

Installation and Upgrade Guide

R75.40VS



25 February 2013

© 2013 Check Point Software Technologies Ltd.

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

RESTRICTED RIGHTS LEGEND:

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

TRADEMARKS:

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

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

Important Information

Latest Software

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

Latest Documentation

The latest version of this document is at:

http://supportcontent.checkpoint.com/documentation_download?ID=16422

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

For more about this release, see the R75.40VS home page (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

Revision History

Date	Description
24 February 2013	Clarification of Full Connectivity Upgrade Options (" Supported Upgrade Scenarios " on page 158)
19 November 2012	<ul style="list-style-type: none">Added: USB Installation (on page 10)Deleted references to non supported versions ("Upgrading Standalone" on page 76)Updated Multi-Domain Server in place upgrade ("SecurePlatform to SecurePlatform" on page 120). Remove the media before rebooting.Added: Upgrading 32/64-bit Cluster Members (on page 154).
30 August 2012	<ul style="list-style-type: none">Added Gaia disk partitions in a clean installation ("Disk Partitions in a Gaia Clean Installation" on page 17).Installing Security Management server on appliances is supported only for Smart-1. Deleted other instructions ("Installing Security Management Server on Appliances" on page 35).Updated Installing Full High Availability Appliances (on page 47).Added upgrade instructions via WebUI for Standalone, Security Management server and Security Gateway deployments on open server.Added instructions for Gaia configuration backup ("Gaia Backup" on page 66) and image management ("Gaia Snapshot Image Management" on page 67).Multi-Domain Security Management can be upgraded from Gaia to Gaia only using an ISO image. Deleted other instructions ("Gaia to Gaia" on page 119).Procedure for exporting the database On Gaia and SecurePlatform - CLI (on page 146) and On Gaia and SecurePlatform - GUI on DVD (on page 146) is the same.Updated instructions for Completing the SmartReporter Upgrade (on page 150).

Date	Description
22 July 2012	<ul style="list-style-type: none"> Added Gaia to Gaia upgrade instructions. Updated number of interfaces in bridge mode and configuring bridge mode for Gaia (on page 52). Updated upgrade command for SecurePlatform Open Servers to <code>patch add cd</code>
16 July 2012	First release of this document

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 Installation and Upgrade Guide R75.40VS).

Contents

Important Information	3
Getting Started	9
Welcome	9
R75.40VS Documentation	9
For New Check Point Customers	10
Downloading R75.40VS	10
USB Installation	10
Glossary	10
Compatibility Tables	12
Licensing	13
Software Licensing	13
Licensing Multi-Domain Security Management	13
Disk Space	14
Gaia Automatic Software Updates	14
SmartDashboard Toolbar	14
Deployment Options	15
Installing Security Management Server and Security Gateways	16
Installing Standalone	17
Disk Partitions in a Gaia Clean Installation	17
Installing Standalone on Appliances	18
Installing Standalone on Open Servers	30
Installing Security Management Server	34
Disk Partitions in a Gaia Clean Installation	34
Installing Security Management Server on Appliances	35
Installing Security Management Server on Open Servers	37
Installing Log Server	39
Installing Security Gateway	40
Installing Security Gateway on Appliances	40
Installing Security Gateway on Open Servers	42
Installing VSX Gateways	44
Converting Gateways to VSX Gateways	44
Installing Full High Availability Appliances	47
Gaia Appliances	47
SecurePlatform Appliances	49
Configuring Standalone Full High Availability	50
Deploying Bridge Mode Security Gateways	52
Gaia	52
SecurePlatform	53
Installing SmartConsole Clients	53
Demo Mode	53
Logging in to SmartConsole	54
Post-Installation Configuration	54
Where to Go From Here	54
Uninstalling R75.40VS	54
Installing Multi-Domain Security Management	56
Basic Architecture	56
Setting Up Multi-Domain Security Management Networking	57
Installing Multi-Domain Server	58
Smart-1 Appliances	58
Converting a Security Management Server to Multi-Domain Server	59
Open Servers	60
Installing Gateways	61

Installing Multi-Domain Security Management GUI Clients	61
Post-Installation Configuration	61
Demo Mode	62
Adding Licenses using the SmartDomain Manager	62
Uninstalling Multi-Domain Security Management	62
Where To From Here?	63
Upgrading Prerequisites	64
Contract Verification	64
Upgrade Tools	65
Using the Pre-Upgrade Verifier Tool	65
Upgrading Successfully	66
Uninstalling Packages	66
Backing Up	66
Gaia Backup	66
Gaia Snapshot Image Management	67
SecurePlatform Backup	69
SecurePlatform Snapshot Image Management	70
Windows and IP Appliance Export	71
Restoring a Deployment	71
SecurePlatform Revert	71
SecurePlatform Restore	72
Restoring Other Platforms	72
Service Contract Files	74
Introduction	74
Working with Contract Files	74
Installing a Contract File	74
Upgrading Security Management Server and Security Gateways	76
Upgrading Standalone	76
Upgrading Standalone Appliances	76
Upgrading Standalone Open Servers	80
Upgrading the Security Management Server	84
Upgrading Security Management Server on Appliances	85
Upgrading Security Management Server on Open Servers	87
Upgrading Security Gateways	91
Upgrading Gateways using SmartUpdate	91
Upgrading Security Gateways on Appliances	93
Upgrading Security Gateways on Open Servers	105
Upgrading a VSX Gateway	109
Upgrading Standalone Full High Availability	110
Upgrading with Minimal Downtime	110
Upgrading with a Clean Installation	111
Upgrading Clusters	111
Upgrading Multi-Domain Security Management	113
Upgrade Multi-Domain Security Management Tools	113
Pre-Upgrade Verifiers and Correction Utilities	113
Container2MultiDomain	113
Export	114
migrate export	115
cma_migrate	116
cma_migrate and Certificates	116
migrate_global_policies	117
Backup and Restore	117
Upgrade Best Practices	119
Multi-Domain Server In-Place Upgrade	119
Exporting and Importing a Multi-Domain Server	120
Replicate and Upgrade	121
Gradual Upgrade to Another Computer	122
Migrating from Security Management Server to Domain Management Server	123
Upgrading a High Availability Deployment	124

Pre-Upgrade Verification and Tools	125
Multi-Domain Server High Availability	125
Upgrading Multi-Domain Servers and Domain Management Servers	125
Updating Objects in the Domain Management Server Databases.....	126
Managing Domain Management Servers During the Upgrade Process	126
Restarting Domain Management Servers	126
Restoring Your Original Environment	126
Removing Earlier Version Multi-Domain Server Installations	127
Changing the Multi-Domain Server Interfaces	127
IPS with Multi-Domain Security Management	128
Upgrading with SmartUpdate.....	129
Introducing SmartUpdate.....	129
Understanding SmartUpdate	130
SmartUpdate - Seeing it for the First Time.....	131
Common Operations	131
Upgrading Packages	132
Prerequisites for Remote Upgrades	132
Retrieving Data from Check Point Security Gateways.....	132
Adding New Packages to the Package Repository	132
Verifying the Viability of a Distribution	133
Transferring Files to Remote Devices	133
Distributions and Upgrades.....	133
Upgrading UTM-1 Edge Firmware with SmartUpdate	134
Canceling and Uninstalling	134
Uninstalling Installations and Upgrades	135
Restarting the Check Point Security Gateway.....	135
Recovering from a Failed Upgrade	135
Deleting Packages from the Package Repository	135
Managing Licenses.....	135
Licensing Terminology	136
License Upgrade.....	137
The License Attachment Process.....	137
Detaching Licenses	139
Deleting Licenses from the License & Contract Repository	139
Viewing License Properties.....	139
Checking for Expired Licenses.....	139
Exporting a License to a File	139
Managing Multi-Domain Security Management Licenses with SmartUpdate	139
Web Security License Enforcement	140
Service Contracts	140
Generating CPInfo.....	140
The SmartUpdate Command Line	141
Advanced Upgrade and Database Migration	142
Supported Upgrade Paths, Platforms and Products.....	142
Legacy Hardware Platforms	142
Migration Workflow	143
General Workflow	144
Preparing the Source Server for New IP Address	145
Getting the Migration Tools Package	145
Using the Pre-Upgrade Verification Tool.....	145
Exporting the Database	146
Importing the Database.....	147
Migrating the Database of a Secondary Security Management Server	148
Completing Migration to a New IP Address.....	148
Migrating to a Server with a Different Platform	149
SmartReporter Database Migration.....	149
SmartEvent Events Database Migration.....	150
Migrate Command Reference.....	152
Upgrading ClusterXL Deployments	153

Planning a Cluster Upgrade.....	153
Permanent Kernel Global Variables	153
Ready State During Cluster Upgrade/Rollback Operations	153
Upgrading 32/64-bit Cluster Members	154
Upgrading OPSEC Certified Cluster Products.....	154
Minimal Effort Upgrade on a ClusterXL Cluster	154
Zero Downtime Upgrade on a ClusterXL Cluster	154
Zero Downtime Upgrade of SecurePlatform ClusterXL to Gaia ClusterXL	155
Converting a Security Gateway Cluster to VSX	155
VSX Cluster Optimal Service Upgrade	156
Upgrade Workflow	156
Upgrading the Cluster R67.10 VSX.....	157
Troubleshooting the Upgrade.....	157
Limitations	158
Full Connectivity Upgrade on a ClusterXL Cluster	158
Understanding a Full Connectivity Upgrade	158
Supported Upgrade Scenarios.....	158
Full Connectivity Upgrade Prerequisites	159
Full Connectivity Upgrade Limitations	159
Performing a Full Connectivity Upgrade.....	159
Displaying Upgrade Statistics (cphaprob fcustat)	160
Display the Connections Table	160
Index.....	163

Chapter 1

Getting Started

In This Chapter

Welcome	9
R75.40VS Documentation	9
For New Check Point Customers	10
Downloading R75.40VS	10
USB Installation	10
Glossary	10
Compatibility Tables	12
Licensing	13
Disk Space	14
Gaia Automatic Software Updates	14
SmartDashboard Toolbar	14

Before you install or upgrade to R75.40VS, read the *R75.40VS Release Notes* (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

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.

R75.40VS 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 is new in R75.40VS, see the *R75.40VS Release Notes* (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

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

Downloading R75.40VS

You can download the R75.40VS software images from the *R75.40VS home page* (<http://supportcontent.checkpoint.com/solutions?id=sk76540>). There are different software images for each operating system.

To use a software image, download it and copy it to the media in one of these ways:

- Create a removable USB device (for installing SecurePlatform or Gaia).
- Burn it to a DVD.

USB Installation

You can install a SecurePlatform or Gaia appliance or open server using an ISO on a removable USB device. To create the removable device, download the Check Point ISomorphic utility (<http://supportcontent.checkpoint.com/solutions?id=sk65205>).

Glossary

Check Point product names and technologies, and industry standard terms:

Term	Definition
Database Migration	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.

Term	Definition
Open Server	Non-Check Point hardware platform that is certified by Check Point as supporting Check Point products. Open Servers allow customers the flexibility of deploying Check Point software on systems which have not been pre-hardened or pre-installed (servers running standard versions of Solaris, Windows, Red Hat Linux).
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	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, previously known as ROBO Gateway)
SmartLSM Profile	(previously ROBO Profile): An object that you define to represent properties of multiple SmartLSM Security Gateways. 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	Used to regulate the incoming and outgoing flow of communication.
Security Management server	Used 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	GUI applications used to manage different aspects of the Security Policy. For example, <i>SmartView Tracker</i> is a SmartConsole client used to view logs.
SmartDashboard	SmartConsole client that is used to create Security Policies.
SmartUpdate	SmartConsole client used to centrally upgrade and manage Check Point software and licenses.

Multi-Domain Security Management specific terms:

Term	Definition
Active Domain Management Server	In a High Availability deployment, the only Domain Management Server that can manage a specific Domain.
Active Multi-Domain Server	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.
Administrator	Security administrator with permissions to manage elements of a Multi-Domain Security Management deployment.
Domain	A network or group of networks belonging to a specified entity, such as a company, business unit or organization.

Term	Definition
Domain Log Server	Virtual log server for a specified Domain.
Domain Management Server	Virtual Security Management Server that manages Security Gateways for one Domain.
Global Objects	Network objects used in global policy rules. Examples of global objects include hosts, global Domain Management Servers, and global VPN communities.
Global Policy	Policies that are assigned to all Domains, or to specified groups of Domains.
Internal Certificate Authority (ICA)	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.
Multi-Domain Log Server	Physical log server that hosts the log database for all Domains.
Multi-Domain Security Management	Check Point centralized management solution for large-scale, distributed environments with many different network Domains.
Multi-Domain Server	Multi-Domain Security Management server that contains all system information as well as the security policy databases for individual Domains.
Primary Multi-Domain Server	The first Multi-Domain Server that you define and log into in a High Availability deployment.
Secondary Multi-Domain Server	Any subsequent Multi-Domain Server that you define in a High Availability deployment.
Standby Domain Management Server	In a High Availability deployment, any Domain Management Server for a specified Domain that is not designated as the active Domain Management Server.
Standby Multi-Domain Server	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.

Compatibility Tables

If the existing Check Point implementation contains products that are not supported by R75.40VS, the installation process terminates. For a list of compatible products by platform, refer to the *R75.40VS Release Notes* (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

Chapter 2

Licensing

In This Chapter

Software Licensing	13
Licensing Multi-Domain Security Management	13

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>).

If you are new to Check Point, we recommend that you visit the Check Point User Center.

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

Software Licensing

If you have not yet migrated to Software Blade licenses, use the migration options from Check Point's website (<http://www.checkpoint.com/products/promo/software-blades/upgrade/index.html>). Migration to Software Blades is free of charge to purchasers of the Software Subscription service (Enterprise Base Support).

Licenses are required for management servers and Security Gateways.

Check Point software is activated using a certificate key. 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.

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

1. Add the required Check Point products/evaluations to your User Center account: select **Accounts & Products > Add Products**.
2. Generate a license key for your products/evaluations: select **Accounts & Products > Products**. Select your products and click **Activate License**. The selected product evaluations are assigned license keys.
3. Complete installation and configuration:
 - a) Read and accept the End Users License Agreement.
 - b) Import the product license key. Using the Check Point Configuration Tool or SmartUpdate to import the license. SmartUpdate lets you centrally upgrade and manage Check Point software and licenses. The certificate keys associate the product license with the Security Management server:
 - 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.

Licensing Multi-Domain Security Management

- Multi-Domain Security Management licenses are associated with the IP address of the licensed entity.
- To add a Management domain, you must add a Domain license to Multi-Domain Security Management.
- To add a Management Software Blade to a Multi-Domain Server, you must add the required blade licenses to Multi-Domain Security Management.
- Multi-Domain Security Management licenses can be imported using the Check Point command-line licensing tool or the SmartDomain Manager.

Disk Space

When you install R75.40VS, the installation wizard makes sure that there is sufficient space on the hard disk to install the product on the computer or appliance.

If there is not sufficient space on the hard disk, an error message is shown. The message states:

- The amount of disk space necessary to install the product.
- The directory where the product is installed.
- The amount of free disk space that is available in the directory.

After there is sufficient disk space, install the product.

Gaia Automatic Software Updates

After you install or upgrade to R75.40VS on Gaia, you can update software automatically.








Gaia automatically locates and shows the available software update packages for Check Point products and the Gaia OS. The updates packages are for minor releases and hotfixes. Only packages that are applicable to the Gaia computer are shown. The packages can be downloaded from the Check Point Support center and installed.

For instructions, see the Gaia Administration Guide

(<http://supportcontent.checkpoint.com/solutions?id=sk76540>), "Software Updates" chapter.

SmartDashboard Toolbar

You can use the SmartDashboard toolbar to do these actions:

Icon	Description
	Open the SmartDashboard menu. When you are instructed to selected menu options, click this button first. For example, if you are instructed to select Manage > Users and Administrators , click this button to open the Manage menu and then select the Users and Administrators option.
	Save current policy and all system objects.
	Refresh policy from the Security Management Server.
	Change global properties.
	Verify rule base consistency.
	Install the policy on Security Gateways or VSX Gateways.
	Open SmartConsoles.

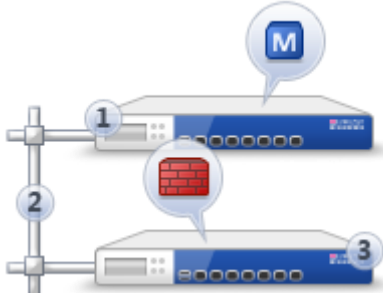


Deployment Options

There are different deployment scenarios for Check Point software products.

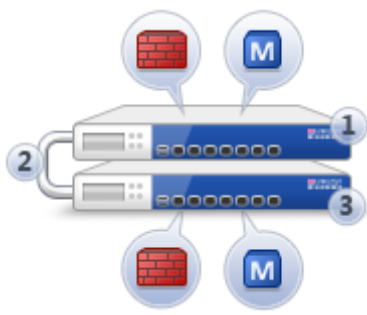


- **Standalone Deployment** - The Security Management Server and the Security Gateway are installed on the same computer or appliance.

	Item	Description
	1	Standalone computer
		Security Gateway component
		Security Management Server component


- **Distributed Deployment** - The Security Gateway and the Security Management Server are installed on different computers or appliances.

	Item	Description
	1	Security Management Server
	2	Network connection
	3	Security Gateway
		Security Gateway component
		Security Management Server component

- **Standalone Full HA** - Security Management server and Security Gateway are each installed on one appliance, and two appliances work in High Availability mode.

	Item	Description
	1	Primary appliance
	2	Direct appliance to appliance connection
	3	Backup appliance
		Security Gateway component
		Security Management Server component

- **Bridge Mode** - Add a Security Gateway to an existing environment without changing IP Routing.

	Item	Description
	1 and 2	Switches
		Security Gateway Firewall bridging Layer-2 traffic over the one IP address, with a subnet on each side using the same address.

Chapter 3

Installing Security Management Server and Security Gateways

In This Chapter

Installing Standalone	17
Installing Security Management Server	34
Installing Security Gateway	40
Installing Full High Availability Appliances	47
Deploying Bridge Mode Security Gateways	52
Installing SmartConsole Clients	53
Post-Installation Configuration	54

Check Point software runs on many platforms and pre-configured appliances. Installations differ by deployment option, platform and operating system.

During installation, an automatic check is done to make sure that there is enough disk space for the installation.

For more about supported deployments, platforms, hardware requirements and operating systems, see the *R75.40VS Release Notes* (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).






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

Installing Standalone

In This Section

Disk Partitions in a Gaia Clean Installation	17
Installing Standalone on Appliances	18
Installing Standalone on Open Servers	30

Standalone Deployment - The Security Management Server and the Security Gateway are installed on the same computer or appliance.

	Item	Description
	1	Standalone computer
		Security Gateway component
		Security Management Server component

Disk Partitions in a Gaia Clean Installation

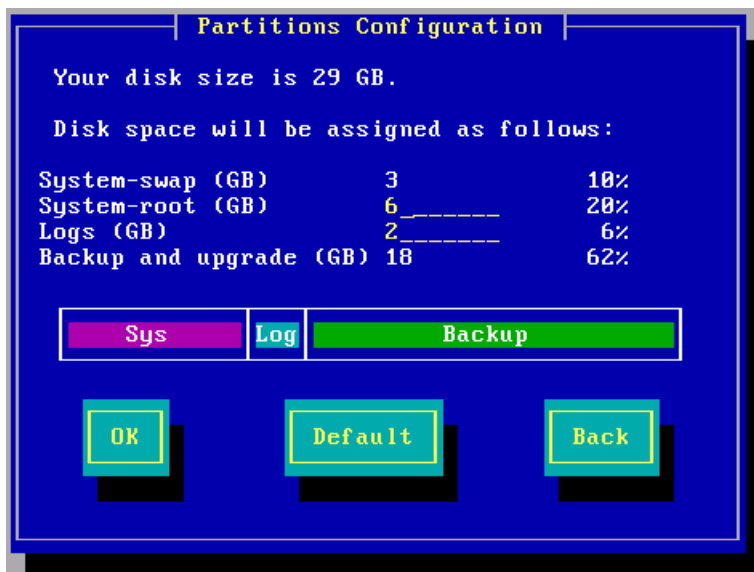
In general, Gaia disk partitions in a clean installation are larger than SecurePlatform partitions.

On an appliance, the size of the disk partitions is predefined.

When installing Gaia on an open server, these partitions have default sizes that you can change:

- System-swap
- System-root
- Logs
- Backup Images

For example:



To see the size of the system-root and log partitions on an installed system, enter `expert` mode and run the `df -h` command.

For example:

```
>df -h
Filesystem                                Size  Used Avail Used%  Mounted on
/dev/mapper/vg_splat-lv_current          13G   3.0G   9.0G   25%   /
/dev/sda1                                145M   19M  119M   14%   /boot
tmpfs                                     187M    0   187M    0%   /dev/shm
/dev/mapper/vg_splat-lv_log              9.0G   78M   2.7G    1%   /var/log
```

In this example, the system root partition has 13G of disk space, and 9.0G is assigned for logs.

Most of the remaining space on the disk is reserved for backup images. To see the disk space assigned for backup images, connect to the Gaia WebUI and go to the **Maintenance > Image Management** page. On an Open Server, the available space shown in the **Image Management** page is less than the space you defined when installing Gaia. The difference between the two amounts is the space reserved for snapshot images that are automatically created during an upgrade. The amount of reserved space equals the size of the system-root partition.

Installing Standalone on Appliances

You can install a Standalone deployment on UTM-1 appliances, certain 2012 Models, and IP appliances. You can install the Gaia or SecurePlatform operating system. For more about supported appliances, see the *R75.40VS Release Notes*.

UTM-1 and 2012 Models

In UTM-1 and 2012 model appliances, the first step to installation is to install the operating system.

Download the R75.40VS ISO file for the relevant operating system and burn it on a DVD disc. Use the ISO to do a clean install of SecurePlatform or Gaia on the appliance.

