gateway Upgrade Process on a Windows Platform • 76
Gateway Upgrade Process Using SmartUpdate • 72
General Workflow • 90
Getting Started • 10
Gradual Upgrade to Another Computer • 120
Gradual Upgrade with Global VPN Communities • 120