To install R75.40VS SecurePlatform or Gaia:

1. Download the ISO file with the R75.40VS image for the Operating System: SecurePlatform or Gaia (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
 2. Burn the ISO file on a DVD.
 3. Turn off the appliance.
 4. Connect an external DVD drive to the USB socket on the appliance.
Make sure that the DVD with the R75.40VS ISO file is in the DVD drive.
 5. Connect the supplied DB9 serial cable to the console port on the front of the appliance.
 6. Connect to the appliance using a terminal emulation program such as Microsoft HyperTerminal or PuTTY.
 7. Configure the terminal emulation program:
 - In the HyperTerminal **Connect To** window, select a port from the **Connect using** list.
 - In PuTTY select the **Serial** connection type.
 8. Define the serial port settings: 9600 BPS, 8 bits, no parity, 1 stop bit.
 9. From the **Flow control** list, select **None**.
 10. Connect to the appliance.
 11. Turn on the appliance.
The appliance begins the boot process and status messages show in the terminal emulation program.
 12. Press **Enter**. You must press the Enter key within 90 seconds or the appliance boots from the hard drive.
The R75.40VS ISO file is installed on the appliance.
 13. Reboot the appliance.
 - For Gaia - Press **CTRL+C**.
 - For SecurePlatform - Turn off the appliance and then turn it on again.
- When the model number is shown on the LCD screen, the installation process is complete.

Gaia

To install Check Point products on Gaia UTM-1 and 2012 model appliances, use the First Time Configuration Wizard.



Note - The internal interface (INT) on a UTM-1 appliance is used as the management interface.

To start the First Time Configuration Wizard:

1. Connect a standard network cable to the appliance management interface and to your management network.
The management interface is marked **MGMT**. This interface is preconfigured with the IP address 192.168.1.1.
2. Connect to the management interface from a computer on the same network subnet.
For example: IP address 192.168.1.x and net mask 255.255.255.0. This can be changed in the WebUI, after you complete the First Time Configuration Wizard.
3. To access the management interface, open a connection from a browser to the default management IP address: `https://192.168.1.1`
4. The login page opens. Log in to the system using the default username and password: `admin` and `admin`
5. Click **Login**.



Note - The features configured in the First Time Configuration Wizard are accessible after completing the wizard using the WebUI menu. The WebUI menu can be accessed by navigating to `https://<appliance_ip_address>`.

6. The **First Time Configuration Wizard** runs.

To configure Gaia standalone appliances:

1. In the First Time Configuration Wizard, set the password for **admin** and then click **Next**.
2. Set the date and time (manually, or enter the hostname or IP address of the NTP server) and then click **Next**.
3. Set the **host name** for the appliance.
4. **Optional:** Set the **domain name**, and IPv4 addresses for the **DNS servers**.
You can use the Gaia WebUI to configure IPv6 DNS servers.
Click **Next**.
5. Set the IPv4 address for the management interface.
If you change the management IP address, the new IP address is assigned to the interface. The old IP address is added as an alias and is used to maintain connectivity.
6. **Optional:** Configure the appliance as a DHCP server.
Click **Next**.
7. Select **Security Gateway** and **Security Management** and then click **Next**.
8. Set the username and password for the Security Management server administrator account and then click **Next**.
9. Define the GUI Clients that can log in to the Security Management server and then click **Next**
10. Click **Finish** and then click OK.
11. If the **Help Check Point Improve Software Updates** window shows, click **Yes** or **No** as necessary.
Gaia R75.40VS is installed on the appliance.
12. If necessary, download SmartConsole from the Gaia WebUI.
 - a) Open a connection from a browser to the WebUI at `https://<management_ip_address>`.
 - b) In the **Overview** page, click **Download Now!**.

SecurePlatform

Use the SecurePlatform First Time Configuration Wizard to configure the new image on the appliance.



Note - The internal interface (INT) on a UTM-1 appliance is used as the management interface.

To start the First Time Configuration Wizard:

1. Connect a standard network cable to the appliance management interface and to your management network.
The management interface is marked **MGMT**.
2. Open Internet Explorer to the default management IP address, `https://192.168.1.1:4434`
3. Log in to the system using the default login name/password: **admin/admin**.



Note - You can use the WebUI menu to configure the appliance settings. Navigate to `https://<appliance_ip_address>:4434`.

4. Set the username and password for the administrator account.
5. Click **Save and Login**.

The First Time Configuration Wizard opens.

To configure SecurePlatform standalone:

1. In the First Time Configuration Wizard, set the date and time and then click **Next**.
2. Configure the settings for the management and other interfaces and then click **Next**.
3. Configure the settings for the routing table and then click **Next**.
4. Set the **host name**, **domain name**, and **DNS servers** and then click **Next**.
5. Select **Locally Managed** and then click **Next**.
6. Do not configure the appliance as part of a cluster and then click **Next**.
7. Set the clients that can manage the appliance using a web or SSH connection and then click **Next**.
8. **Optional:** Download SmartConsole and then click **Next**.
9. Click **Finish**.

The **Summary** window shows the settings for the appliance.

SecurePlatform R75.40VS is installed on the appliance.

IP Appliances

For the IP Appliance models that are supported for this release, see the *R75.40VS Release Notes*.

Gaia

You can install the Gaia operating system and Check Point Standalone, Security Management server, and Security Gateway deployments on IP appliances. This section tells you how to install a Standalone deployment.

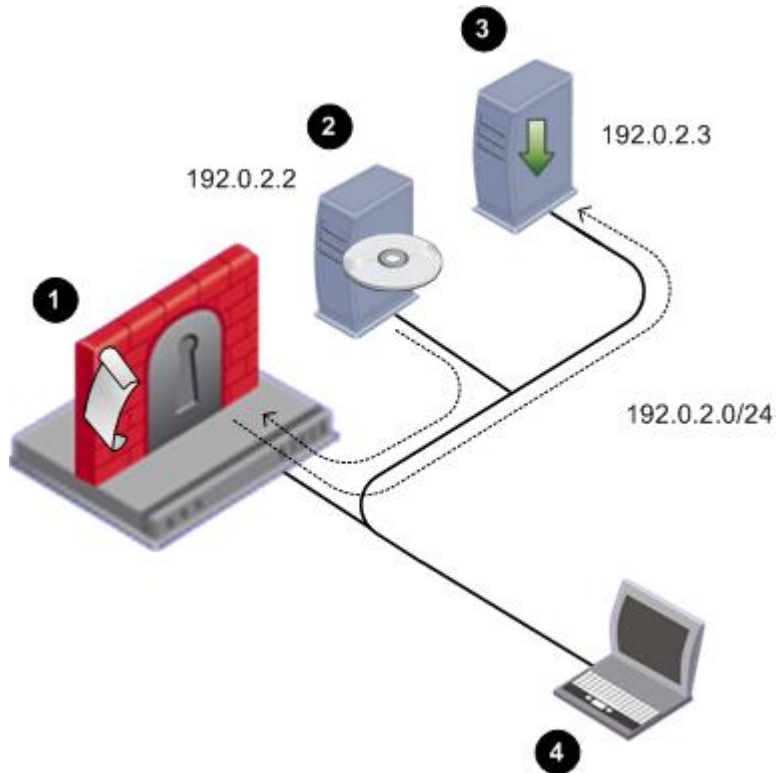
This is a clean installation. The IPSO and Check Point product configurations are not imported into Gaia.



Note - You cannot upgrade an IPSO Standalone or Security Management server appliance to Gaia.

Preparing for Installation

Set up this environment.



Item	
1	<p>IP Appliance with</p> <ul style="list-style-type: none"> • IPSO • IPSO to Gaia installation package or upgrade package.
2	<p>FTP Server with a Gaia ISO image mounted. The ISO is copied to the IP Appliance as part of the installation or upgrade process. The FTP server can be Linux-based or Windows-based ("Step 2: Putting the Gaia ISO on an FTP Server" on page 23).</p> <p>In this example, the FTP Server is at 192.0.2.2.</p>
3	<p>Optional: FTP Server used as a location for one or more of the following:</p> <ul style="list-style-type: none"> • Backup of IPSO and the Security Gateway configuration. (recommended) • A special SmartUpdate package that can be to distribute the IPSO to Gaia installation and upgrade package to multiple Security Gateways. • A special package that can be used to install or upgrade Security Gateways, one at a time, without having to answer any questions. This package is created using the answers supplied when running the installation and upgrade package. <p>You can use the same FTP server as for the Gaia ISO, or a different one. In this example, the FTP Server is at 192.0.2.3.</p>
4	<p>Computer with console access to the IP appliance and to the FTP server(s).</p> <p>Console access is recommended because it allows you to keep the connection to the IP Appliance throughout the installation or upgrade. If you connect via SSH you lose the connection after the IP Appliance reboots, and you will not be able to track the installation or upgrade progress.</p>

Installation Procedure Overview



Important - This is an overview of the steps. Detailed instructions follow.

Step 1: Get the IPSO to Gaia installation and upgrade package (tgz) and the Gaia ISO image.

Step 2: Put the Gaia ISO on an FTP server.

Step 3: Install the installation and upgrade package on the IP Appliance using Network Voyager or `clish`.

Step 4: Run the script:

- Clean install - `run-install-gaia`
- Upgrade - `run-upgrade-to-Gaia`

Step 5: Enter FTP server details and the ISO location. The script tests the FTP Server environment:

- a) Route to the FTP server
- b) Interface speed and duplex settings
- c) FTP access with the given credentials
- d) FTP access to the specified path
- e) Path contains the Gaia ISO and the user has Read/Write access to the directory
- f) Multiple simultaneous connections (>20) to the FTP server are allowed
- g) Timeout on FTP server is not too low
- h) FTP access to files downloaded by the Gaia boot manager

Step 6: Optional, but recommended: Enter data for an FTP server to hold IPSO system and configuration backup.

Step 7: Optional: Enter data to make a customized IPSO to Gaia upgrade package. Use this to upgrade multiple Security Gateways with SmartUpdate.

- a) Upgrade one Security Gateway with the standard IPSO to Gaia upgrade package. Enter the required data to create the special upgrade package.
- b) Upgrade all other Security Gateways simultaneously, using the special upgrade package, without more data. All IP Appliances must be able to access the same ftp servers as the first Security Gateway.

Step 8: Confirm your selections.

Step 9: The installation or upgrade package now runs automatically:

- a) If you made a backup package: The backup tar files are copied from the IP Appliance to the FTP server.
- b) If you made a customized installation or upgrade package: The package is copied from the IP Appliance to the FTP server.
- c) The Gaia image is copied from the FTP server to the IP Appliance.
- d) The Gaia image is installed.
- e) The Gaia boot manager is installed.
- f) The IP Appliance reboots.

You see the Gaia prompt on the IP Appliance.

Step 10: Run the First Time Configuration Wizard and select the products to install.

Step 1: Getting the Upgrade Package and the Gaia Image

1. Download the Gaia packages for IP Appliance from the R75.40VS home page on the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

You will see two packages:

- Gaia ISO image
 - IPSO to Gaia installation and upgrade package. The file name is `Check_Point_Install_and_Upgrade_IPSO6.2_to_Gaia_R75.40VS.tgz`
2. Prepare the installation and upgrade packages:
Copy the packages to an FTP server, in a directory of your choice. Or transfer the packages by FTP to the IP Appliance.

Step 2: Putting the Gaia ISO on an FTP Server**Network Requirements**

Important - High network traffic or large transfers (more than 10/100 Mbps links) can interfere with the FTP transfers for installation.

- Make sure the appliance can reach the FTP server.
- Make sure there is no Firewall which blocks incoming FTP requests from the appliance to the FTP server.
- Configure the FTP server to allow more than 100 (or an unlimited number of) concurrent connections.
- Make sure the Gaia ISO file is mounted on a directory to which the user has access permissions.

On a Linux-based FTP Server:

1. Upload the Gaia ISO file to the FTP server
2. On the FTP server, run:

```
mount -o loop -t iso9660 <ISO_filename> <mounting_destination_dir>
```

On a Windows-based FTP Server:

1. Upload the Gaia ISO file to the FTP server
2. Extract the Gaia ISO file to a folder on the FTP Server. Use 7-zip, Winzip, WinRAR or similar.
3. In the folder, run the file `copyrpms.bat`

This batch file copies installation files, to give a required workaround to Windows' inability to support soft links.

4. Give FTP credentials to the folder, so the folder can be accessed via FTP.

Step 3: Installing the Package on the IP Appliance

1. Log in to the IP Appliance using a console.
2. Run `clish`
3. Install the IPSO to Gaia installation and upgrade package on the IPSO appliance using `clish` or using Network Voyager (see the Network Voyager Reference Guide (http://supportcontent.checkpoint.com/documentation_download?ID=10293)).

To use `clish`:

- If the IPSO to Gaia package is on an FTP server, run:

```
add package media ftp addr <FTP_IP> user <uname> password <pass> name  
<full_path>/Check_Point_Upgrade_Package_R75.40VS.IPSO6.2_to_Gaia.tgz
```

Note - If using anonymous ftp, change `ftp` to `anonftp`.

- If the IPSO to Gaia package is on the IP Appliance, go to the directory where the package is located, and run the `clish` command:

```
add package media local name  
./Check_Point_Upgrade_Package_R75.40VS.IPSO6.2_to_Gaia.tgz
```

The installation and upgrade package is installed.

```
Trying to install package: ./package_name.tgz
Package Information --
Name       : IPSO to Gaia Upgrade
Version    : <version>
Release    : <Release>
Description: IPSO to Gaia Upgrade Package (<package_version>)
Package will be installed under: /opt
Package installed and activated successfully.
End of package installation.
```

The installation success message is Package installed and activated successfully.

The package is reported to be activated, but there are no background processes running.

4. Show the installed and active packages:

```
show package active
```

Name	Ver	Rel	Dir	Desc
{Check Point CPinfo }	10	00	/opt/CPinfo-10	{Check Point CPinfo}
{Check Point R70}	R70	00	/opt/CPsuite-R70	{Check Point R70}
{IPSO to Gaia Upgrade}	<ver>	<rel>	/opt/<package_name>	{IPSO to Gaia Upgrade Package (<upgrade_package_version>)}

5. Exit clish. Run: exit

Step 4: Running the Installation and Upgrade Script

1. Go to the location of the package

```
cd /opt/<package_name>/
```

2. To upgrade, run

```
./run-upgrade-to-Gaia
```

To do a clean installation, run

```
./run-install-Gaia
```

If you are upgrading multiple appliances from a special upgrade package that was previously saved, the installation or upgrade runs automatically. Continue with [Step 9](#) ("[Step 9: Upgrade Runs Automatically](#)" on page [103](#)).

If you are upgrading or installing one appliance, continue here.

The script runs. The following shows an upgrade. If you do a clean installation, the IPSO configuration is not transferred to Gaia.


```

Welcome to the IPSO to Gaia Install/Upgrade procedure.

Checking platform...OK
Checking IPSO OS version ...OK
Checking hostname ...
Checking your configuration
Summary:
    Errors:      0
    Warnings:    0
    Information: 14
Total Grade: 94
Details in file "/var/tmp/verify-IPSO-for-Gaia.msgs".

A newer version of this script may be available.
Contact the Check Point UserCenter at https://usercenter.checkpoint.com
and see SK66569.

Do you want to continue with the upgrade ? [y] y

=====
The following types of information are needed to prepare
your IPSO appliance for the upgrade:

- info about downloading the Gaia image.
- info about transferring the verification reports (optional).
- info about transferring an IPSO backup (optional).
- info about transferring a special upgrade package with your answers
(optional).

Answer the prompts for this info and then the upgrade is performed.

Hit 'Enter' to continue or Ctrl-C to exit

```

3. Supply the information for downloading the Gaia image



Note - If you have run the upgrade script before, the previously entered values are shown in square brackets []. Press **Enter** to accept the values, or type in the new values and press **Enter**.

Step 5: Verifying the FTP Server

Enter the requested FTP server data and the path to the Gaia installation file.

	Required Directory Value
If ISO is mounted to a non-FTP directory	Enter full path to ISO. A relative path or shortcut link will not work. Example: if /home/username/gaia , ./gaia will not work.
If ISO is mounted to /var/ftp , and FTP user account is used to install	Enter path to ISO. A shortened path will work. Example: if /var/ftp/gaia , gaia will work.
If ISO is mounted to /var/ftp , and non-FTP user account is used to install	Enter full path to ISO. A relative path or shortcut link will not work.

The script runs some tests to verify the FTP environment. If errors are detected, correct the FTP server configuration and then instruct the program to verify the FTP environment again.

Here is an example of a successful test:

```

Info for download of the Gaia image:
Info for download of the Gaia image:
IP address of FTP server [192.0.2.2]:
User name [gwhite]:
Password [*****]:
Directory [/mnt/fiber292]:
Performing tests of access to FTP server and Gaia ISO
Checking route to 192.0.2.2 ... OK
Interface: eth-s4p1 speed 100M, duplex full
Checking FTP access with given credentials ... OK
Checking FTP access to /mnt/fiber292 ... OK
Checking /mnt/fiber292 is Gaia ISO ... Yes
Checking multiple simultaneous connections to 192.0.2.2 ... OK
Checking timeout to 192.0.2.2 ... OK
Checking FTP access to files downloaded by Gaia boot-manager
    system/ramdisk.pxe ... OK
    system/base/stage2.img ... OK

```

Step 6 (Optional, Recommended): Supplying Reports and Backup Server Information

The script will request details of the FTP server to store reports and backup data. The same path-rules apply here as in *Step 5* ("[Step 5: Verifying the FTP Server](#)" on page 25). The backup creates two tgz files, for:

- IPSO operating system configuration files, user directories, and log files.
- Security Gateway backup files.

Here is an example:

```

A complete backup of the IPSO system can performed
including system configuration, user home directories,
log files and files from packages.

Do you want to perform this backup ? [y]

Use IP address '192.0.2.2' and user 'root' for the backup? [n]

Details for transferring the IPSO Backup:
IP address of FTP server []: 192.0.2.3
User name []: ftp
Password []: ***
Directory []: /backupdir

Checking FTP access to 192.0.2.3 (it may take a minute) ... done

```

Step 7: (Optional): Supplying Special Package Server Information

Enter data of the destination FTP server for the special upgrade package. Enter a destination directory, with the same rules as in *Step 5* ("[Step 5: Verifying the FTP Server](#)" on page 25).

```

A package with your answers to the previous prompts can be created.
This package can be used on other IPSO gateways for
unattended conversion to Gaia.

Do you want to create such a package? [y]

Details for transferring the package with your answers:
IP address of FTP server [192.0.2.3]:
User name [ftp]:
Password [***]:
Directory [packagedir]:
Checking FTP access to 192.0.2.3 (it may take a minute) ... done

```

Step 8: Confirming Your Selections

You see a summary of all your answers.

```
Information for download of the Gaia image:
  FTP Server IP Address = 192.0.2.2
  FTP Server user name = root
  Directory on FTP Server = /imagedir

Information for transferring the IPSO Backup:
  FTP Server IP Address = 192.0.2.3
  FTP Server user name = ftp
  Directory on FTP Server = /backupdir

Information for transferring the package with your answers:
  FTP Server IP Address = 192.0.2.3
  FTP Server user name = ftp
  Directory on FTP Server = /packagedir

Are these values correct? [y]
```

1. Click **n** to change the selections you made before, or type **y** to start the upgrade.

The backup file and the special upgrade package file, if you chose to create them, are created.

```
Writing values to file
Performing IPSO backup (file <ipso_backup_file_name>.tgz) ... done
Performing Check Point Security Gateway backup (file <Security
Gateway_backup_file_name>.tgz) ... done
Transferring IPSO and Check Point Security Gateway backup files ... done
Creating a package with your answers (<package_name>_AUTO.tgz) ... done
Transferring package with your answers ... done
Installing Gaia Boot Manager ... done
```

2. You have 30 seconds to abort. To stop the upgrade, press **Enter**.

```
IP appliance reboots in 30 seconds to complete the upgrade.
Hit 'Enter' to abort.
```



Important - If you want to make changes, press **Enter** now.

This stops the upgrade to Gaia. To complete the upgrade to Gaia, reboot the IP Appliance.

Step 9: Installation Runs Automatically

The installation runs unattended.

- The IP Appliance reboots.
- The Gaia Boot Manager runs.



Important - After reboot, the system sometimes shows the Boot Manager prompt.

To complete installation, type **INSTALL** at the Boot Manager prompt, and enter the requested data. Installation continues.

- The Gaia image is installed.



- The IPSO and R75.40VS configurations are not imported into Gaia.
- The Gaia prompt shows.



Important - The HTTPS port for the WebUI is set to 443 after an installation or upgrade.

To change this, you must use SmartDashboard > **Gateway Properties** > **Portal Settings**.

Step 10: Selecting Check Point Products

To configure Check Point products on Gaia, use the First Time Configuration Wizard. Configure the operating system and install the products in one wizard.

To configure standalone products on Gaia:

1. Using your Web browser, go to the WebUI:
`https://<Gaia management IP address>`
2. In the **Gaia Portal** window, log in using the administrator name and password that you defined during the installation procedure.
3. The WebUI shows the **First Time Configuration Wizard**. Click **Next**.
4. Set the date and time (manually, or enter the hostname or IP address of the NTP server) and then click **Next**.
5. Set the **host name** for the appliance.
6. **Optional:** Set the **domain name**, and IPv4 addresses for the **DNS servers**.
You can use the Gaia WebUI to configure IPv6 DNS servers.
Click **Next**.
7. Set the IPv4 address for the management interface.
If you change the management IP address, the new IP address is assigned to the interface. The old IP address is added as an alias and is used to maintain connectivity.
8. **Optional:** Configure the appliance as a DHCP server.
Click **Next**.
9. Set the username and password for the Security Management server administrator account and then click **Next**.
10. Select **Security Gateway** and **Security Management** and then click **Next**.
11. Define the GUI Clients that can log in to the Security Management server and then click **Next**.
12. Click **Finish** and then click OK.
13. If the **Help Check Point Improve Software Updates** window shows, click **Yes** or **No** as necessary.

After some minutes, you can use the WebUI to configure your standalone environment.

Rollback from Gaia to IPSO

You can roll back from Gaia to IPSO 6.2. You can also restore the Check Point Security Gateway and/or Security Management server configuration.

Before doing a rollback from Gaia to IPSO:

Make sure that:

1. The IPSO boot manager installer is available. Download it from the R75.40VS home page (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
2. An IPSO image is available. Put the IPSO image on an FTP server, and make sure that the FTP server is accessible from the Gaia IP Appliance.
3. A backup of the Check Point Security Gateway on the Gaia IP Appliance is available. Put the backup tar file on an FTP server, and make sure the FTP server is accessible from the Gaia IP Appliance.

To roll back from Gaia to IPSO:

1. At the Gaia command line prompt, login as the administrator.
2. Go to expert mode. Type `expert` and supply the credentials.
3. Download the IPSO boot manager installer
`Check_Point_R75.40VS_Install_IPSOBootmanager.sh` from the R75.40VS home page on the Support Center.
4. Copy the IPSO boot manager installer to a location of your choice on the Gaia IP Appliance. For example, to `/var/tmp`.
5. Change file attributes to give executable permissions. Run

```
chmod 777 Check_Point_R75.40VS_Install_IPSOBootmanager.sh
```

6. Install the IPSO boot manager. At the command prompt run

```
./Check_Point_R75.40VS_Install_IPSOBootmanager.sh /dev/hda
```

The script asks if you want to roll back to

1. IPSO 4.2
2. IPSO 6.2

7. Choose 2

8. Type `reboot`

After the reboot, the system is running the IPSO boot manager.

9. At the `BOOTMGR>` prompt, install the IPSO image. Run

```
install
```

10. Enter this data:

- IP address of the IP Appliance.
- Default gateway of the IP Appliance.
- IP address of the FTP server with the IPSO image.
- User credentials.
- Directory path.
- Various configuration questions (about the chassis serial number, whether the system is part of a VRRP cluster, and whether IGMP and BGP are enabled).

The system automatically reboots into IPSO.

11. Configure the IP Appliance:

- Hostname
- New password for `admin`
- Enable the management port physical interface
- IP address for the management interface
- Default gateway

To restore the Check Point Security Gateway configuration:

1. Log in to the newly installed and configured IPSO IP Appliance as `admin`
2. Use FTP to transfer the backup archive file containing the Check Point Security Gateway to the IP Appliance, and then uncompress the archive. In the following example,
 - The name of the backup archive is `CP_archive_nms71_20101124.tgz`
 - The IP address of the FTP server containing the backup archive is `192.0.2.3`.

```
cd /tmp
ftp ftp://192.0.2.3>/pub/CP_archive_nms71_20101124.tgz
tar xzf /tmp/CP_archive_nms71_20101124.tgz
```

3. Restore the IPSO backup file using the `set restore` CLI commands. In the following example,
 - The IP address of the FTP server containing the IPSO backup file is `192.0.2.2`
 - The IPSO backup file is in the `pub` directory.



Important - If the backup contains IPSO and Check Point configuration data, the Check Point packages must be installed first before trying to restore the backup; otherwise the restore will fail.

```
clish
set restore remote ftp-site ftp://192.0.2.2
set restore remote ftp-user <username e.g. anonymous>
set restore remote ftp-pass <password>
set restore remote ftp-dir pub
set restore remote filename i2g_backup_<hostname and timestamp>.tgz
```

IPSO automatically reboots.

4. Log out.
5. Log in as `admin`.
6. Verify the configuration has been restored.

Installing Standalone on Open Servers

A standalone deployment can be installed on any computer that meets the minimum requirements (see the *Release Notes*). For Gaia and SecurePlatform, first install and configure the operating system. Then install Check Point products. You can also install on Windows.

Gaia

This procedure explains how to install the Gaia operating system on an open server. Then you configure the Standalone Check Point products.

To install Gaia on an open server:

1. Start the computer using the installation DVD.
2. When the first screen shows, select **Install Gaia on the system** and press **Enter**.
3. You must press **Enter** in 60 seconds, or the computer will try to start from the hard drive. The timer countdown stops once you press **Enter**. There is no time limit for the subsequent steps.
4. Press **OK** to continue with the installation.
5. Select a keyboard language. English US is the default.
6. Make sure the disk space allocation is appropriate for the environment.
7. Enter and confirm the password for the **admin** account.
8. Select the management interface (default = `eth0`).
9. Configure the management IP address, net mask and default gateway. You can define the DHCP server on this interface.
10. Select **OK** to format your hard drive and start the installation.
11. Press **reboot** to complete the installation.

To configure Check Point products on Gaia, use the First Time Configuration Wizard. Configure the operating system and install the products in one wizard.

To configure standalone products on Gaia:

1. Using your Web browser, go to the WebUI:
`https://<Gaia management IP address>`
2. In the **Gaia Portal** window, log in using the administrator name and password that you defined during the installation procedure.
3. The WebUI shows the **First Time Configuration Wizard**. Click **Next**.
4. Set the date and time (manually, or enter the hostname or IP address of the NTP server) and then click **Next**.
5. Set the **host name** for the appliance.
6. **Optional:** Set the **domain name**, and IPv4 addresses for the **DNS servers**.
You can use the Gaia WebUI to configure IPv6 DNS servers.
Click **Next**.
7. Set the IPv4 address for the management interface.
If you change the management IP address, the new IP address is assigned to the interface. The old IP address is added as an alias and is used to maintain connectivity.
8. **Optional:** Configure the appliance as a DHCP server.
Click **Next**.
9. Set the username and password for the Security Management server administrator account and then click **Next**.
10. Select **Security Gateway** and **Security Management** and then click **Next**.
11. Define the GUI Clients that can log in to the Security Management server and then click **Next**.
12. Click **Finish** and then click OK.
13. If the **Help Check Point Improve Software Updates** window shows, click **Yes** or **No** as necessary.
After some minutes, you can use the WebUI to configure your standalone environment.
14. If necessary, download SmartConsole from the Gaia WebUI.


- a) Open a connection from a browser to the WebUI at `https://<management_ip_address>`.
- b) In the **Overview** page, click **Download Now!**.

SecurePlatform



Important - Installing the SecurePlatform operating system deletes all data on the hard drive.

To install on SecurePlatform using a DVD:

1. Put the installation DVD into the drive and boot the computer from the DVD.
 2. When the SecurePlatform window opens, press **Enter**.
You must press **Enter** in 90 seconds, or the computer starts 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. **Optional:** Click **Device List** to resolve hardware compatibility issues.
 5. Click **OK** to continue with the installation.
 6. Select a keyboard language and then click **OK**.
 7. Select **eth0** as the management interface (networking device) and then click **OK**.
 8. Configure the settings for the **eth0** interface (NIC) and then click **OK**.
 9. **Not for Multi-Domain Server:** Configure the clients that can connect to the WebUI and then click **OK**.
- 

Note - If you are going to deploy remote access or Endpoint Security software, do not use the default port, 443.
10. Click **OK** to install SecurePlatform.
 11. When the **Complete** window opens, disconnect the DVD drive from the computer.
 12. Click **OK** to complete the installation process and restart the computer.

When the computer restarts, configure the operating system. You can use the WebUI or using the CLI.

To configure SecurePlatform using the WebUI:

1. Open a browser to the administration IP address:
 - For appliances - `https://<IP_address>:4434`
 - For open servers - `https://<IP_address>`



Note - Pop-ups must always be allowed on `https://<IP_address>`.

The login page appears.

2. Login with the default login name (**admin**) password (**admin**) and click **Login**.
3. Download the password recovery login token file. Save it in a safe place.
4. Change the default login name and password.
5. Click **Save and Login**.

In the First Time Configuration Wizard, configure these settings:

- Network connections. The management interface has the administration IP address.
 - Routing table.
 - DNS servers.
 - Host and domain name.
 - Date, time, and time zone.
 - Allowed IPs of SSH and administration WebUI clients.
 - Products to install.
 - Security Management GUI Clients.
 - Security Management administrators.
6. Click **Finish**

To configure SecurePlatform using the CLI:

1. Log in to the system using the default login name/password: **admin/admin**.
2. Set the username and password for the administrator account.
3. Run: `sysconfig`.
The first-time system configuration wizard starts. Enter **n** to continue.
4. Set the **host name**, **domain name**, and **DNS servers**.
5. Configure the settings for the management and other interfaces (network connections).
6. Configure the settings for the routing table and then enter **n**.
7. Set the date and time and then enter **n**.

After you install and configure the SecurePlatform operating system on an open server, install the Check Point products for Security Management Server and Security Gateway.

When you complete this procedure, IP forwarding is automatically disabled on the Security Gateway. A default security policy is enforced. This policy blocks all inbound connections, except for control connections. This policy is used until you install a new security policy.

To install products on a standalone SecurePlatform computer:

1. To import a product configuration file from a TFTP server, enter **1** and do the on-screen instructions. Otherwise, enter **n** to continue.
2. In the **Welcome** window, enter **n** to continue.
3. Enter **y** to accept the End User License agreement.
4. Do one of these actions:
 - New product installation - Select **New Installation** and then enter **n**.
 - Use the imported installation file - Select **Installation Using Imported Configuration** and then enter **n**.
5. Select the Check Point Security Gateway and Security Management server Software Blades to install, and enter **n**.
6. Select **Security Gateway** and **Security Management** and enter **n**.
7. Select **Primary Security Management**.
8. In the **Validation** window, enter **n**.
9. Enter **n** to enter your licenses later (recommended) using SmartUpdate or the WebUI.
10. **Optional:** Enter **y** to save the certificate fingerprint to a file. Otherwise press **n**.
11. Press **Enter**.
12. Restart the computer.

Windows

You can do a clean installation of Check Point products on a Windows open server. If you have a configuration file from a supported upgrade path, you can import the configuration to the new R75.40VS installation.



Note - If the required version of Microsoft.Net framework is not installed, it is installed during installation. This can take several minutes.
If necessary, the Windows Imaging Component is installed during installation.

To install on Windows:

1. Log in to Windows using **Administrator** credentials.
2. Put the installation media in the drive.
The installation wizard starts automatically.
Click **Next**.
3. Accept the **License Agreement**
Click **Next**.
4. Select **New installation**
5. Click **Next**.
6. Select **Custom** and click **Next**.

7. Select **Security Gateway**, **Security Management** and **SmartConsole**.
8. Optional: Select **SmartEvent and Reporter Suite**.
9. Click **Next**.
10. If prompted, confirm or change the destination folder and click **Next**.
11. Select **Primary Security Management** and click **Next**.
12. Review your selections, and click **Next**.
13. Click **Finish**.
14. Restart the computer.

To install on Windows with a configuration file:

1. In the first window after the License Agreement, select **Installation using imported configuration** and click **Next**.
2. Select the path of the imported configuration file and click **Next**.
3. Select an option for obtaining the latest upgrade utilities and click **Next**.
4. Continue with step 6 above.

Installing Security Management Server

In This Section

Disk Partitions in a Gaia Clean Installation	34
Installing Security Management Server on Appliances	35
Installing Security Management Server on Open Servers	37
Installing Log Server	39

Distributed Deployment - The Security Gateway and the Security Management Server are installed on different computers.

	Item	Description
	1	Security Management Server
	2	Network connection
	3	Security Gateway
		Security Gateway component
		Security Management Server component

This section explains how to install the Security Management Server.

Disk Partitions in a Gaia Clean Installation

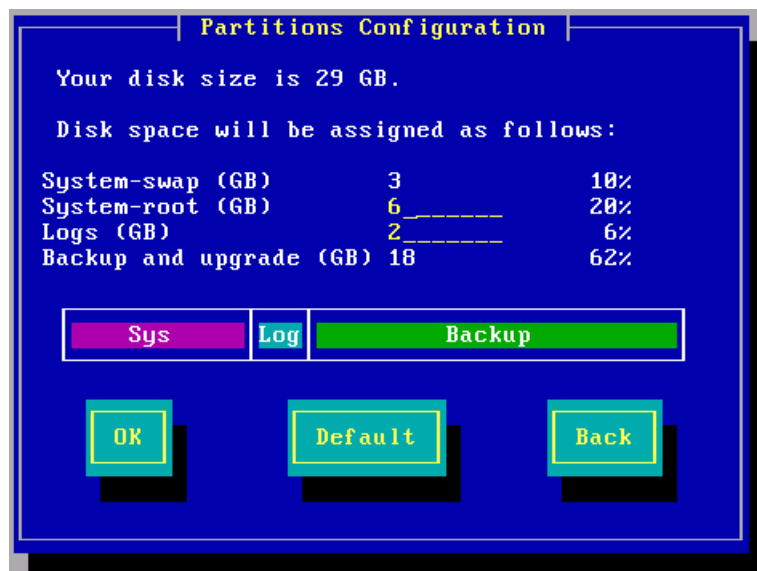
In general, Gaia disk partitions in a clean installation are larger than SecurePlatform partitions.

On an appliance, the size of the disk partitions is predefined.

When installing Gaia on an open server, these partitions have default sizes that you can change:

- System-swap
- System-root
- Logs
- Backup Images

For example:



To see the size of the system-root and log partitions on an installed system, enter `expert` mode and run the `df -h` command.

For example:

```
>df -h
Filesystem                                Size  Used Avail Used%  Mounted on
/dev/mapper/vg_splat-lv_current           13G   3.0G   9.0G   25%    /
/dev/sda1                                 145M    19M   119M   14%    /boot
tmpfs                                     187M      0   187M    0%    /dev/shm
/dev/mapper/vg_splat-lv_log                9.0G    78M   2.7G    1%    /var/log
```

In this example, the system root partition has 13G of disk space, and 9.0G is assigned for logs.

Most of the remaining space on the disk is reserved for backup images. To see the disk space assigned for backup images, connect to the Gaia WebUI and go to the **Maintenance > Image Management** page. On an Open Server, the available space shown in the **Image Management** page is less than the space you defined when installing Gaia. The difference between the two amounts is the space reserved for snapshot images that are automatically created during an upgrade. The amount of reserved space equals the size of the system-root partition.

Installing Security Management Server on Appliances

You can install a Security Management server on Smart-1 appliances. The appliance platform can be Gaia or SecurePlatform. For more about supported appliances, see the *R75.40VS Release Notes*.

Smart-1

1. Make sure that you have the correct ISO file.
2. Install the Gaia or SecurePlatform operating system on Smart-1. See instructions in *UTM-1 and 2012 Models* (on page 18).
3. **Smart-1 50 only:** Smart-1 50 appliances have two images: Security Management server and Multi-Domain Server. To select the Security Management server image:
 - a) While the appliance is restarting, open the terminal emulation program.
 - b) When prompted, press any key to enter the boot menu.
 - c) Select **Reset to factory defaults - Security Management server** and press **Enter**.
 - d) Type **yes** and press **Enter**.

The Security Management server image is selected for the appliance and then the appliance resets.

4. Install the Security Management server using the First Time Configuration Wizard.

Gaia

To install the Security Management Server on Smart-1, use the First Time Configuration Wizard.

To start the First Time Configuration Wizard:

1. Connect a standard network cable to the appliance management interface and to your management network.
The management interface is marked **MGMT**. This interface is preconfigured with the IP address 192.168.1.1.
2. Connect to the management interface from a computer on the same network subnet.
For example: IP address 192.168.1.x and net mask 255.255.255.0. This can be changed in the WebUI, after you complete the First Time Configuration Wizard.
3. To access the management interface, open a connection from a browser to the default management IP address: `https://192.168.1.1`
4. The login page opens. Log in to the system using the default username and password: `admin` and `admin`
5. Click **Login**.



Note - The features configured in the First Time Configuration Wizard are accessible after completing the wizard using the WebUI menu. The WebUI menu can be accessed by navigating to `https://<appliance_ip_address>`.

6. The **First Time Configuration Wizard** runs.

To configure Gaia Security Management on appliances:

1. In the First Time Configuration Wizard, set the password for the administrator account and then click **Next**.
2. Set the date and time (manually, or enter the hostname or IP address of the NTP server) and then click **Next**.
3. Set the **host name** for the appliance.
4. **Optional:** Set the **domain name**, and IPv4 addresses for the **DNS servers**.
You can use the Gaia WebUI to configure IPv6 DNS servers.
Click **Next**.
5. Set the IPv4 address for the management interface.
If you change the management IP address, the new IP address is assigned to the interface. The old IP address is added as an alias and is used to maintain connectivity.
6. **Optional:** Configure the appliance as a DHCP server.
Click **Next**.
7. For the appliance type, select **Smart-1 appliance** and then click **Next**.
8. In the **Products** section, make sure that **Security Management** and **Primary** are selected and then click **Next**.
9. Set the username and password for the Security Management server administrator account for SmartConsole clients and then click **Next**.
10. Define the GUI Clients that can log in to the Security Management server and then click **Next**.
11. Click **Finish** and then click OK.
12. If the **Help Check Point Improve Software Updates** window shows, click **Yes** or **No** as necessary.
Gaia R75.40VS is installed on the appliance.
13. If necessary, download SmartConsole from the Gaia WebUI.
 - a) Open a connection from a browser to the WebUI at `https://<management_ip_address>`.
 - b) In the **Overview** page, click **Download Now!**.

To configure a secondary Gaia Security Management on appliances:

Do steps 1 - 10 with these changes:

- Step 4 - Use a different IP address for the management interface on the secondary appliance. Make sure that the primary and secondary appliances are on the same subnet.
- Step 7 - Make sure that **Security Management** and **Secondary** are selected.
- Define the Secure Internal Communication (SIC) **Activation Key** that is used by the gateway object in SmartDashboard and then click **Next**.

This key is necessary to configure the appliances in SmartDashboard.

SecurePlatform

To install the Security Management Server on Smart-1 appliances, use the First Time Configuration Wizard.

To start the First Time Configuration Wizard:

1. Connect a standard network cable to the appliance management interface and to your management network.
The management interface is marked **MGMT**.
2. Open Internet Explorer to the default management IP address, `https://192.168.1.1:4434`
3. Log in to the system using the default login name/password: **admin/admin**.



Note - You can use the WebUI menu to configure the appliance settings. Navigate to `https://<appliance_ip_address>:4434`.

4. Set the username and password for the administrator account.
5. Click **Save and Login**.

The First Time Configuration Wizard opens.

To configure a SecurePlatform R75.40VS Security Management configuration:

1. In the First Time Configuration Wizard, set the date and time and then click **Next**.
 2. Configure the settings for the management and other interfaces and then click **Next**.
 3. Configure the settings for the routing table and then click **Next**.
 4. Set the **host name**, **domain name**, and **DNS servers** and then click **Next**.
 5. For Security Management installation type, select **Primary Security Management** and then click **Next**.
 6. Set the clients that can manage the appliance using a web or SSH connection and then click **Next**.
 7. **Optional:** Download SmartConsole and then click **Next**.
- The **Summary** window shows the settings for the appliance.

8. Click **Finish**.

SecurePlatform R75.40VS is installed on the appliance.

To configure a secondary SecurePlatform Security Management on appliances:

Do steps 1 - 8 above with these changes:

- Step 2 - Use a different IP address for the management interface on the secondary appliance. Make sure that the primary and secondary appliances are on the same subnet.
- Step 5 - Select **Secondary Security Management**.
- Define the Secure Internal Communication (SIC) **Activation Key** that is used by the gateway object in SmartDashboard and then click **Next**.

This key is necessary to configure the appliances in SmartDashboard.

Installing Security Management Server on Open Servers

A Security Management server can be installed on any computer that meets the minimum requirements (see the *Release Notes*). For Gaia and SecurePlatform, first install and configure the operating system. Then install Check Point products. You can also install on Windows.

Gaia

This procedure explains how to install a Security Management Server in a distributed deployment after you install the operating system ("[Gaia](#)" on page [30](#)).

To configure a Security Management Server on Gaia:

1. Using your Web browser, go the WebUI:
`https://<Gaia management IP address>`
2. In the **Gaia Portal** window, log in using the administrator name and password that you defined during the installation procedure.
3. The WebUI shows the **First Time Configuration Wizard**. Click **Next**.
4. Set the date and time (manually, or enter the hostname or IP address of the NTP server) and then click **Next**.
5. Set the **host name** for the appliance.
6. **Optional:** Set the **domain name**, and IPv4 addresses for the **DNS servers**.
You can use the Gaia WebUI to configure IPv6 DNS servers.
Click **Next**.
7. Set the IPv4 address for the management interface.
If you change the management IP address, the new IP address is assigned to the interface. The old IP address is added as an alias and is used to maintain connectivity.
8. **Optional:** Configure the appliance as a DHCP server.

Click **Next**.

9. Set the username and password for the Security Management server administrator account and then click **Next**.
10. Select **Security Management** and then click **Next**.
11. Define the GUI Clients that can log in to the Security Management server and then click **Next**.
12. Click **Finish** and then click OK.
13. If the **Help Check Point Improve Software Updates** window shows, click **Yes** or **No** as necessary.
14. If necessary, download SmartConsole from the Gaia WebUI.
 - a) Open a connection from a browser to the WebUI at `https://<management_ip_address>`.
 - b) In the **Overview** page, click **Download Now!**.

SecurePlatform

This procedure explains how to install a Security Management Server in a distributed deployment when you install the operating system ("[SecurePlatform](#)" on page 31).

To install Security Management Server on SecurePlatform:

1. To import a product configuration file from a TFTP server, enter **1** and do the instructions on the screen. Otherwise, enter **n** to continue.
2. In the **Welcome** window, enter **n** to continue.
3. Enter **y** to accept the End User License agreement.
4. Do one of these actions:
 - New product installation - Select **New Installation** and then enter **n**.
 - Use the imported installation file - Select **Installation Using Imported Configuration** and then enter **n**.
5. Select the Check Point management Software Blade to install, and enter **n**.
6. In the **SmartEvent** window, select the components to install and enter **n**.
7. Enter **n** to enter your licenses later (recommended) using SmartUpdate or the WebUI.
8. Do the on-screen instructions to add administrators and GUI clients.
9. Press **Enter**.
10. Restart the computer.

Windows

You can do a clean installation of Security Management Server on a Windows open server. If you have a configuration file from a supported upgrade path, you can import the configuration to the new R75.40VS installation.



Note - If the required version of Microsoft.Net framework is not installed, it is installed during installation. This can take several minutes.
If necessary, the Windows Imaging Component is installed during installation.

To install on Windows:

1. Log in to Windows using **Administrator** credentials.
2. Put the installation media in the drive.
The installation wizard starts automatically.
Click **Next**.
3. Accept the **License Agreement**
Click **Next**.
4. Select **New installation**
5. Click **Next**.
6. Select **Custom** and click **Next**.
7. Select **Security Management** and **SmartConsole**.
8. Optional: Select **SmartEvent and Reporter Suite**.

9. Click **Next**.
10. If prompted, confirm or change the destination folder and click **Next**.
11. Select **Primary** or **Secondary Security Management** as applicable. Click **Next**.
12. Review your selections, and click **Next**.
13. Click **Finish**.
14. When prompted, restart the computer.

To install on Windows with a configuration file:

1. In the first window after the License Agreement, select **Installation using imported configuration** and click **Next**.
2. Select the path of the imported configuration file and click **Next**.
3. Select an option for obtaining the latest upgrade utilities and click **Next**.
4. Continue with step 6 above.

Installing Log Server

You can install a log server for a distributed deployment. Install the operating system and start to install the products as for a Security Management server, but stop at the step where you select components.

To install a Log Server:

Do the steps for installing a Security Management Server ("[Windows](#)" on page [32](#)) with these changes:

- In step 7, select **Security Management**.
- In step 8, do not select **SmartEvent and Reporter Suite**.
- In step 11, select **Log Server**.

Installing Security Gateway

In This Section

Installing Security Gateway on Appliances	40
Installing Security Gateway on Open Servers	42
Installing VSX Gateways	44
Converting Gateways to VSX Gateways	44

Distributed Deployment - The Security Gateway and the Security Management Server are installed on different computers.

	Item	Description
	1	Security Management Server
	2	Network connection
	3	Security Gateway
		Security Gateway component
		Security Management Server component

This section explains how to install the Security Gateway.

Installing Security Gateway on Appliances

You can install a Security Gateway on UTM-1 appliances, Power-1 appliances, certain 2012 Models, and IP appliances. The appliance operating system can be Gaia or SecurePlatform. For more about supported appliances, see the *R75.40VS Release Notes*.

UTM-1, Power-1, and 2012 Models

After you install the Gaia or SecurePlatform operating system ("[UTM-1 and 2012 Models](#)" on page 18), install the Security Gateway.

Gaia

To install the Security Gateway on Gaia appliances, use the First Time Configuration Wizard.



Note - The internal interface (INT) on a UTM-1 appliance is used as the management interface.

To start the First Time Configuration Wizard:

1. Connect a standard network cable to the appliance management interface and to your management network.
The management interface is marked **MGMT**. This interface is preconfigured with the IP address 192.168.1.1.
2. Connect to the management interface from a computer on the same network subnet.
For example: IP address 192.168.1.x and net mask 255.255.255.0. This can be changed in the WebUI, after you complete the First Time Configuration Wizard.
3. To access the management interface, open a connection from a browser to the default management IP address: `https://192.168.1.1`
4. The login page opens. Log in to the system using the default username and password: `admin` and `admin`
5. Click **Login**.



Note - The features configured in the First Time Configuration Wizard are accessible after completing the wizard using the WebUI menu. The WebUI menu can be accessed by navigating to `https://<appliance_ip_address>`.

6. The **First Time Configuration Wizard** runs.

To configure Gaia Security Gateway appliances:

1. In the First Time Configuration Wizard, set the username and password for the administrator account and then click **Next**.
2. Set the date and time (manually, or enter the hostname or IP address of the NTP server) and then click **Next**.
3. Set the **host name** for the appliance.
4. **Optional:** Set the **domain name**, and IPv4 addresses for the **DNS servers**.
You can use the Gaia WebUI to configure IPv6 DNS servers.
Click **Next**.
5. Set the IPv4 address for the management interface.
If you change the management IP address, the new IP address is assigned to the interface. The old IP address is added as an alias and is used to maintain connectivity.
6. **Optional:** Configure the appliance as a DHCP server.
Click **Next**.
7. Select **Security Gateway** and then click **Next**.
8. Define the Secure Internal Communication (SIC) **Activation Key** that is used by the gateway object in SmartDashboard and then click **Next**.
The **Summary** window shows the settings for the appliance.
9. Click **Finish**.
Gaia R75.40VS is installed on the appliance.

SecurePlatform

To install the Security Gateway on SecurePlatform appliances, use the First Time Configuration Wizard.



Note - The internal interface (INT) on a UTM-1 appliance is used as the management interface.

To start the First Time Configuration Wizard:

1. Connect a standard network cable to the appliance management interface and to your management network.
The management interface is marked **MGMT**.
2. Open Internet Explorer to the default management IP address, `https://192.168.1.1:4434`
3. Log in to the system using the default login name/password: **admin/admin**.



Note - You can use the WebUI menu to configure the appliance settings. Navigate to `https://<appliance_ip_address>:4434`.

4. Set the username and password for the administrator account.
5. Click **Save and Login**.
The First Time Configuration Wizard opens.

To configure a Security Gateway on SecurePlatform appliance:

1. In the First Time Configuration Wizard, set the date and time and then click **Next**.
2. Configure the settings for the management and other interfaces and then click **Next**.
3. Configure the settings for the routing table and then click **Next**.
4. Set the **host name**, **domain name**, and **DNS servers** and then click **Next**.
5. Select **Centrally Managed** and then click **Next**.
6. Set the clients that can manage the appliance using a web or SSH connection and then click **Next**.
7. Select the type of gateway for the appliance and then click **Next**.

8. Define the Secure Internal Communication (SIC) **Activation Key** that is used by the gateway object in SmartDashboard and then click **Next**.
9. Click **Finish**.
SecurePlatform R75.40VS is installed on the appliance.

IP Appliances

Gaia

You can install the Gaia operating system and Check Point Security Gateway on IP appliances.

This is a clean installation. The IPSO and Check Point product configurations are not imported into Gaia.

To install, do the procedure for installing Gaia operating system and Check Point Standalone on IP appliances ("[Gaia](#)" on page 20). The only difference between the procedures is when running the First Time Configuration Wizard ("[Step 10: Selecting Check Point Products](#)" on page 28). When choosing the products to install, select **Security Gateway**. Do *not* select **Security Management**.

Installing Security Gateway on Open Servers

A Security Gateway can be installed on any computer that meets the minimum requirements (see the *Release Notes*). For Gaia and SecurePlatform, first install and configure the operating system. Then install Check Point products. You can also install on Windows.

Gaia

This procedure explains how to install a Security Gateway in a distributed deployment after you install the operating system ("[Gaia](#)" on page 30).

To configure a Security Gateway on Gaia:

1. Using your Web browser, go to the WebUI:
`https://<Gaia management IP address>`
2. In the Gaia Portal window, log in using the administrator name and password that you defined during the installation procedure.
3. The WebUI shows the First Time Configuration Wizard. Click **Next**.
4. Set the date and time and then click **Next**.
5. Set the **host name**, **domain name**, and **DNS servers** for IPv4 addresses and then click **Next**.
6. Make sure that the IPv4 address for the management interface is correct.
7. **Optional:** Configure the appliance as a DHCP server.
Click **Next**.
8. Select **Security Gateway**.
9. **Optional:** Configure these settings if the Security Gateway is a cluster member:
 - Select **Unit is part of a cluster**
 - Select **Cluster XL** or **VRRP** as applicable.
 - Select **Primary** or **Secondary** as applicable.Click **Next**.
10. Define the Secure Internal Communication (SIC) **Activation Key** that is used by the gateway object in SmartDashboard and then click **Next**.
The Summary window shows the settings for the appliance.
11. Click **Finish**.
Gaia R75.40VS is installed on the computer.

SecurePlatform

This procedure explains how to install a Security Gateway in a distributed deployment when you install the operating system ("[SecurePlatform](#)" on page 31).

When you complete this procedure, IP forwarding is automatically disabled on the Security Gateway. A default security policy is enforced. This policy blocks all inbound connections, except for control connections. This policy is used until you install a new security policy.

To install products on a standalone SecurePlatform computer:

1. To import a product configuration file from a TFTP server, enter **1** and do the instructions on the screen. Otherwise, enter **n** to continue.
2. In the **Welcome** window, enter **n** to continue.
3. Enter **y** to accept the End User License agreement.
4. Do one of these actions:
 - New product installation - Select **New Installation** and then enter **n**.
 - Use the imported installation file - Select **Installation Using Imported Configuration** and then enter **n**.
5. Select the Check Point Security Gateway Software Blade to install, and enter **n**.
6. Enter **n** to enter your licenses later (recommended) using SmartUpdate or the WebUI.
7. Press **Enter**.
8. Restart the computer.

Windows

You can do a clean installation of Check Point products on a Windows open server. If you have a configuration file from a supported upgrade path, you can import the configuration to the new R75.40VS installation.



Note - If the required version of Microsoft.Net framework is not installed, it is installed during installation. This can take several minutes.
If necessary, the Windows Imaging Component is installed during installation.

To install on Windows:

1. Log in to Windows using **Administrator** credentials.
2. Put the installation media in the drive.
The installation wizard starts automatically.
Click **Next**.
3. Accept the **License Agreement**
Click **Next**.
4. Select **New installation**
5. Click **Next**.
6. Select **Custom** and then click **Next**.
7. Select Security Gateway and clear all other options. Click **Next** to continue.
8. If prompted, confirm or change the destination folder and then click **Next**.
9. Click **Next**.
10. Click **Finish**.
11. In the **Licenses and Contracts** screen, you can add a license now or use the trial period license. Make your selection and then click **Next**.
12. In the **Clustering** window, specify whether or not this Security Gateway is cluster member. Click **Next** to continue.
13. In the **Secure Internal Communication** window, enter and confirm the activation key.
14. Click **Finish**.
15. Restart the computer.

To install on Windows with a configuration file:

1. In the first window after the License Agreement, select **Installation using imported configuration** and click **Next**.
2. Select the path of the imported configuration file and click **Next**.
3. Select an option for obtaining the latest upgrade utilities and click **Next**.
4. Continue with step 6 above.

Installing VSX Gateways

A VSX Gateway can be installed on certain Check Point appliances. You can also install it on any computer that meets the minimum requirements (see the *Release Notes*). Install and configure the Gaia operating system for a Security Gateway. Then install Check Point products and use SmartDashboard to change the Security Gateway to a VSX Gateway. The Security Gateway becomes virtual (VSX) when the VSX object is defined in SmartDashboard. The basic installation procedure for a Security Gateway and a VSX Gateway is the same.

For VSX Gateways on a Crossbeam platform, you must convert the gateway to VSX before you create the VSX object in SmartDashboard. For more about converting to VSX on a Crossbeam platform, see the *Crossbeam Administration Guide*.

To install a VSX Gateway:

1. Install and configure the R75.40VS ISO file on the VSX Gateway.
The steps are different if the VSX Gateway is on an appliance ("Gaia" on page 40) or an Open Server ("Gaia" on page 42).
In the **Products** window, make sure to only select **Security Gateway**.
2. For a VSX Gateway on a Crossbeam platform, convert the gateway to VSX.
3. Open SmartDashboard.
4. From the **Network Objects** tree, right-click **Check Point** and select **VSX > Gateway**.
5. Do the on-screen instructions.
6. Install the necessary licenses on the VSX Gateway.

Converting Gateways to VSX Gateways

Use the VSX Gateway Conversion wizard in SmartDashboard to convert Gaia Security Gateways to VSX Gateways. You can convert one Security Gateway or all the members of a cluster to VSX. The settings of the Security Gateways are applied to the VSX Gateway (VS0). You can also use SmartDashboard to convert a VSX Gateway to a Security Gateway.

We recommend that you go to sk79260 (<http://supportcontent.checkpoint.com/solutions?id=sk79260>), before you use the Conversion wizard. You can only convert Security Gateways or clusters that use the Gaia operating system.



Note - The Security Gateway loses connectivity during the conversion process.

Converting a Security Gateway

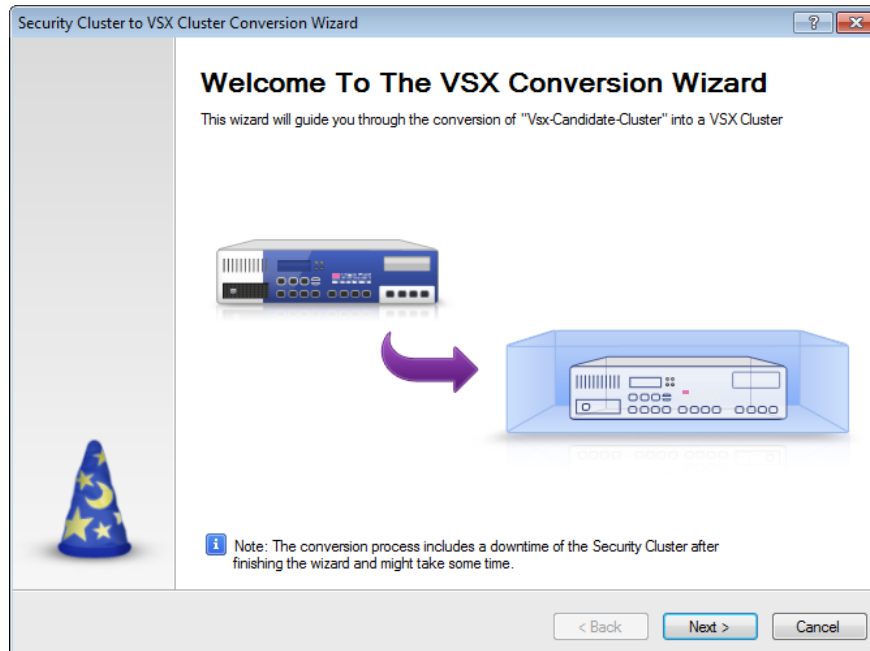
SmartDashboard converts a Security Gateway or cluster to VSX. You can only complete the Conversion Wizard if the features and settings of the Security Gateway or cluster are compatible with VSX.

When the **Conversion Process** window is shown, you cannot cancel or close the Conversion Wizard.

To convert a Security Gateway:

1. Open SmartDashboard.
2. In the **Network Objects** tree, right-click the Security Gateway or cluster and select **Convert to VSX**.

- When the **Welcome to the VSX Conversion** window opens, click **Next** to continue.



- In the **Compatibility Check** window, click **Next to continue**.
The compatibility check makes sure that the Security Gateway or cluster is compatible with VSX.
- In the **Security Management Server Interface Sharing** window, configure how interfaces are created for the new Virtual Systems and then click **Convert**.
- After the conversion process completes, click **Finish**.
The **Converting** window shows as the management database is updated.



Note - You cannot use SmartDashboard while the **Converting** window shows.

Checking Compatibility

The VSX Gateway Conversion Wizard cannot convert a Security Gateway or cluster that uses Software Blades or other features that VSX does not support. The wizard automatically checks for common compatibility problems with the Security Gateway. We recommend that you go to sk79260 (<http://supportcontent.checkpoint.com/solutions?id=sk79260>), to see a full list of limitations and compatibility problems.

If the Security Gateway is not compatible, the **Compatibility Check** window tells you the solution for each compatibility problem. Close the wizard, disable the unsupported features, and run the VSX Gateway Conversion Wizard again.

Completing the Conversion

Complete the Security Gateway to VSX Gateway Conversion Wizard. When you complete the wizard, the management database is updated with the new VSX Gateway object.

To complete the Conversion Wizard:

Click **Finish**. The **Converting** window is shown as the management database is updated.



Note - You cannot use SmartDashboard while the **Converting** window is shown.

Converting a VSX Gateway

SmartDashboard converts a VSX Gateway or cluster to a Security Gateway. You must remove all the Virtual Systems and other virtual devices from the VSX object before you can convert the VSX Gateway.

You cannot convert a VSX Gateway that uses a shared interface configuration to a Security Gateway.

To convert a VSX Gateway to a Security Gateway:

1. Remove all the virtual devices from the VSX object.
From the **Network Objects** tree, right-click each virtual device object and select **Delete**.
2. Right-click the VSX Gateway or cluster and select **Convert to Gateway**.
A confirmation window opens.
3. Click **Yes**.
The VSX Gateway is converted to a Security Gateway.



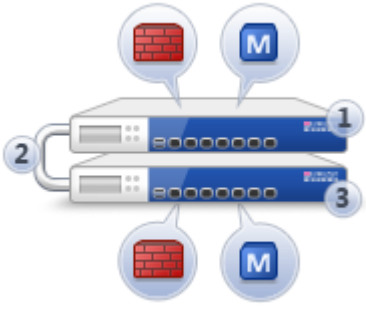


Note - You cannot use SmartDashboard while the **Converting** window is shown.

Installing Full High Availability Appliances

In This Section

Gaia Appliances	47
SecurePlatform Appliances	49
Configuring Standalone Full High Availability	50

Standalone Full HA - Security Management server and Security Gateway are each installed on one appliance, and two appliances work in High Availability mode. One is active, and one is standby.

	Item	Description
	1	Primary appliance
	2	Direct appliance to appliance connection
	3	Backup appliance
		Security Gateway component
		Security Management Server component

- If the active member has a failure that affects the Security Management server and the Security Gateway, they failover to the standby.
- If the Security Management server on the active member experiences a failure, only the Security Management server fails over to the standby. The Security Gateway on the first member continues to function.
- If the Security Gateway on the active member experiences a failure, only the Security Gateway fails over to the standby. The Security Management server on the first member continues to function.

After you install the Gaia or SecurePlatform operating system ("[UTM-1 and 2012 Models](#)" on page 18), configure Standalone Full HA. First, configure each of the two standalone appliances with its First Time Configuration Wizard. Then configure the High Availability options in SmartDashboard.

Gaia Appliances

Some appliances have a dedicated SYNC interface that is used to synchronize with the other appliance. If there is no SYNC interface on the appliance, use the ETH1 interface.



Note - The internal interface (INT) on a UTM-1 appliance is used as the management interface.

To start the First Time Configuration Wizard:

1. Connect a standard network cable to the appliance management interface and to your management network.
The management interface is marked **MGMT**. This interface is preconfigured with the IP address 192.168.1.1.
2. Connect to the management interface from a computer on the same network subnet.
For example: IP address 192.168.1.x and net mask 255.255.255.0. This can be changed in the WebUI, after you complete the First Time Configuration Wizard.
3. To access the management interface, open a connection from a browser to the default management IP address: <https://192.168.1.1>
4. The login page opens. Log in to the system using the default username and password: `admin` and `admin`
5. Click **Login**.



Note - The features configured in the First Time Configuration Wizard are accessible after completing the wizard using the WebUI menu. The WebUI menu can be accessed by navigating to `https://<appliance_ip_address>`.

6. The **First Time Configuration Wizard** runs.

To configure Gaia Full HA appliances:

1. In the First Time Configuration Wizard, set the username and password for the administrator account and then click **Next**.
2. Set the date and time (manually, or enter the hostname or IP address of the NTP server) and then click **Next**.
3. Set the **host name** for the appliance.
4. **Optional:** Set the **domain name**, and IPv4 addresses for the **DNS servers**.
You can use the Gaia WebUI to configure IPv6 DNS servers.
Click **Next**.
5. Set the IPv4 address for the management interface.
If you change the management IP address, the new IP address is assigned to the interface. The old IP address is added as an alias and is used to maintain connectivity.
6. **Optional:** Configure the appliance as a DHCP server.
Click **Next**.
7. Select **Security Gateway** and **Security Management**.
8. Configure these **Advanced** settings:
 - Select **Unit is part of a cluster**
 - Select **Cluster XL**
 - Select **Primary**
 Click **Next**.
9. Set the username and password for the Security Management server administrator account and then click **Next**.
10. Define the GUI Clients that can log in to the Security Management server and then click **Next**.
11. Click **Finish** and then click OK.
12. If the **Help Check Point Improve Software Updates** window shows, click **Yes** or **No** as necessary.
Gaia R75.40VS is installed on the appliance.
13. Log in to the Gaia WebUI with the new management IP address that you entered in the First Time Configuration Wizard.
14. Double-click the **SYNC** or **eth1** interface and configure the settings. This interface is used to synchronize with the other appliance. Click **Apply**.
15. Configure the settings for other interfaces that you are using.
16. Use a cross-over cable to connect the **SYNC** or **eth1** interfaces on the appliances.
17. Do steps 1 - 15 again for the secondary appliance, with these changes:
 - Step 5 - It is not necessary to change the management IP address.
 - Step 7 - Select **Secondary**.
 - Define the Secure Internal Communication (SIC) **Activation Key** that is used by the gateway object in SmartDashboard and then click **Next**.
This key is necessary to configure the appliances in SmartDashboard.
 - Step 14 - Use a different IP address for the **SYNC** or **eth1** interface on the secondary appliance. Make sure that the primary and secondary appliances are on the same subnet.
18. If necessary, download SmartConsole from the Gaia WebUI.
 - a) Open a connection from a browser to the WebUI at `https://<management_ip_address>`.
 - b) In the **Overview** page, click **Download Now!**.

SecurePlatform Appliances

Some appliances have a dedicated SYNC interface that is used to synchronize with the other appliance. If there is no SYNC interface on the appliance, use the ETH1 interface.



Note - The internal interface (INT) on a UTM-1 appliance is used as the management interface.

To start the First Time Configuration Wizard:

1. Connect a standard network cable to the appliance management interface and to your management network.
The management interface is marked **MGMT**.
2. Open Internet Explorer to the default management IP address, <https://192.168.1.1:4434>
3. Log in to the system using the default login name/password: **admin/admin**.



Note - You can use the WebUI menu to configure the appliance settings. Navigate to https://<appliance_ip_address>:4434.

4. Set the username and password for the administrator account.
5. Click **Save and Login**.

The First Time Configuration Wizard opens.

To configure Full High Availability:

1. In the First Time Configuration Wizard, set the date and time and then click **Next**.
2. Configure the settings for the network connections.
 - a) Click the **Mgmt** interface and configure the settings and then click **Apply**.
 - b) Click the **SYNC** or **eth1** interface and configure the settings and then click **Apply**. This interface is used to synchronize with the other appliance.
 - c) Configure the settings for other interfaces that you are using.

Click **Next**.

3. Configure the settings for the routing table and then click **Next**.
4. Set the **host name** (required), **domain name** (optional), and **DNS servers** (optional) and then click **Next**.
5. Select **Locally Managed** and then click **Next**.
6. Configure the appliance as the primary cluster member.
 - a) Select **This appliance is part of a Check Point Cluster**.
 - b) Select **Primary cluster member**.

Click **Next**.

7. Set the clients that can manage the appliance using a web or SSH connection and then click **Next**.
8. **Optional:** Download SmartConsole and then click **Next**.
The **Summary** window shows the settings for the appliance.
9. Click **Finish**.

SecurePlatform R75.40VS is installed on the primary appliance.

10. Use a cross-over cable to connect the **SYNC** or **eth1** interfaces on the appliances.
11. Do steps 1 - 9 again for the secondary appliance, with these changes:
 - Step 2b - Use a different IP address for the **SYNC** or **eth1** interface on the secondary appliance. Make sure that the primary and secondary appliances are on the same subnet.
 - Step 6b - Select **Secondary cluster member**.
 - Define the Secure Internal Communication (SIC) **Activation Key** that is used by the gateway object in SmartDashboard and then click **Next**.

This key is necessary to configure the appliances in SmartDashboard.

Configuring Standalone Full High Availability

After you set up the appliances for Standalone Full High Availability, configure this deployment in SmartDashboard. You must configure both cluster members before you open the cluster configuration wizard in SmartDashboard.

The LAN1 interface serves as the SYNC interface between cluster members. If not configured, SYNC interfaces are automatically set to 10.231.149.1 and 10.231.149.2. If these addresses are already in use, their values can be manually adjusted. If you manually adjust the default IP SYNC addresses, verify that both reside on the same subnet.



Note - All interfaces in the cluster must have unique IP addresses. If the same IP address is used twice, policy installation will fail. A Load on gateway failed error message is displayed.

The cluster has a unique IP address, visible to the internal network. The unique Virtual IP address makes the cluster visible to the external network, and populates the network routing tables. Each member interface also has a unique IP address, for internal communication between the cluster members. These IP addresses are not in the routing tables.

To configure Standalone Full High Availability:

1. Open SmartDashboard.
2. Connect to the primary appliance and then click **Approve** to accept the fingerprint as valid.
The **Security Cluster wizard** opens.
Click **Next**.
3. Enter the name of the Standalone Full High Availability configuration and then click **Next**.
4. Configure the settings for the secondary appliance.
 - a) In **Secondary Member Name**, enter the hostname.
 - b) In **Secondary Member Name IP Address**, enter the IP address of the management interface.
 - c) Enter and confirm the SIC activation key.
 Click **Next**.
5. Configure the IP address of the paired interfaces on the appliances. Select one of these options:
 - **Cluster Interface with Virtual IP** - Enter a virtual IP address for the interface.
 - **Cluster Sync Interface** - Configure the interface as the synchronization interface for the appliances.
 - **Non-Cluster Interface** - Use the configured IP address of this interface.
 Click **Next**.
6. Do step 5 again for all the interfaces.
7. Click **Finish**.

Removing a Cluster Member

You can remove one of the two members of a cluster without deleting the cluster object. A cluster object can have only a primary member, as a placeholder, while you do maintenance on an appliance. You must remove the cluster member in the WebUI and in the CLI.

To remove a cluster member:

1. Open the **WebUI** of the member to keep.
2. Open **Product Configuration > Cluster**.
3. Click **Remove Peer**.
 - If the current member is the primary member, the secondary member is deleted.
 - If the current member is the secondary member, the secondary member is promoted to primary. Then the peer is deleted.
 Services running on the appliance are restarted.
4. On the appliance command line, run: `cp_conf fullha disable`
This command changes back the primary cluster member to a standalone configuration.
5. Reboot.

The former cluster object is now a locally managed gateway and Security Management server.

Adding a New Appliance to a High Availability Cluster

You can add a standalone appliance to a cluster, after the High Availability cluster is defined. You can change which member is primary.

To add an existing appliance to a cluster:

1. Open the WebUI of the appliance.
2. On the **Product Configuration, Cluster** page, select **Make this Appliance the primary member of a High Availability Cluster**.
3. Click **Apply**.
4. Reboot the appliance.
5. In SmartDashboard, open the object of the primary member.
The first-time cluster configuration wizard opens.
6. Complete the wizard to configure the secondary cluster member.

Troubleshooting network objects:

In SmartDashboard, the network object of the standalone appliance is converted to a cluster object. If the standalone appliance was in the Install On column of a rule, or in the Gateways list of an IPSec VPN community, the cluster object is updated automatically. *For all other uses, you must manually change the standalone object to the cluster object.* These changes can affect policies.

To see objects and rules that use the object to change:

1. Right-click the standalone object and select **Where Used**.
2. Select a line and click **Go To**.
3. In the window that opens, replace the standalone object with the cluster object.
If the **Where Used** line is a:
 - **Host, Network, Group** - Browse through the pages of the properties window that opens, until you find the object to change.
 - **Policy** (for example, **dlp_policy**) - Open the Gateways page of the Software Blade. Remove the standalone object. Add the cluster object.
4. In **Where Used > Active Policies**, see the rules that use the standalone object.
5. Select each rule and click **Go To**.
6. Edit those rules to use the cluster object.



Note - The icon in SmartDashboard changes to show new status of the appliance as a primary cluster member. The **Name** and **UID** of the object in the database stay the same.

Recommended Logging Options for High Availability

In High Availability, log files are not synchronized between the two cluster members. For this reason, we recommend that you configure the logs of the cluster.

To forward cluster logs to an external log server:

1. Open the properties of the cluster object.
2. Open **Logs > Additional Logging**.
3. Click **Forward log files to Log Server**, and select the Log Server ("[Installing Log Server](#)" on page 39).
4. Select or define a time object for **Log forwarding schedule**.

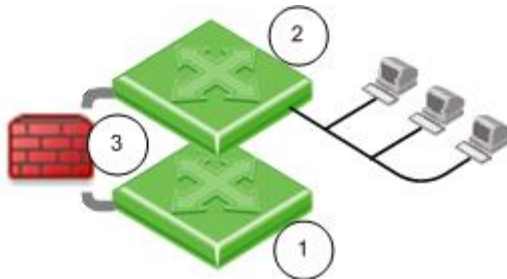
Or:

Configure SmartEvent and SmartReporter with standard reports, to use only one of the cluster members as a source for log file correlation and consolidation.

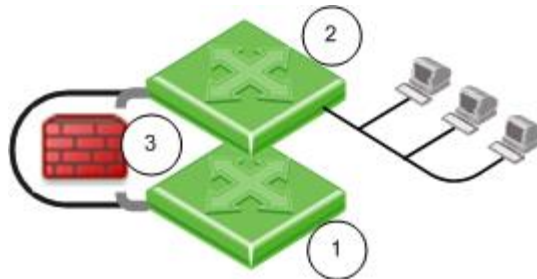
Deploying Bridge Mode Security Gateways

If you install a new Security Gateway in a network and cannot change the IP routing scheme, use bridge mode. A Security Gateway in bridge mode is invisible to Layer-3 traffic. When authorized traffic arrives, the Security Gateway passes it to the next interface through bridging. This creates a Layer-2 relationship between two or more interfaces. Traffic that enters one interface exits the other interface. Bridging lets the Security Gateway inspect and forward traffic, without the original IP routing.

Before



After



Item	Description
1	Switch 1
2	Switch 2
3 before	Connection between switches, one IP address.
3 after	Security Gateway Firewall bridging Layer-2 traffic over the one IP address, with a subnet on each side using the same address.

Before configuring the bridge, install the Security Gateway ("[Installing Security Gateway](#)" on page 40).

To manage the gateway in bridge mode, it must have a separate, routed IP address. You must configure the bridged interfaces.

Gaia

You can configure bridge mode in the Gaia WebUI or the CLI.

To configure a bridge interface in the WebUI:

1. In the WebUI navigation tree, select **Network Interfaces**.
2. Click **Add > Bridge**, or select an interface and click **Edit**.
The **Add (or Edit) Bridge** window opens.
3. On the **Bridge** tab, enter or select a **Bridge Group ID** (unique integer between 1 and 1024).
4. Select the interfaces from the **Available Interfaces** list and then click **Add**.
5. Click the **IPv4** or **IPv6** tabs, and then enter the IP addresses and subnet.
Or click **Obtain IP Address automatically**.
6. Click **OK**.

To configure a bridge interface with the CLI:

1. Run: `add bridging group <Group Name> interface <physical interface name>`
2. Run again for each interface in the bridge.
3. Run: `save config`
4. Add a bridge interface IP address:
 - IPv4: `set interface <Group Name> ipv4-address <IP> subnet-mask <Mask>`
 - IPv6: `set interface <Group Name> ipv6-address <IP> mask-length <Prefix>`
5. Run: `save config`

SecurePlatform

You can configure bridge mode in the SecurePlatform WebUI or the CLI.

To configure a bridge interface in the SecurePlatform WebUI:

1. Connect to the management interface of the Security Gateway.
2. Select **Network > Connections > New > Bridge**.
3. Select the two interfaces of the bridge and click **Add**.
4. Enter the **IP Address** and **Netmask** of the bridge (not the physical) interface.
5. Select **Apply**.

To configure a bridge interface in the Command Line:

1. Enter: `sysconfig`
2. Select **Network Connections > Add new connection > Bridge**.
3. Add a pair of interfaces which are not configured with an IP address to the bridge.
4. Enter: `N`
5. Enter the IP address and netmask of the bridge (not the physical) interface.

If anti-spoofing is required for the bridged interfaces, define different IP address ranges behind each bridged interface. Do not use the same network for the two interfaces, as this can cause a loss of connectivity.

To see the bridge status:

The **brctl show** command displays the status of the bridge configuration. For example:

```
[Expert@GW-1]# brctl show
```

bridge name	bridge id	STP enabled	interfaces
br0	8000.000423b93e56	no	eth0 eth1

The **interfaces** are the two bridged interfaces. The MAC address of the bridge is inherited from one of the physical interfaces.

Installing SmartConsole Clients

The SmartDashboard and other SmartConsole applications are the GUI clients to manage the Security Management server and Security Gateways.

For SmartConsole requirements, see the *R75.40VS Release Notes* (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

To install the SmartConsole clients on Windows platforms:

1. Insert the R75.40VS distribution media or download the SmartConsole application from the Support Center (<http://supportcenter.checkpoint.com>).
2. If you are using the installation media, go to the `Linux\linux\windows` folder.
3. Run the **SmartConsole** executable.
4. Continue with the instructions on the screen.

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 the **Demo** mode to experiment with different objects, views, modes and features before you create a production system. The Demo mode includes several pre-configured sample Domains, Domain Management Servers, Security Gateways and policies.

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

Logging in to SmartConsole

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.

You can create a new certificate for future logins. For more about certificates, see the *R75.40VS Security Management Administration Guide* (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

To log in to SmartConsole clients:

1. Open the SmartConsole from the **Start** menu.
2. Enter your credentials:
 - To use a password, enter the Security Management server host name or IP address. Then enter your administrator user name and password.
 - To use a certificate, enter the Security Management server host name or IP address. Then click **Certificate** and select the certificate.
 - To start without credentials, select **Demo mode**.
 - Optional: Enter a description of this session.
 - Optional: Select **Read Only**. This option lets you connect to the Security Management server while other administrators are connected. You cannot change settings in this mode.
3. Click **Login**.
4. If necessary, confirm the connection using the fingerprint generated during installation.
You see this only the first time that you log in from a client 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 makes 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.

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>)

Uninstalling R75.40VS

A command line uninstall utility, available for all platforms, performs a silent uninstallation of the release on IP appliances and Windows open servers.

To uninstall the release on SecurePlatform or Gaia appliances and computers, use the built-in Backup and Restore (see "[Backing Up](#)" on page 66) functionality.

To uninstall R75.40VS:

Platform	Procedure
Windows	<ol style="list-style-type: none">1. Open Start > Check Point > Uninstall R75.40VS2. At the prompt, enter Y to continue.
IP appliance	<ol style="list-style-type: none">1. Change directory to: <code>/opt/CPUninstall/R75.40VS/</code>2. Run: <code>./UnixUninstallScript</code>

If a package fails to uninstall, the script shows the log on screen.

Chapter 4

Installing Multi-Domain Security Management

In This Chapter

Basic Architecture	56
Setting Up Multi-Domain Security Management Networking	57
Installing Multi-Domain Server	58
Installing Gateways	61
Installing Multi-Domain Security Management GUI Clients	61
Post-Installation Configuration	61

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.

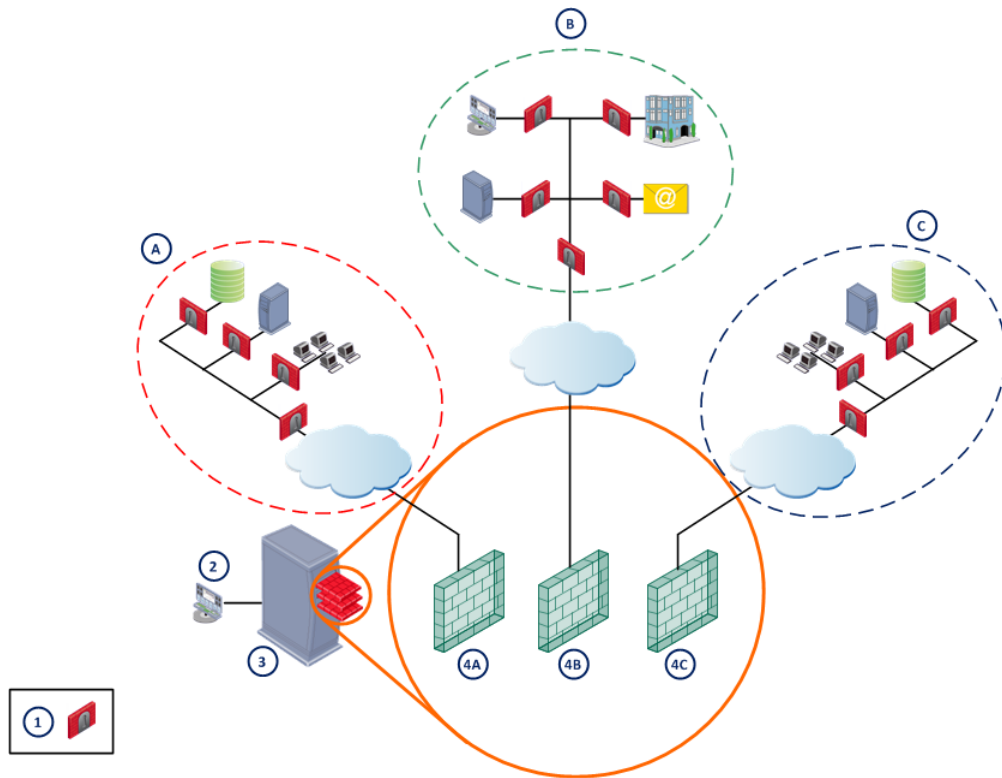
Centralized management gives administrators the flexibility to manage policies for many diverse entities. Security policies should be applicable to the requirements of different departments, business units, branches and partners, balanced with enterprise-wide requirements.

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.



List of Callouts

Callout	Description
A	USA Development Domain
B	Headquarters Domain
C	UK Development Domain
1	Security Gateway
2	Network Operation Center
3	Multi-Domain Server
4A	USA Development Domain Management Server
4B	Headquarters Domain Management Server
4C	UK Development Domain Management Server

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 Multi-Domain Server

You can install a Multi-Domain Server on certain Smart-1 appliances, or Open Servers on SecurePlatform or Gaia. For more about supported appliances and platforms, see the *R75.40VS Release Notes*.

Smart-1 Appliances

Install a Multi-Domain Server on supported Smart-1 models. Make sure that you use the Smart-1 ISO file when you install the operating system.

To install Multi-Domain Server on an appliance:

1. Install the SecurePlatform operating system on the appliance, as described for the UTM-1 and 2012 Models (on page 18).
2. While the appliance restarts, open the terminal emulation program.
3. When prompted, press any key to enter the boot menu.
4. Select **Reset to factory defaults - Multi-Domain Server** and press **Enter**.
5. Type **yes** and press **Enter**.

Multi-Domain Server is installed on the appliance and then the appliance resets.

To start the First Time Configuration Wizard:

1. Connect a standard network cable to the appliance management interface and to your management network.
The management interface is marked **MGMT**.
2. Open Internet Explorer to the default management IP address, <https://192.168.1.1:4434>
3. Log in to the system using the default login name/password: **admin/admin**.



Note - You can use the WebUI menu to configure the appliance settings. Navigate to https://<appliance_ip_address>:4434.

4. Set the username and password for the administrator account.
5. Click **Save and Login**.

The First Time Configuration Wizard opens.

To configure Multi-Domain Server R75.40VS on appliances:

1. In the First Time Configuration Wizard, set the date and time and then click **Next**.
2. Configure the settings for the management and other interfaces and then click **Next**.
3. Configure the settings for the routing table and then click **Next**.
4. Set the **host name**, **domain name**, and **DNS servers** and then click **Next**.
5. Set the clients that can manage the appliance using a web or SSH connection and then click **Next**.
6. Select **Multi-Domain Server** and then click **Next**.
7. Select **Primary Multi-Domain Server** and then click **Next**.
8. Define the Multi-Domain Server administrator that is a Multi-Domain Server Superuser and then click **Apply**.
Click **Next**.
9. **Optional:** Download SmartConsole and SmartDomain Manager and then click **Next**.
The **Summary** window shows the settings for the appliance.
10. Click **Finish**.

Multi-Domain Server R75.40VS is installed on the appliance.

To configure a secondary Multi-Domain Server R75.40VS on appliances:

Do steps 1 - 10 with these changes:

- Step 2 - Use a different IP address for the management interface on the secondary appliance. Make sure that the primary and secondary appliances are on the same subnet.
- Step 7 - Select **Secondary Multi-Domain Server**.
- Define the Secure Internal Communication (SIC) **Activation Key** that is used by the gateway object in SmartDashboard and then click **Next**.

This key is necessary to configure the appliances in SmartDashboard.

To configure a Multi-Domain Server R75.40VS log server on appliances:

Do steps 1 - 10 with these changes:

- Step 6 - Select **Multi-Domain Log Server**.
- Define the Secure Internal Communication (SIC) **Activation Key** that is used by the gateway object in SmartDashboard and then click **Next**.

This key is necessary to configure the appliances in SmartDashboard.

Converting a Security Management Server to Multi-Domain Server

The Single2Multi Domain utility lets you easily convert a Security Management server on Smart-1 50 and 150 appliances to a Multi-Domain Server.

- Security Management server is converted to a Domain Management Server with the same name and IP address.
- Security Management administrators and GUI clients that are defined using `cpconfig` are converted to Multi-Domain Superuser administrators and Superuser GUI clients.
- Security Management administrators defined in the SmartDashboard are converted to Domain Management administrators.
- Security Management High Availability server is converted to a Security Management backup server to the Domain Management Server.

Preparing to Convert

Before you run the Single2Multi Domain utility, do these steps to prepare for the conversion.

- Install SmartDomain Manager on a computer to configure the Multi-Domain Server.
- Connect to the appliance using the console port or LOM.
- Make sure that you have these details:
 - New routable IP address and netmask for the Multi-Domain Server. The new Domain Management Server uses the Security Management server IP address.
 - Name for the Multi-Domain Server that can be resolved with DNS.
 - File with the Multi-Domain Server license.

Converting the Security Management Server

Use the `s2mwrapper` command to convert the Smart-1 50 or 150 appliance to a Multi-Domain Server.

The utility lets you create a snapshot of the Security Management server during the conversion process. You can use this snapshot to revert back to the Security Management server.



Note - Before you revert back to the Security Management server, backup the Multi-Domain Server log file in the `/opt/CPInstlog` directory.

To convert the Security Management server:

1. Log in to the Smart-1 50 or 150 appliance and enter Expert mode.

2. Run `s2mwrapper`.
3. Follow the on-screen instructions.
4. Log out of the appliance.
5. Log in to SmartDomain Manager with the `cpconfig` administrator username and password.

Open Servers

Install Multi-Domain Server on a dedicated Gaia or SecurePlatform open server.

Configure the Multi-Domain Server when you install the operating system on the open server. This procedure starts after you configure the date and time in the Gaia or SecurePlatform installation.

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

- Primary Multi-Domain Server - The first Multi-Domain Server that you install and log on to.
- Secondary Multi-Domain Server
- Standalone log servers - Domain Log Server or Multi-Domain Log Servers.

To install a Primary Multi-Domain Server on SecurePlatform:

1. Use the Multi-Domain Security Management removable media or ISO file to install and configure SecurePlatform (on page 31).
2. In the Multi-Domain Security Management welcome screen, enter **yes**.
3. Select **Multi-Domain Server**.
4. Enter **yes** when prompted to install a Primary Multi-Domain Server.
You must install the **Primary Multi-Domain Server** first.
You can install a secondary Multi-Domain Server or a Multi-Domain Log Server later.
5. When prompted, enter **yes** to confirm installation of a **Primary Multi-Domain Server**.
You cannot change this installation setting later.
6. At the **Are you sure** prompt, enter **yes** to continue.
7. When prompted, press the space bar to scroll through the license agreement and then press **y**.
8. If there is more than one interface on the Multi-Domain Server, enter the interface that connects Domain Management Servers to their managed networks and gateways. This is typically the management interface.
You can only have one interface for this purpose.
9. In **Configuring Licenses**, 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.
10. In **Configuring Groups**, press **Enter** and then press **y** to assign the **root** user group by default. You can define groups later.
11. Press **Enter** to start the Certificate Authority.
12. Press **y** to save the certificate fingerprint to a file.
13. Define least one Multi-Domain Security Management administrator.
You must define the first administrator as a **Multi-Domain Security Management Superuser**. You can add this administrator to a group.
You can define more administrators, but we recommend that you use the SmartDomain Manager to do this later.
14. Enter **n** when prompted to add this administrator to an administrators group. You can do this later.
15. Define at least one GUI client (SmartDomain Manager) to manage this Multi-Domain Server.
16. When prompted, press **Enter**.
17. Restart the Multi-Domain Server.

To install a secondary Multi-Domain Server:

Do the steps in the above procedure with these exceptions:

- In step 5, enter **no** when prompted to install a Primary Multi-Domain Server.
- In step 6, do the action to confirm this choice.

To install a Multi-Domain Server log server:

Do the steps in the above procedure with these exceptions:

- In step 4, select **Multi-Domain Log Server**.
- In step 5, enter **no** when prompted to install a Primary Multi-Domain Server.
- In step 6, do the action to confirm this choice.

Installing Gateways

Install the Network Operation Center (NOC) and Security Gateways of the domain using the R75.40VS DVD ("[Installing Security Gateway](#)" on page 40).

Installing Multi-Domain Security Management GUI Clients

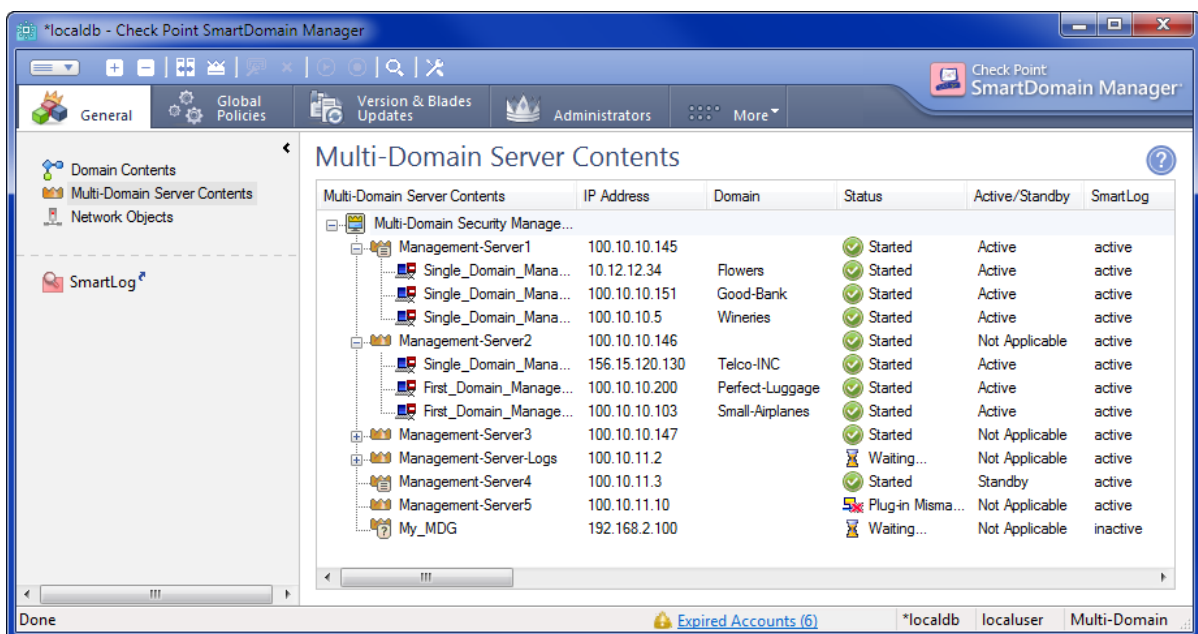
The SmartDomain Manager is automatically installed together with Check Point SmartConsole. If you have not yet installed SmartConsole, do so now.

To install the SmartConsole clients on Windows platforms:

1. Insert the R75.40VS distribution media or download the SmartConsole application from the Support Center (<http://supportcenter.checkpoint.com>).
2. If you are using the installation media, go to the `Linux\linux\windows` folder.
3. Run the **SmartConsole** executable.
4. Continue with the instructions on the screen.

Post-Installation Configuration

Use the SmartDomain Manager to configure and manage the Multi-Domain Security Management deployment. Make sure to install 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.



To start the SmartDomain Manager:

1. Click **Start > All Programs > Check Point SmartConsole R75.40VS > SmartDomain Manager**.
2. Enter your credentials:
 - To use a password, enter the Multi-Domain Server host name or IP address. Then enter your administrator user name and password.
 - To use a certificate, enter the Multi-Domain Server host name or IP address. Then click **Certificate** and select the certificate.
 - To start without credentials, select **Demo mode**.
 - Optional: Enter a description of this session.
3. Click **Login**.
SmartDomain Manager connects to the Multi-Domain Server. When SmartDomain Manager opens, it shows the network objects and options that you have permission to work with.
4. If necessary, confirm the connection using the fingerprint generated during installation.
You see this only the first time that you log in from a client computer.

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 the **Demo** mode to experiment with different objects, views, modes and features before you create a production system. The Demo mode includes several pre-configured sample Domains, Domain Management Servers, Security Gateways and policies.

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

Adding Licenses using the SmartDomain Manager

You can 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**:
 - Fetch License File**
 - a) Click **Fetch From 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.

Uninstalling Multi-Domain Security Management

To uninstall a Multi-Domain Server:

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 the SmartDomain Manager and SmartConsole applications:

- Use **Add/Remove Programs** to uninstall the clients.

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>).

Chapter 5

Upgrading Prerequisites

In This Chapter

Contract Verification	64
Upgrade Tools	65
Using the Pre-Upgrade Verifier Tool	65
Upgrading Successfully	66
Uninstalling Packages	66
Backing Up	66
Restoring a Deployment	71
Service Contract Files	74

Before you upgrade:

- For information about supported upgrade paths, see the *Release Notes*.
- Make sure that you have the latest version of this document.

For the latest R75.40VS documentation, see the *R75.40VS home page* (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

If you use Mobile Access Software Blade and you edited the configurations, review the edits before you upgrade to R75.40VS!

1. Open these files and make note of your changes.

Data	Path
Gateway Configurations	\$CVPNDIR/conf/cvpnd.C
Apache Configuration Files	\$CVPNDIR/conf/httpd.conf
	\$CVPNDIR/conf/includes/*
Local certificate authorities	\$CVPNDIR/var/ssl/ca-bundle/
DynamicID (SMS OTP) Local Phone List	\$CVPNDIR/conf/SmsPhones.lst
RSA configuration	/var/ace/sdconf.rec
Any PHP files that were edited	
Any image file that was replaced (*.gif, *.jpg)	

2. Upgrade to R75.40VS.
3. Update Endpoint Compliance (**SmartDashboard > Mobile Access > Endpoint Security On Demand > Update Databases Now**).
4. Manually edit the new versions of the files, to include your changes.
Do not overwrite the R75.40VS files with your customized files!

Contract Verification

A valid Service Contract (see "[Service Contract Files](#)" on page 74) is required for all upgrades. The installation procedure makes sure that a service contract is in force before continuing with installation.

Upgrade Tools

Before you upgrade appliances or computers, use the upgrade tools. There is a different package of tools for each platform. After installation, you can find the upgrade tools in the installation directory.

- Gaia or SecurePlatform: `$FWDIR/bin/upgrade_tools`
- Windows: `%FWDIR%/bin/upgrade_tools`

To make sure you have the latest version of the upgrade tools, you can download the appropriate package from the Check Point Support site (<http://supportcenter.checkpoint.com>).

When you open the **upgrade_tools** package, you see these files:

Package	Description
migrate.conf	For an Advanced Upgrade (migration of Security Management Server database) or a Security Management Server to Multi-Domain Server migration, this file is necessary.
migrate	Runs Advanced Upgrade or migration. On Windows, this is migrate.exe .
pre_upgrade_verifier.exe	Analyzes compatibility of the currently installed configuration with the upgrade version. It gives a report on the actions to take before and after the upgrade.
upgrade_export	Backs up all Check Point configurations, without operating system information. On Windows, this is upgrade_export.exe .
upgrade_import	Restores backed up configuration. On Windows, this is upgrade_import.exe .

Using the Pre-Upgrade Verifier Tool

The Pre-upgrade Verifier runs automatically during the upgrade process. You can also run it manually with this command.

Syntax:

```
pre_upgrade_verifier.exe -p ServerPath -c CurrentVersion (-t TargetVersion |
-i) [-f FileName] [-w]
```

Parameters:

Parameter	Description
-p	Path of the installed Security Management Server (FWDIR)
-c	Currently installed version
-t	Target version
-i	If -i is used, only the INSPECT files are analyzed, to see if they were customized.
-f	Output report to this file
-w	Output report to a web format file

Upgrading Successfully

- When upgrading a Security Management Server, IPS profiles remain in effect on earlier gateways and can be managed from the IPS tab. When the gateway is upgraded, install the policy to get the new IPS profile.
- When upgrading a Security Gateway, remember to change the gateway object in SmartDashboard to the new version.

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

Uninstalling Packages

Some upgrade procedures require an uninstall of certain packages. You must uninstall Check Point packages in the opposite order from which they were installed. For example, CPsuite is the first package installed, so it is the last package uninstalled.

To see a list of the installed packages:

- SecurePlatform: `rpm -e <package name>`
- Windows: Use the **Control Panel > Add / Remove Programs** utility

Backing Up

Before you upgrade, it is recommended to back up the Security Management Servers and Security Gateways. Use the tools appropriate for each platform.

Use the snapshot mechanism if it is available. SecurePlatform on an open server does not have snapshot, so use backup instead.

Gaia Backup

Back up the configuration of the Gaia operating system and of the Security Management server database. You can use the backup to restore a previously saved configuration. The configuration is saved to a .tgz file. You can store backups locally, or remotely to a TFTP, SCP or FTP server. You can run the backup manually, or do a scheduled backup.

For Gaia backup limitations, see sk91400 (<http://supportcontent.checkpoint.com/solutions?id=sk91400>).

Backing Up the System - WebUI

To add a backup:

1. In the tree view, click **Maintenance > System Backup**
2. Click **Add Backup**.
The **New Backup** window opens.
3. Select the location of the backup file:
 - **This appliance**
 - **TFTP server**. Specify the IP address.
 - **SCP server**. Specify the IP address, user name and password.
 - **FTP server**. Specify the IP address, user name and password.

Backing Up the System - CLI (Backup)

Backing Up a Configuration

Description Use these commands to create and save the system's configuration

Syntax

To create and save a backup locally:

```
add backup local
```

To create and save a backup on a remote server using FTP:

```
add backup ftp ip VALUE username VALUE password plain
```

To create and save a backup on a remote server using TFTP:

```
add backup tftp ip VALUE
```

To save a backup on a remote server using SCP:

```
add backup scp ip VALUE username VALUE password plain
```

Parameters

Parameter	Description
ip VALUE	The IP address of the remote server.
username VALUE	User name required to log in to the remote server.
password plain	At the prompt, enter the password for the remote server.

Example

```
add backup local
```

Output

```
gw> add backup local
Creating backup package. Use the command 'show backups' to
monitor creation progress.

gw> show backup status
Performing local backup

gw> show backups
backup_gw-8b0891_22_7_2012_14_29.tgz Sun, Jul 22, 2012 109.73
MB
```

Comments

Backup configurations are stored in: /var/CPbackup/backups/

Monitoring Backup Status

To monitor the creation of a backup:

```
show backup status
```

To show the status of the last backup performed:

```
show backups
```

Gaia Snapshot Image Management

You can:

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

Configuring Image Management - WebUI

To create an image:

1. In the tree view, click **Maintenance > Image Management**.
2. Below available images, click **New Image**. The **Create New Image window** opens.
3. In the **Name** field, enter a name for the image.
4. Optional: In the **Description** field, enter a description for the image.
5. Click **OK**.



Note - To create the snapshot requires free space on the Backup partition. The required free disk space is the actual size of the root partition, multiplied by 1.15.

To revert to an image:

1. In the tree view, click **Maintenance > Image Management**.
2. Select an image.
3. Click **Revert**. The **Revert** window opens.



Note - Pay close attention to the warnings about overwriting settings, the credentials, and the reboot and the image details.

4. Click **OK**.

To delete an image:

1. In the tree view, click **Maintenance > Image Management**.
2. Select an image.
3. Click **Delete**. The **Delete Image** window opens.
4. Click **Ok**.

To export an image:

1. In the tree view, click **Maintenance > Image Management**.
2. Select an image.
3. Click **Export**. The **Export Image (name)** window.
4. Click **Start Export**.



Note -

- The snapshot image exports to `/var/log`. The free space required in the export file storage location is the size of the snapshot multiplied by two.
- The minimum size of a snapshot is 2.5G, so the minimum free space you need in the export file storage location is 5G.

To import an image:

1. In the tree view, click **Maintenance > Image Management**.
2. Select an image.
3. Click **Import**. The **Import Image** window opens.
4. Click **Browse** to select the import file for upload.
5. Click **Upload**.
6. Click **OK**.

Configuring Image Management - CLI (snapshot)

Description Manage system images (also known as snapshots)

Syntax

To make a new image:

```
add snapshot VALUE desc VALUE
```

To delete an image

```
delete snapshot VALUE
```

To export or import an image, or to revert to an image:

```
set snapshot export VALUE path VALUE name VALUE
```

```
set snapshot import VALUE path VALUE name VALUE
```

```
set snapshot revert VALUE
```

To show image information

```
show snapshot VALUE all
```

```
show snapshot VALUE date
```

```
show snapshot VALUE desc
```

```
show snapshot VALUE size
```

```
show snapshots
```

Parameters

Parameter	Description
snapshot VALUE	Name of the image
desc VALUE	Description of the image
snapshot export VALUE	The name of the image to export
snapshot import VALUE	The name of the image to import
path VALUE	The storage location for the exported image. For example: /var/log
name VALUE	The name of the exported image (not the original image).
all	All image details

Comments

- To create the snapshot image requires free space on the Backup partition. The required free disk space is the actual size of the root partition, multiplied by 1.15.
- The free space required in the export file storage location is the size of the snapshot multiplied by two.
- The minimum size of a snapshot is 2.5G, so the minimum free space you need in the export file storage location is 5G.

SecurePlatform Backup

SecurePlatform has a command line or Web GUI utility for backups of your system settings and product configuration. The **backup** utility can store backups locally on the Security Management Server, or remotely to a TFTP server or an SCP server. You can run the backup manually, or schedule backups.

The backups are TGZ files. When saved locally, the default path is: /var/CPbackup/backups

Backup and Restore commands require expert permissions.

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>]]
```

Parameter	Description
-h	See help on the command
-d	Debug flag
-l	Enables VPN log backup (by default, VPN logs are not backed up)
--purge	Deletes older backup files, from the number of days given
--sched	Schedule backups <ul style="list-style-type: none"> • On - enter time and day of week, or date of month • Off - disable schedule Example: <code>--sched on 03:00 1</code>
--tftp	Back up to TFTP. Enter IP addresses of TFTP servers Optional: <code>-path</code> pathname of backup on TFTP Example: <code>--tftp 192.0.2.3 -path /var/backups/mybckup.tgz</code>
--scp	Back up to SCP. Enter IP addresses of SCP servers, username (with access to SCP server), password, and optionally the filename Example: <code>--scp 192.0.2.4 usr 123 mybckup.tgz</code>
--file	For local backups, enter an optional filename, or <code>-path</code> parameter and pathname

SecurePlatform Snapshot Image Management

You can back up the entire SecurePlatform operating system and installed configuration with the **snapshot** command. A snapshot is made automatically during upgrade with the `SafeUpgrade` option. You can take a snapshot manually with the `snapshot` command.

The **snapshot** and **revert** commands can use a TFTP server or an SCP server to store snapshots. Snapshots can also be stored locally.

Syntax:

```
snapshot [-h] [-d] [[--tftp <Server IP> <Filename>] |
  [--scp <Server IP> <Username> <Password> <Filename>] |
  [--file <Filename>]]
```

Parameter	Description
-h	See help on the command
-d	Debug flag
--tftp	Back up to TFTP. Enter IP addresses of TFTP servers Optional: <code>-path</code> pathname of backup on TFTP Example: <code>--tftp 192.0.2.3 -path /var/backups/mybckup.tgz</code>
--scp	Back up to SCP. Enter IP addresses of SCP servers, username (with access to SCP server), password, and optionally the filename Example: <code>--scp 192.0.2.4 usr 123 mybckup.tgz</code>
--file	For local backups, enter an optional filename, or <code>-path</code> parameter and pathname

Windows and IP Appliance Export

Before you upgrade a Windows computer or IP appliance, back up the current configuration.

Use the **Export** utility tool of the version for which you are creating a backup file. The backup file has the current system configuration (for example, objects, rules, and users).



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

If upgrade ends with issues, you can restore the computers and appliances with the **Import** utility.

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. We recommend you delete it after completing import.

Restoring a Deployment

There are different ways to restore a deployment or revert a snapshot. Use the one that fits the backup you made.

To restore a deployment with an export file:

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, install using an imported configuration file.

SecurePlatform Revert

If you saved a snapshot of a SecurePlatform appliance or computer, you can revert the entire system image. The revert command run without parameters, uses default settings, and restarts the system from a local snapshot.

To revert to an earlier version (R70 or R6X):

1. Before upgrading to the newer version, take a snapshot.
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 command to restore your configuration.

To revert to snapshots of later versions, run the revert command.

Syntax:

```
revert [-h] [-d] [(--tftp <Server IP> <Filename>) | (--scp <Server IP> <Username> <Password> <Filename>) | --file <Filename>]
```

Parameter	Meaning
-h	Obtain usage
-d	Debug flag
--tftp	Revert from snapshot on TFTP server Enter IP address of the server and filename of the snapshot

Parameter	Meaning
--scp	Revert from snapshot on SCP server Enter IP address of the server, username, password, and filename of the snapshot
--file	Revert from local snapshot Enter the filename of the snapshot

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

SecurePlatform Restore

SecurePlatform has a command line or Web GUI utility for backups of your system settings and product configuration. The **backup** utility can store backups locally on the Security Management Server, or remotely to a TFTP server or an SCP server. You can run the backup manually, or schedule backups.

The backups are TGZ files. When saved locally, the default path is: `/var/CPbackup/backups`

Backup and Restore commands require expert permissions.

Syntax:

```
restore [-h] [-d] [--tftp <Server IP> <Filename>) | (--scp
<Server IP> <User name> <Password> <Filename>) | --file
<Filename>]
```

Parameter	Meaning
-h	See help on the command
-d	Debug flag
--tftp	Restore from a file on a TFTP server Enter the TFTP server IP address and the filename of the backup file
--scp	Restore from a file on a SCP server Enter the SCP server IP address, username, password, and filename of the backup file
--file	Restore from a local file Enter the filename of the backup file

For more about the **backup** and **restore** utilities, see the *System Commands* section in the *R75.40VS SecurePlatform Administration Guide* (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

Restoring Other Platforms

You can restore a computer to a version that was active before it was upgraded to R75.40VS. This will uninstall the last active version only, and leave the previously installed version as the now-active version.

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.



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: `set config-lock on override`

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 R75.40VS and click **Apply**.
3. Click the link **Click to check the status of the operation**.

There is no check in the checkbox.

4. In the **Enable** column, select:
 - All packages that have the required version number in the package name
 - Any required compatibility packages suitable for the reverted version
5. Click **Apply**.
6. Click the link **Click to check the status of the operation**. There is no check in the checkbox. The revert starts.
7. Upon completion, a success message appears.
8. Save the configuration. At the bottom of the page, click **Save**.
9. Reboot the appliance.

To revert to an earlier version on an IP appliance using the CLI:

1. At the CLI command prompt, run: `clish`
2. Run: `show package active`
3. To set the active package to inactive, run: `set package name <directory_name> off`
For example:
`set package name /opt/CPsuite-R71 off`
4. To revert to a previous package, run: `set package name <directory_name> on`
For example:
`set package name /opt/CPsuite-R65 on`
5. When prompted, restart the appliance.

To an Earlier Version on a Windows Open Server

To restore to an earlier version on a Windows platform:

1. In Add/Remove Programs, select **Check Point <product> R75.40VS**.
2. Click **Remove**.

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

ICA Considerations

When a computer or appliance installation is restored, certificates issued during the use of R75.40VS remain valid. But 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 R75.40VS to a suitable location.
2. Copy the R75.40VS `InternalCA.NDB`, `ICA.crl` and the `*.crl` files (located in the `$FWDIR/conf` directory) from the current R75.40VS version and use them to overwrite the files in the location specified in the `$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 from the reverted environment.

3. When the Revert process is complete, use the ICA Management Tool to review certificates created using R75.40VS 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.

Service Contract Files

Introduction

Before upgrading a gateway or Security Management server to R75.40VS, 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 Gaia, SecurePlatform and Windows

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 contract file or import it.

If the contract file does not cover the Security Management server, a message on Download or Import informs you that the Security Management server is not eligible for upgrade. The absence of a valid contract file does not prevent upgrade. Download a valid contract at a later date using SmartUpdate.

- **Download a contracts file from the User Center**

If you have Internet access and a valid user account, 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)

- **Import a local contract file**

If the server does not have Internet access:

- a) On a machine with Internet access, log in to the User Center (<http://usercenter.checkpoint.com>).
- b) Click **Support** in the top menu.
- c) Click **Additional Services** in the secondary menu.
- d) In the **Service Contract File Download** section, click **Download Now**.
- e) 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.

- **Continue without contract information**

Select this option if you intend to get 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.

On IP Appliances

Contract verification on IPSO is not interactive. 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/nginx/upgrade/contract/
```

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

On Security Gateways

After you accept 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. If not found, you can download or import a contract.

If the contract file does not cover the gateway, a message informs you (on Download or Import) that the gateway is not eligible for upgrade. The absence of a valid contract file does not prevent upgrade. When the upgrade is complete, contact your local support provider to obtain a valid contract. Use SmartUpdate to install the contract file.

Use the download or import instructions for installing a contract file on a Security Management Server.

If you continue without a contract, you install a valid contract file later. But the gateway is not eligible for upgrade. You may be in violation of your Check Point Licensing Agreement, as shown in the final message of the upgrade process. Contact your reseller.

Chapter 6

Upgrading Security Management Server and Security Gateways

In This Chapter

Upgrading Standalone	76
Upgrading the Security Management Server	84
Upgrading Security Gateways	91
Upgrading Standalone Full High Availability	110
Upgrading Clusters	111

Upgrading Standalone

This section explains how to upgrade a standalone (Security Management Server and Security Gateway installed on one appliance or computer). A Security Management Server upgraded to R75.40VS can enforce and manage gateways from earlier versions. Some new features are not available on earlier versions (see the "Compatibility Tables" in the *Release Notes*).

Upgrading Standalone Appliances

You can upgrade a Standalone deployment on UTM-1 appliances, certain 2012 Models, and IP appliances.

UTM-1 and 2012 Models

When you upgrade the Check Point release version on the appliance you can also upgrade from SecurePlatform to Gaia. Alternatively, you can upgrade Check Point release version and stay with the SecurePlatform operating system.

Gaia to Gaia

Upgrade Requirements:

Ensure you have at least 6 GB of disk space available to do the upgrade.

- Using the WebUI: Check the space available for images in the **Maintenance > Image Management** page.
- Using the CLI: In expert mode, run the `df -h` command and check the available space in `/var/log`.

To upgrade using the WebUI:

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>) to the Gaia WebUI client computer. The upgrade package has a name similar to `gaia_upg_R75.40VS.tgz`
2. Connect to the Gaia WebUI from a Web browser to `https://<management_IP_address>`
3. In the WebUI go to the **Maintenance > Upgrade** page. (Ensure the **View Mode** is **Advanced**.)
4. Click **Upload**.
5. Browse to the location of the upgrade package.
6. After the package is uploaded, either click **Done** to add the package to the **Upgrade Packages** repository, or click **Upgrade**.

If you added the package to the package repository, select the package, and click **Upgrade**.

The package is extracted.

7. After the package is extracted, click **OK**.

A console window opens.

You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer *Yes*.

8. The pre-upgrade verifier runs. The output is stored in a text file at `/tmp/pre_upgrade_out.txt`.
9. If you see the error: "Pre-upgrade verification failed" we recommend that you review the file, fix the problems, and restart the upgrade. Do not take another system snapshot.
10. You are asked if you want to start the upgrade. Select *Yes*.
11. After the upgrade, click **Reboot**.

To upgrade using the upgrade package, with CLI:

You can upload the TGZ to the WebUI, and upgrade Gaia with CLI commands.

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
Check_Point_Upgrade_WEBUI_and_SmartUpdate_R75.40VS.Gaia.tgz
2. In the Gaia CLI, enter `expert` mode.
3. Use FTP, SCP or similar to transfer the upgrade package to the Gaia appliance or computer. We recommend that you place the package in `/var/log/upload`.
4. Exit `expert` mode.
5. In `clish`, register the file as an upgrade package. Run the command:
`add upgrade <version> package file <full path>`
6. Run:
`upgrade local <version>`
For example:
`upgrade local R75.40VS`
You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer *Yes*.
7. The pre-upgrade verifier runs. The output is stored in a text file at `/tmp/pre_upgrade_out.txt`.
If you see the error: "Pre-upgrade verification failed" we recommend that you review the file, fix the problems, and restart the upgrade. Do not take another system snapshot.
8. You are asked if you want to start the upgrade. Select *Yes*.
9. After the upgrade, type `OK` to reboot.

To upgrade using an ISO image on a DVD:

1. Download the Gaia ISO image from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
The upgrade package has a name similar to
`Check_Point_R75.40VS_Gaia.iso`
2. Burn the ISO file on a DVD.
3. Connect an external DVD drive to a USB socket on the appliance or computer.
4. Run
`upgrade cd`
5. You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer *Yes*.
6. The pre-upgrade verifier runs. The output is stored in a text file at `/tmp/pre_upgrade_out.txt`.
7. If you see the error: "Pre-upgrade verification failed" we recommend that you review the file, fix the problems, and restart the upgrade. Do not take another system snapshot.
8. You are asked if you want to start the upgrade. Select *Yes*.
The upgrade takes place.
9. After the upgrade, before rebooting, remove the DVD from the drive.

10. Type **OK** to reboot.

SecurePlatform to Gaia



Note - When upgrading from SecurePlatform to Gaia, the size of the disk partitions does not change. To have larger disk partitions, you need to do a clean installation of Gaia ("[Disk Partitions in a Gaia Clean Installation](#)" on page 17).

You can upgrade from the SecurePlatform operating system to the Gaia operating system.

To upgrade a SecurePlatform appliance:

1. Upgrade product licenses to R75 or higher, and attach the licenses to the appliance.
2. Download the appliance upgrade package.
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R75.40VS.Gaia.tgz`
3. Connect to the SecurePlatform appliance from a Web browser to `https://<appliance_ip_address>`.
4. In the login page, enter an administrator username and password.
5. Go to the **Upgrade** page.
6. Upload the appliance upgrade package to the appliance.
7. Ignore any warning messages.
8. Continue according to the on-screen instructions.

After the upgrade is complete, the appliance boots to Gaia.



Note - The connection to the SecurePlatform WebUI closes after Gaia is installed.

9. Install the Policy on the Security Gateway. This is highly recommended. The Security Gateway enforces the Initial Policy until you install the Policy:
 - a) Using SmartDashboard of the correct version, connect to the Security Management server.
 - b) Open the **General Properties** page of the Gateway object.
 - c) Click **Get** to update the **Platform** details.
 - d) Install the policy on the Gateway.

If the Gaia appliance has more than 4 GB of memory, it automatically boots to the 64-bit edition. Otherwise, it boots to the 32-bit edition.

If you upgrade and the appliance has more than 4 GB, the appliance boots to the 32-bit edition. You can configure Gaia to automatically boot to the 64-bit edition.

To configure Gaia to automatically boot to the 64-bit edition:

1. Run `set edition default 64-bit`
2. Run `save config`
3. Reboot



Note - The appliance must have at least 6 GB of memory for this to work.

To see which edition is running:

- Go to the WebUI **System Overview** pane. The edition shows in the **System Overview** widget.
or
- Run: `show version os edition`

SecurePlatform to SecurePlatform

Use the WebUI of the appliance to upgrade Standalone UTM-1 and 2012 Model appliances.

To upgrade appliances using the WebUI:

1. Open Internet Explorer and log in to the appliance.
2. Select **Appliance > Upgrade**.
3. Click **Check Point Download Center**.

- The Internet browser opens to the Check Point Support Center.
4. Search for and download the R75.40VS upload package file.
 5. In the WebUI, click **Upload upgrade package to appliance**.
The **Upload Package to Appliance** window opens.
 6. Select the upgrade file:
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R76.SecurePlatform.tgz`
 7. Click **Upload**.
 8. Click **Start Upgrade**.
 9. 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**.
 10. 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**.
 11. The **Current Upgrade File on Appliance** section displays the information of the current upgrade.
 12. To begin the upgrade, click **Start**.

IP Appliances

Gaia to Gaia

Upgrade Requirements:

Ensure you have at least 6 GB of disk space available to do the upgrade.

- Using the WebUI: Check the space available for images in the **Maintenance > Image Management** page.
- Using the CLI: In expert mode, run the `df -h` command and check the available space in `/var/log`.

To upgrade using the WebUI:

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>) to the Gaia WebUI client computer. The upgrade package has a name similar to `gaia_upg_R75.40VS.tgz`
2. Connect to the Gaia WebUI from a Web browser to `https://<management_IP_address>`
3. In the WebUI go to the **Maintenance > Upgrade** page. (Ensure the **View Mode** is **Advanced**.)
4. Click **Upload**.
5. Browse to the location of the upgrade package.
6. After the package is uploaded, either click **Done** to add the package to the **Upgrade Packages** repository, or click **Upgrade**.
If you added the package to the package repository, select the package, and click **Upgrade**.
The package is extracted.
7. After the package is extracted, click **OK**.
A console window opens.
You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer **Yes**.
8. The pre-upgrade verifier runs. The output is stored in a text file at `/tmp/pre_upgrade_out.txt`.
9. If you see the error: "Pre-upgrade verification failed" we recommend that you review the file, fix the problems, and restart the upgrade. Do not take another system snapshot.
10. You are asked if you want to start the upgrade. Select **Yes**.
11. After the upgrade, click **Reboot**.

To upgrade using the upgrade package, with CLI:

You can upload the TGZ to the WebUI, and upgrade Gaia with CLI commands.

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
Check_Point_Upgrade_WEBUI_and_SmartUpdate_R75.40VS.Gaia.tgz
2. In the Gaia CLI, enter `expert` mode.
3. Use FTP, SCP or similar to transfer the upgrade package to the Gaia appliance or computer. We recommend that you place the package in `/var/log/upload`.
4. Exit `expert` mode.
5. In `clish`, register the file as an upgrade package. Run the command:
`add upgrade <version> package file <full path>`
6. Run:
`upgrade local <version>`
For example:
`upgrade local R75.40VS`
You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer `Yes`.
7. The pre-upgrade verifier runs. The output is stored in a text file at `/tmp/pre_upgrade_out.txt`.
If you see the error: "Pre-upgrade verification failed" we recommend that you review the file, fix the problems, and restart the upgrade. Do not take another system snapshot.
8. You are asked if you want to start the upgrade. Select `Yes`.
9. After the upgrade, type `OK` to reboot.

Upgrading Standalone Open Servers

Before you upgrade:

- Back up your current configuration (see "Backing Up" on page 66).
- See the Release Notes to make sure that you have enough disk space (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

Gaia to Gaia**Upgrade Requirements:**

Ensure you have at least 6 GB of disk space available to do the upgrade.

- Using the WebUI: Check the space available for images in the **Maintenance > Image Management** page.
- Using the CLI: In expert mode, run the `df -h` command and check the available space in `/var/log`.

To upgrade using the WebUI:

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>) to the Gaia WebUI client computer. The upgrade package has a name similar to
`gaia_upg_R75.40VS.tgz`
2. Connect to the Gaia WebUI from a Web browser to
`https://<management_IP_address>`
3. In the WebUI go to the **Maintenance > Upgrade** page. (Ensure the **View Mode** is **Advanced**.)
4. Click **Upload**.
5. Browse to the location of the upgrade package.
6. After the package is uploaded, either click **Done** to add the package to the **Upgrade Packages** repository, or click **Upgrade**.
If you added the package to the package repository, select the package, and click **Upgrade**.
The package is extracted.
7. After the package is extracted, click **OK**.

A console window opens.

You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer **Yes**.

8. The pre-upgrade verifier runs. The output is stored in a text file at `/tmp/pre_upgrade_out.txt`.
9. If you see the error: "Pre-upgrade verification failed" we recommend that you review the file, fix the problems, and restart the upgrade. Do not take another system snapshot.
10. You are asked if you want to start the upgrade. Select **Yes**.
11. After the upgrade, click **Reboot**.

To upgrade using the upgrade package, with CLI:

You can upload the TGZ to the WebUI, and upgrade Gaia with CLI commands.

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R75.40VS.Gaia.tgz`
2. In the Gaia CLI, enter `expert mode`.
3. Use FTP, SCP or similar to transfer the upgrade package to the Gaia appliance or computer. We recommend that you place the package in `/var/log/upload`.
4. Exit `expert mode`.
5. In `clish`, register the file as an upgrade package. Run the command:
`add upgrade <version> package file <full path>`
6. Run:
`upgrade local <version>`
For example:
`upgrade local R75.40VS`
You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer **Yes**.
7. The pre-upgrade verifier runs. The output is stored in a text file at `/tmp/pre_upgrade_out.txt`.
If you see the error: "Pre-upgrade verification failed" we recommend that you review the file, fix the problems, and restart the upgrade. Do not take another system snapshot.
8. You are asked if you want to start the upgrade. Select **Yes**.
9. After the upgrade, type **OK** to reboot.

To upgrade using an ISO image on a DVD:

1. Download the Gaia ISO image from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
The upgrade package has a name similar to
`Check_Point_R75.40VS_Gaia.iso`
2. Burn the ISO file on a DVD.
3. Connect an external DVD drive to a USB socket on the appliance or computer.
4. Run
`upgrade cd`
5. You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer **Yes**.
6. The pre-upgrade verifier runs. The output is stored in a text file at `/tmp/pre_upgrade_out.txt`.
7. If you see the error: "Pre-upgrade verification failed" we recommend that you review the file, fix the problems, and restart the upgrade. Do not take another system snapshot.
8. You are asked if you want to start the upgrade. Select **Yes**.
The upgrade takes place.
9. After the upgrade, before rebooting, remove the DVD from the drive.
10. Type **OK** to reboot.

SecurePlatform to Gaia

Use this procedure to upgrade a SecurePlatform computer on to a Gaia computer. Upgrade the operating system and the installed products.



Note - When upgrading from SecurePlatform to Gaia, the size of the disk partitions does not change. To have larger disk partitions, you need to do a clean installation of Gaia ("[Disk Partitions in a Gaia Clean Installation](#)" on page 17).

To upgrade an open server using the DVD:

1. Upgrade your product licenses to R75 or higher, and attach the licenses to the Security Gateway or standalone server.
2. Insert R75.40VS DVD into the drive.
3. At the command prompt, enter: `patch add cd`
4. Select the Gaia upgrade package.
5. Confirm the MD5 checksum.
6. If relevant, when prompted, create a backup image for automatic revert.
7. After extracting files, the Installation program opens.
8. Accept the license agreement.
9. Select **upgrade**.
10. Configure your contract options.
You can also continue without contract information and configure it later using SmartUpdate.
11. Select a source for the upgrade utilities.
Wait for the pre-upgrade verifier to complete successfully.
12. Select **Stop Check Point processes**.
13. Select **Upgrade installed products**, or **upgrade installed products and add new products**, and confirm.
14. Wait while the required installation files are extracted.
 - a) Part one of the upgrade procedure saves data and upgrades the operating system.
 - b) Part two upgrades Check Point products.
15. After the upgrade completes successfully, remove the DVD from the drive.
16. Reboot when prompted.
17. Install the Policy on the Security Gateway. This is highly recommended. The Security Gateway enforces the Initial Policy until you install the Policy:
 - a) Using SmartDashboard of the correct version, connect to the Security Management server.
 - b) Open the **General Properties** page of the Gateway object.
 - c) Click **Get** to update the **Platform** details.
 - d) Install the policy on the Gateway.

o upgrade a SecurePlatform Open Server using the WebUI:

1. Open Internet Explorer and log in to the SecurePlatform WebUI.
2. Select **Device > Upgrade**.
3. Click **Check Point Download Center**.
The Internet browser opens to the Check Point Support Center.
4. Search for and download the R75.40VS file for upgrades via the WebUI.
5. Click **Browse** and select the upgrade file:
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R76.Gaia.tgz`
6. Click **Upload package to device**.
The package is uploaded to the SecurePlatform computer.
After the **Upgrade Status** shows that the *Uploading* is *Completed* you can start the upgrade.
7. **Recommended:** In the **Safe Upgrade** section, click **Save snapshot of the current system before the upgrade**. The snapshot is used to revert the system if the upgrade is not successful.

8. Click **Start Upgrade**.

Follow the **Upgrade Status**. After the upgrade, the computer automatically reboots.



Note - The connection to the SecurePlatform WebUI closes after Gaia is installed.

9. Install the Policy on the Security Gateway. This is highly recommended. The Security Gateway enforces the Initial Policy until you install the Policy:

- a) Using SmartDashboard of the correct version, connect to the Security Management server.
- b) Open the **General Properties** page of the Gateway object.
- c) Click **Get** to update the **Platform** details.
- d) Install the policy on the Gateway.

SecurePlatform to SecurePlatform

Use this procedure to upgrade a SecurePlatform installation on the same computer. Upgrade the operating system and the installed products.

To upgrade a SecurePlatform Open Server using a DVD:

1. Insert R75.40VS DVD into the drive.
2. At the command prompt, enter: `patch add cd`
3. Select **SecurePlatform R75.40VS Upgrade Package** (CPspupgrade_<version_number>.tgz).
4. Press **y** to accept the checksum calculation.
5. Optional: When prompted, create a backup image so that you can restore the old version.



Note - Creating the snapshot image can take a long time. Check Point products are stopped during this time.

6. Press **N** at the welcome message.
7. Press **Y** to accept the license agreement.
8. In the next window, select **Upgrade** and then press **N**.
9. In the next window, press **N** to continue.
10. If prompted to download or import a valid support contract, select **Continue without contract information**. Press **N** to continue.
11. If a message shows that says your gateway is not eligible for upgrade, press **N** to continue.
You can safely ignore this message and use SmartUpdate to update your service contract later.
12. In the next window, select **Download most updated files**.
13. In the **Pre-Upgrade Verification Results** window, press **N** to continue.
If the Pre-Upgrade Verification fails, do the suggested steps to correct the problem. Start this procedure again from step 2.
14. When prompted, select **Stop Check Point processes** and press **N** to continue.
15. When prompted, select **Upgrade installed products** and press **N** to continue.
16. In the **Validation** window, press **N**.
17. When the upgrade completes successfully, restart the computer.

To upgrade a SecurePlatform Open Server using the WebUI:

1. Open Internet Explorer and log in to the SecurePlatform WebUI.
2. Select **Device > Upgrade**.
3. Click **Check Point Download Center**.
The Internet browser opens to the Check Point Support Center.
4. Search for and download the R75.40VS file for upgrades via the WebUI.
5. Click **Browse** and select the upgrade file:
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R75.40VS.SecurePlatform.tgz`
6. Click **Upload package to device**.
The package is uploaded to the SecurePlatform computer.
After the **Upgrade Status** shows that the *Uploading* is *Completed* you can start the upgrade.

7. **Recommended:** In the **Safe Upgrade** section, click **Save snapshot of the current system before the upgrade**. The snapshot is used to revert the system if the upgrade is not successful.

Your browser will automatically try to perform the first login immediately after the upgrade. To allow this, do not close the browser window or browse to another page.

8. Click **Start Upgrade**.
Follow the **Upgrade Status**. After the upgrade, the computer automatically reboots.
9. Install the Policy on the Security Gateway. This is highly recommended. The Security Gateway enforces the Initial Policy until you install the Policy:
 - a) Using SmartDashboard of the correct version, connect to the Security Management server.
 - b) Open the **General Properties** page of the Gateway object.
 - c) Click **Get** to update the **Platform** details.
 - d) Install the policy on the Gateway.

Windows to Windows

Use this procedure to upgrade a Windows installation on the computer. Upgrade the installed products.

To upgrade a Windows standalone computer:

1. Insert the R75.40VS DVD into the drive. The Installation Wizard starts automatically.
If the wizard does not start automatically, manually run setup.exe from the DVD drive.
2. Click **Next** at the welcome message.
3. Accept the license agreement and click **Next**.
4. Select **Upgrade** and click **Next**.
5. On the next screen, click **Next**.
6. If prompted to download or import a valid support contract, select **Continue without contract information**. Click **Next** to continue.
7. If a message shows that says your gateway is not eligible for upgrade.
You can safely ignore this message and use SmartUpdate to update your service contract later. Click **Next**.
8. Select **Download most updated files** and click **Next**.
9. In the **Pre-Upgrade Verification Results** window, click **Next**.
If the Pre-Upgrade Verification fails, do the suggested steps to correct the problem. Start this procedure again from step 2.
10. When prompted to add new products, clear **Add new products** and then click **Next**.
You can add new products at a later time.
11. Click **Next** at the confirmation message.
12. When the installation completes successfully, click **Finish**.
13. When prompted, restart the computer.

Upgrading the Security Management Server

You do not have to upgrade the Security Management server and all of the gateways at the same time. When the Security Management server is upgraded, you can still manage gateways from earlier versions (though the gateways may not support new features).



Important - To upgrade to R76 Gaia, there must be at least 4GB free disk space in `/var/log`.

Use the Pre-Upgrade Verification tool to reduce the risk of incompatibility with your existing environment. The Pre-Upgrade Verification tool generates a detailed report of the actions to take before an upgrade (see ["Using the Pre-Upgrade Verifier Tool"](#) on page 65).

There are different upgrade methods for the Security Management server:

- Upgrade Production Security Management server

- Migrate and Upgrade to a New Security Management server ("[Advanced Upgrade and Database Migration](#)" on page 142)



Important - After upgrade, you cannot restore a version with a database revision that was made with the old version. You can see old version database saves in Read-Only mode.

Upgrading Security Management Server on Appliances

You can upgrade a Security Management server on some Smart-1 appliances, 2012 Models and open servers.

Smart-1 and 2012 Models

You can upgrade a 2012 Model appliance from SecurePlatform to Gaia, or you can upgrade the SecurePlatform version.

Gaia to Gaia

Upgrade Requirements:

Ensure you have at least 6 GB of disk space available to do the upgrade.

- Using the WebUI: Check the space available for images in the **Maintenance > Image Management** page.
- Using the CLI: In expert mode, run the `df -h` command and check the available space in `/var/log`.

To upgrade using the WebUI:

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>) to the Gaia WebUI client computer. The upgrade package has a name similar to `gaia_upg_R75.40VS.tgz`
2. Connect to the Gaia WebUI from a Web browser to `https://<management_IP_address>`
3. In the WebUI go to the **Maintenance > Upgrade** page. (Ensure the **View Mode** is **Advanced**.)
4. Click **Upload**.
5. Browse to the location of the upgrade package.
6. After the package is uploaded, either click **Done** to add the package to the **Upgrade Packages** repository, or click **Upgrade**.
If you added the package to the package repository, select the package, and click **Upgrade**.
The package is extracted.
7. After the package is extracted, click **OK**.
A console window opens.
You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer **Yes**.
8. The pre-upgrade verifier runs. The output is stored in a text file at `/tmp/pre_upgrade_out.txt`.
9. If you see the error: "Pre-upgrade verification failed" we recommend that you review the file, fix the problems, and restart the upgrade. Do not take another system snapshot.
10. You are asked if you want to start the upgrade. Select **Yes**.
11. After the upgrade, click **Reboot**.

To upgrade using the upgrade package, with CLI:

You can upload the TGZ to the WebUI, and upgrade Gaia with CLI commands.

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R75.40VS.Gaia.tgz`
2. In the Gaia CLI, enter `expert` mode.

3. Use FTP, SCP or similar to transfer the upgrade package to the Gaia appliance or computer. We recommend that you place the package in `/var/log/upload`.
4. Exit `expert` mode.
5. In `clish`, register the file as an upgrade package. Run the command:
`add upgrade <version> package file <full path>`
6. Run:
`upgrade local <version>`
For example:
`upgrade local R75.40VS`
You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer `Yes`.
7. The pre-upgrade verifier runs. The output is stored in a text file at `/tmp/pre_upgrade_out.txt`.
If you see the error: "Pre-upgrade verification failed" we recommend that you review the file, fix the problems, and restart the upgrade. Do not take another system snapshot.
8. You are asked if you want to start the upgrade. Select `Yes`.
9. After the upgrade, type `OK` to reboot.

To upgrade using an ISO image on a DVD:

1. Download the Gaia ISO image from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
The upgrade package has a name similar to
`Check_Point_R75.40VS_Gaia.iso`
2. Burn the ISO file on a DVD.
3. Connect an external DVD drive to a USB socket on the appliance or computer.
4. Run
`upgrade cd`
5. You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer `Yes`.
6. The pre-upgrade verifier runs. The output is stored in a text file at `/tmp/pre_upgrade_out.txt`.
7. If you see the error: "Pre-upgrade verification failed" we recommend that you review the file, fix the problems, and restart the upgrade. Do not take another system snapshot.
8. You are asked if you want to start the upgrade. Select `Yes`.
The upgrade takes place.
9. After the upgrade, before rebooting, remove the DVD from the drive.
10. Type `OK` to reboot.

SecurePlatform to Gaia



Note - When upgrading from SecurePlatform to Gaia, the size of the disk partitions does not change. To have larger disk partitions, you need to do a clean installation of Gaia ("[Disk Partitions in a Gaia Clean Installation](#)" on page 17).

You can upgrade from the SecurePlatform operating system to the Gaia operating system.

To upgrade a SecurePlatform appliance:

1. Upgrade product licenses to R75 or higher, and attach the licenses to the appliance.
2. Download the appliance upgrade package.
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R75.40VS.Gaia.tgz`
3. Connect to the SecurePlatform appliance from a Web browser to
`https://<appliance_ip_address>`.
4. In the login page, enter an administrator username and password.
5. Go to the **Upgrade** page.
6. Upload the appliance upgrade package to the appliance.
7. Ignore any warning messages.
8. Continue according to the on-screen instructions.

After the upgrade is complete, the appliance boots to Gaia.



Note - The connection to the SecurePlatform WebUI closes after Gaia is installed.

9. Install the Policy on the Security Gateway. This is highly recommended. The Security Gateway enforces the Initial Policy until you install the Policy:
 - a) Using SmartDashboard of the correct version, connect to the Security Management server.
 - b) Open the **General Properties** page of the Gateway object.
 - c) Click **Get** to update the **Platform** details.
 - d) Install the policy on the Gateway.

SecurePlatform to SecurePlatform

Use the WebUI of the appliance to upgrade Security Management server Smart-1 and 2012 Model appliances.

To upgrade appliances using the WebUI:

1. Open Internet Explorer and log in to the appliance.
2. Select **Appliance > Upgrade**.
3. Click **Check Point Download Center**.
The Internet browser opens to the Check Point Support Center.
4. Search for and download the R75.40VS upload package file.
5. In the WebUI, click **Upload upgrade package to appliance**.
The **Upload Package to Appliance** window opens.
6. Select the upgrade file:
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R76.SecurePlatform.tgz`
7. Click **Upload**.
8. Click **Start Upgrade**.
9. 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**.
10. 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**.
11. The **Current Upgrade File on Appliance** section displays the information of the current upgrade.
12. To begin the upgrade, click **Start**.

Upgrading Security Management Server on Open Servers

A Security Management server on any computer that meets the minimum requirements can be upgraded. You can upgrade from SecurePlatform to Gaia, or you can upgrade the SecurePlatform version. On a Windows Security Management server, you can upgrade the installed Check Point products.

Before you upgrade:

It is recommended to back up your current configuration (see "[Backing Up](#)" on page 66).

Gaia to Gaia

Upgrade Requirements:

Ensure you have at least 6 GB of disk space available to do the upgrade.

- Using the WebUI: Check the space available for images in the **Maintenance > Image Management** page.
- Using the CLI: In expert mode, run the `df -h` command and check the available space in `/var/log`.

To upgrade using the WebUI:

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>) to the Gaia WebUI client computer. The upgrade package has a name similar to `gaia_upg_R75.40VS.tgz`
2. Connect to the Gaia WebUI from a Web browser to `https://<management_IP_address>`
3. In the WebUI go to the **Maintenance > Upgrade** page. (Ensure the **View Mode** is **Advanced**.)
4. Click **Upload**.
5. Browse to the location of the upgrade package.
6. After the package is uploaded, either click **Done** to add the package to the **Upgrade Packages** repository, or click **Upgrade**.
If you added the package to the package repository, select the package, and click **Upgrade**.
The package is extracted.
7. After the package is extracted, click **OK**.
A console window opens.
You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer *Yes*.
8. The pre-upgrade verifier runs. The output is stored in a text file at `/tmp/pre_upgrade_out.txt`.
9. If you see the error: "Pre-upgrade verification failed" we recommend that you review the file, fix the problems, and restart the upgrade. Do not take another system snapshot.
10. You are asked if you want to start the upgrade. Select *Yes*.
11. After the upgrade, click **Reboot**.

To upgrade using the upgrade package, with CLI:

You can upload the TGZ to the WebUI, and upgrade Gaia with CLI commands.

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R75.40VS.Gaia.tgz`
2. In the Gaia CLI, enter `expert` mode.
3. Use FTP, SCP or similar to transfer the upgrade package to the Gaia appliance or computer. We recommend that you place the package in `/var/log/upload`.
4. Exit `expert` mode.
5. In `clish`, register the file as an upgrade package. Run the command:
`add upgrade <version> package file <full path>`
6. Run:
`upgrade local <version>`
For example:
`upgrade local R75.40VS`
You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer *Yes*.
7. The pre-upgrade verifier runs. The output is stored in a text file at `/tmp/pre_upgrade_out.txt`.
If you see the error: "Pre-upgrade verification failed" we recommend that you review the file, fix the problems, and restart the upgrade. Do not take another system snapshot.
8. You are asked if you want to start the upgrade. Select *Yes*.
9. After the upgrade, type `OK` to reboot.

To upgrade using an ISO image on a DVD:

1. Download the Gaia ISO image from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
The upgrade package has a name similar to `Check_Point_R75.40VS_Gaia.iso`
2. Burn the ISO file on a DVD.

3. Connect an external DVD drive to a USB socket on the appliance or computer.
4. Run
`upgrade cd`
5. You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer **Yes**.
6. The pre-upgrade verifier runs. The output is stored in a text file at `/tmp/pre_upgrade_out.txt`.
7. If you see the error: "Pre-upgrade verification failed" we recommend that you review the file, fix the problems, and restart the upgrade. Do not take another system snapshot.
8. You are asked if you want to start the upgrade. Select **Yes**.
The upgrade takes place.
9. After the upgrade, before rebooting, remove the DVD from the drive.
10. Type **OK** to reboot.

SecurePlatform to Gaia

Use this procedure to upgrade the SecurePlatform operating system to Gaia, and to upgrade the installed products.



Note - When upgrading from SecurePlatform to Gaia, the size of the disk partitions does not change. To have larger disk partitions, you need to do a clean installation of Gaia ("[Disk Partitions in a Gaia Clean Installation](#)" on page 17).

To upgrade Security Management Server on Gaia open servers:

1. Upgrade product licenses to R75 or higher, and attach the licenses to the appliance.
2. Connect a DVD drive to the USB port on the computer.
3. Run: `patch add cd`
4. Select the Gaia upgrade package.
5. Confirm the MD5 checksum.
6. When prompted, create a backup image for automatic revert.
After extracting files, the Installation program opens.
7. Accept the license agreement.
8. Select **upgrade**.
9. Configure your contract options.
You can also continue without contract information and configure it later using SmartUpdate.
10. Select a source for the upgrade utilities.
Wait for the pre-upgrade verifier to complete successfully.
11. Select **Stop Check Point processes**.
12. Select **Upgrade installed products**, or **upgrade installed products and add new products**, and confirm.
13. Wait while the required installation files are extracted.
 - a) Part one of the upgrade procedure saves data and upgrades the operating system.
 - b) Part two upgrades Check Point products.
14. After the upgrade completes successfully, remove the DVD from the drive.
15. Restart when prompted.
16. Install the Policy on the Security Gateway. This is highly recommended. The Security Gateway enforces the Initial Policy until you install the Policy:
 - a) Using SmartDashboard of the correct version, connect to the Security Management server.
 - b) Open the **General Properties** page of the Gateway object.
 - c) Click **Get** to update the **Platform** details.
 - d) Install the policy on the Gateway.

o upgrade a SecurePlatform Open Server using the WebUI:

1. Open Internet Explorer and log in to the SecurePlatform WebUI.
2. Select **Device > Upgrade**.
3. Click **Check Point Download Center**.
The Internet browser opens to the Check Point Support Center.
4. Search for and download the R75.40VS file for upgrades via the WebUI.
5. Click **Browse** and select the upgrade file:
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R76.Gaia.tgz`
6. Click **Upload package to device**.
The package is uploaded to the SecurePlatform computer.
After the **Upgrade Status** shows that the *Uploading* is *Completed* you can start the upgrade.
7. **Recommended:** In the **Safe Upgrade** section, click **Save snapshot of the current system before the upgrade**. The snapshot is used to revert the system if the upgrade is not successful.
8. Click **Start Upgrade**.
Follow the **Upgrade Status**. After the upgrade, the computer automatically reboots.



Note - The connection to the SecurePlatform WebUI closes after Gaia is installed.

SecurePlatform to SecurePlatform

Use this procedure to upgrade a SecurePlatform installation on the same computer. Upgrade the operating system and the installed products.

To upgrade a SecurePlatform Open Server using a DVD:

1. Insert R75.40VS DVD into the drive.
2. At the command prompt, enter: `patch add cd`
3. Select **SecurePlatform R75.40VS Upgrade Package** (`CPspupgrade_<version_number>.tgz`).
4. Press **y** to accept the checksum calculation.
5. Optional: When prompted, create a backup image so that you can restore the old version.



Note - Creating the snapshot image can take a long time. Check Point products are stopped during this time.

6. Press **N** at the welcome message.
7. Press **Y** to accept the license agreement.
8. In the next window, select **Upgrade** and then press **N**.
9. In the next window, press **N** to continue.
10. If prompted to download or import a valid support contract, select **Continue without contract information**. Press **N** to continue.
11. If a message shows that says your gateway is not eligible for upgrade, press **N** to continue.
You can safely ignore this message and use SmartUpdate to update your service contract later.
12. In the next window, select **Download most updated files**.
13. In the **Pre-Upgrade Verification Results** window, press **N** to continue.
If the Pre-Upgrade Verification fails, do the suggested steps to correct the problem. Start this procedure again from step 2.
14. When prompted, select **Stop Check Point processes** and press **N** to continue.
15. When prompted, select **Upgrade installed products** and press **N** to continue.
16. In the **Validation** window, press **N**.
17. When the upgrade completes successfully, restart the computer.

To upgrade a SecurePlatform Open Server using the WebUI:

1. Open Internet Explorer and log in to the SecurePlatform WebUI.
2. Select **Device > Upgrade**.
3. Click **Check Point Download Center**.
The Internet browser opens to the Check Point Support Center.

4. Search for and download the R75.40VS file for upgrades via the WebUI.
5. Click **Browse** and select the upgrade file:
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R75.40VS.SecurePlatform.tgz`
6. Click **Upload package to device**.
The package is uploaded to the SecurePlatform computer.
After the **Upgrade Status** shows that the *Uploading* is *Completed* you can start the upgrade.
7. **Recommended:** In the **Safe Upgrade** section, click **Save snapshot of the current system before the upgrade**. The snapshot is used to revert the system if the upgrade is not successful.

Your browser will automatically try to perform the first login immediately after the upgrade. To allow this, do not close the browser window or browse to another page.
8. Click **Start Upgrade**.
Follow the **Upgrade Status**. After the upgrade, the computer automatically reboots.

Windows to Windows

Before you begin, back up the server.

To upgrade a Windows Security Management Server:

1. Insert the R75.40VS 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.
8. When the pre-upgrade verification recommendation appears, select to execute the Pre-upgrade Verification Tool.
9. Select **Add new products** and click **Next**.
Note - SmartReporter is installed by default, if it was not installed before.
Depending on the components you have chosen to install, you may need to install other components. Follow the instructions.
A list of the products that will be upgraded appears. Click **Next**.
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 is not installed, it will be installed before the Check Point components.
10. Follow the instructions for license management and fingerprint handling.
11. Click **Finish**.
12. When prompted, restart the Security Management Server.

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 Gateways using SmartUpdate

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 upgrades all packages installed on a gateway. For IPSO and SecurePlatform, this feature also upgrades your operating system as a part of the upgrade procedure.

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.
- **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 - 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.

Upgrading Security Gateways on Appliances

UTM-1, Power-1, and 2012 Models

Gaia to Gaia

Upgrade Requirements:

Ensure you have at least 6 GB of disk space available to do the upgrade.

- Using the WebUI: Check the space available for images in the **Maintenance > Image Management** page.
- Using the CLI: In expert mode, run the `df -h` command and check the available space in `/var/log`.

To upgrade using the WebUI:

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>) to the Gaia WebUI client computer. The upgrade package has a name similar to `gaia_upg_R75.40VS.tgz`
2. Connect to the Gaia WebUI from a Web browser to `https://<management_IP_address>`
3. In the WebUI go to the **Maintenance > Upgrade** page. (Ensure the **View Mode** is **Advanced**.)
4. Click **Upload**.
5. Browse to the location of the upgrade package.
6. After the package is uploaded, either click **Done** to add the package to the **Upgrade Packages** repository, or click **Upgrade**.

If you added the package to the package repository, select the package, and click **Upgrade**.
The package is extracted.

7. After the package is extracted, click **OK**.

A console window opens.

You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer `Yes`.

8. You are asked if you want to start the upgrade. Select `Yes`.
9. After the upgrade, click **Reboot**.

To upgrade using the upgrade package, with CLI:

You can upload the TGZ to the WebUI, and upgrade Gaia with CLI commands.

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R75.40VS.Gaia.tgz`
2. In the Gaia CLI, enter `expert` mode.

3. Use FTP, SCP or similar to transfer the upgrade package to the Gaia appliance or computer. We recommend that you place the package in `/var/log/upload`.
4. Exit `expert` mode.
5. In `clish`, register the file as an upgrade package. Run the command:
`add upgrade <version> package file <full path>`
6. Run:
`upgrade local <version>`
For example:
`upgrade local R75.40VS`
You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer `Yes`.
7. You are asked if you want to start the upgrade. Select `Yes`.
8. After the upgrade, type `OK` to reboot.

To upgrade using an ISO image on a DVD:

1. Download the Gaia ISO image from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
The upgrade package has a name similar to
`Check_Point_R75.40VS_Gaia.iso`
2. Burn the ISO file on a DVD.
3. Connect an external DVD drive to a USB socket on the appliance or computer.
4. Run
`upgrade cd`
5. You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer `Yes`.
6. You are asked if you want to start the upgrade. Select `Yes`.
The upgrade takes place.
7. After the upgrade, before rebooting, remove the DVD from the drive.
8. Type `OK` to reboot.

SecurePlatform to Gaia

You can upgrade from the SecurePlatform operating system to the Gaia operating system.

To upgrade a SecurePlatform appliance:

1. Upgrade product licenses to R75 or higher, and attach the licenses to the appliance.
2. Download the appliance upgrade package.
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R75.40VS.Gaia.tgz`
3. Connect to the SecurePlatform appliance from a Web browser to
`https://<appliance_ip_address>`.
4. In the login page, enter an administrator username and password.
5. Go to the **Upgrade** page.
6. Upload the appliance upgrade package to the appliance.
7. Ignore any warning messages.
8. Continue according to the on-screen instructions.
After the upgrade is complete, the appliance boots to Gaia.



Note - The connection to the SecurePlatform WebUI closes after Gaia is installed.

9. Install the Policy on the Security Gateway. This is highly recommended. The Security Gateway enforces the Initial Policy until you install the Policy:
 - a) Using SmartDashboard of the correct version, connect to the Security Management server.
 - b) Open the **General Properties** page of the Gateway object.
 - c) Click **Get** to update the **Platform** details.
 - d) Install the policy on the Gateway.

SecurePlatform to SecurePlatform

Use the WebUI to upgrade Security Gateways on appliances.

To upgrade appliances using the WebUI:

1. Open Internet Explorer and log in to the appliance.
2. Select **Appliance > Upgrade**.
3. Click **Check Point Download Center**.
The Internet browser opens to the Check Point Support Center.
4. Search for and download the R75.40VS upload package file.
5. In the WebUI, click **Upload upgrade package to appliance**.
The **Upload Package to Appliance** window opens.
6. Select the upgrade file:
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R76.SecurePlatform.tgz`
7. Click **Upload**.
8. Click **Start Upgrade**.
9. 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**.
10. 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**.
11. The **Current Upgrade File on Appliance** section displays the information of the current upgrade.
12. To begin the upgrade, click **Start**.

IP Appliances

Gaia to Gaia

Upgrade Requirements:

Ensure you have at least 6 GB of disk space available to do the upgrade.

- Using the WebUI: Check the space available for images in the **Maintenance > Image Management** page.
- Using the CLI: In expert mode, run the `df -h` command and check the available space in `/var/log`.

To upgrade using the WebUI:

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>) to the Gaia WebUI client computer. The upgrade package has a name similar to `gaia_upg_R75.40VS.tgz`
2. Connect to the Gaia WebUI from a Web browser to `https://<management_IP_address>`
3. In the WebUI go to the **Maintenance > Upgrade** page. (Ensure the **View Mode** is **Advanced**.)
4. Click **Upload**.
5. Browse to the location of the upgrade package.
6. After the package is uploaded, either click **Done** to add the package to the **Upgrade Packages** repository, or click **Upgrade**.
If you added the package to the package repository, select the package, and click **Upgrade**.
The package is extracted.
7. After the package is extracted, click **OK**.
A console window opens.
You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer **Yes**.

8. You are asked if you want to start the upgrade. Select **Yes**.
9. After the upgrade, click **Reboot**.

To upgrade using the upgrade package, with CLI:

You can upload the TGZ to the WebUI, and upgrade Gaia with CLI commands.

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R75.40VS.Gaia.tgz`
2. In the Gaia CLI, enter `expert` mode.
3. Use FTP, SCP or similar to transfer the upgrade package to the Gaia appliance or computer. We recommend that you place the package in `/var/log/upload`.
4. Exit `expert` mode.
5. In `clish`, register the file as an upgrade package. Run the command:
`add upgrade <version> package file <full path>`
6. Run:
`upgrade local <version>`
 For example:
`upgrade local R75.40VS`
 You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer **Yes**.
7. You are asked if you want to start the upgrade. Select **Yes**.
8. After the upgrade, type **OK** to reboot.

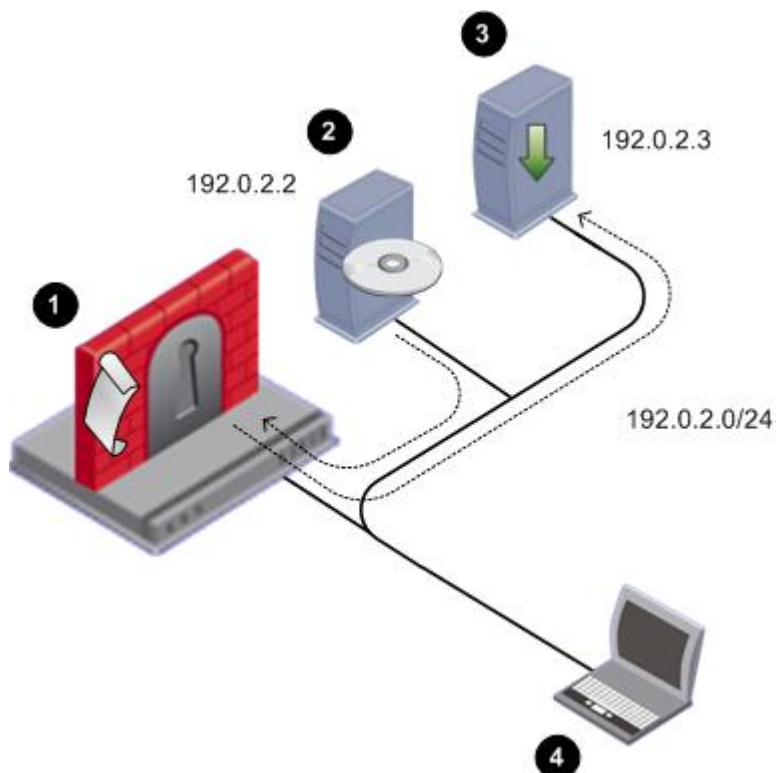
IPSO to Gaia

You can upgrade an IPSO IP Appliance Security Gateway to Gaia with R75.40VS. If necessary, you can do a rollback from Gaia to IPSO.

The IPSO and Check Point configuration is imported into Gaia, including the SIC trust settings.

Preparing for Upgrade

Set up this environment.



Item	
1	<p>IP Appliance with</p> <ul style="list-style-type: none"> • IPSO • IPSO to Gaia installation package or upgrade package.
2	<p>FTP Server with a Gaia ISO image mounted. The ISO is copied to the IP Appliance as part of the installation or upgrade process. The FTP server can be Linux-based or Windows-based ("Step 2: Putting the Gaia ISO on an FTP Server" on page 23).</p> <p>In this example, the FTP Server is at 192.0.2.2.</p>
3	<p>Optional: FTP Server used as a location for one or more of the following:</p> <ul style="list-style-type: none"> • Backup of IPSO and the Security Gateway configuration. (recommended) • A special SmartUpdate package that can be to distribute the IPSO to Gaia installation and upgrade package to multiple Security Gateways. • A special package that can be used to install or upgrade Security Gateways, one at a time, without having to answer any questions. This package is created using the answers supplied when running the installation and upgrade package. <p>You can use the same FTP server as for the Gaia ISO, or a different one. In this example, the FTP Server is at 192.0.2.3.</p>
4	<p>Computer with console access to the IP appliance and to the FTP server(s).</p> <p>Console access is recommended because it allows you to keep the connection to the IP Appliance throughout the installation or upgrade. If you connect via SSH you lose the connection after the IP Appliance reboots, and you will not be able to track the installation or upgrade progress.</p>

Upgrade Procedure Overview



Important - This is an overview of the steps. Detailed instructions follow.

Step 1: Get the IPSO to Gaia installation and upgrade package (tgz) and the Gaia ISO image.

Step 2: Put the Gaia ISO on an FTP server.

Step 3: Install the installation and upgrade package on the IP Appliance using Network Voyager or `clish`.

Step 4: Run the script:

- Clean install - `run-install-gaia`
- Upgrade - `run-upgrade-to-Gaia`

Step 5: Enter FTP server details and the ISO location. The script tests the FTP Server environment:

- a) Route to the FTP server
- b) Interface speed and duplex settings
- c) FTP access with the given credentials
- d) FTP access to the specified path
- e) Path contains the Gaia ISO and the user has Read/Write access to the directory
- f) Multiple simultaneous connections (>20) to the FTP server are allowed
- g) Timeout on FTP server is not too low
- h) FTP access to files downloaded by the Gaia boot manager

Step 6: Optional, but recommended: Enter data for an FTP server to hold IPSO system and configuration backup.

Step 7: Optional: Enter data to make a customized IPSO to Gaia upgrade package. Use this to upgrade multiple Security Gateways with SmartUpdate.

- a) Upgrade one Security Gateway with the standard IPSO to Gaia upgrade package. Enter the required data to create the special upgrade package.
- b) Upgrade all other Security Gateways simultaneously, using the special upgrade package, without more data. All IP Appliances must be able to access the same ftp servers as the first Security Gateway.

Step 8: Confirm your selections.

Step 9: The installation or upgrade package now runs automatically:

- a) If you made a backup package: The backup tar files are copied from the IP Appliance to the FTP server.
- b) If you made a customized installation or upgrade package: The package is copied from the IP Appliance to the FTP server.
- c) The Gaia image is copied from the FTP server to the IP Appliance.
- d) The Gaia image is installed.
- e) The Gaia boot manager is installed.
- f) The IP Appliance reboots.

You see the Gaia prompt on the IP Appliance.

Step 10: Make sure the upgrade succeeded.

Step 1: Getting the Upgrade Package and the Gaia Image

1. Download the Gaia packages for IP Appliance from the R75.40VS home page on the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

You will see two packages:

- Gaia ISO image
 - IPSO to Gaia installation and upgrade package. The file name is `Check_Point_Install_and_Upgrade_IPSO6.2_to_Gaia_R75.40VS.tgz`
2. Prepare the installation and upgrade packages:
Copy the packages to an FTP server, in a directory of your choice. Or transfer the packages by FTP to the IP Appliance.

Step 2: Putting the Gaia ISO on an FTP Server

Network Requirements



Important - High network traffic or large transfers (more than 10/100 Mbps links) can interfere with the FTP transfers for installation.

- Make sure the appliance can reach the FTP server.
- Make sure there is no Firewall which blocks incoming FTP requests from the appliance to the FTP server.
- Configure the FTP server to allow more than 100 (or an unlimited number of) concurrent connections.
- Make sure the Gaia ISO file is mounted on a directory to which the user has access permissions.

On a Linux-based FTP Server:

1. Upload the Gaia ISO file to the FTP server
2. On the FTP server, run:

```
mount -o loop -t iso9660 <ISO_filename> <mounting_destination_dir>
```

On a Windows-based FTP Server:

1. Upload the Gaia ISO file to the FTP server
2. Extract the Gaia ISO file to a folder on the FTP Server. Use 7-zip, Winzip, WinRAR or similar.
3. In the folder, run the file `copyrpms.bat`
This batch file copies installation files, to give a required workaround to Windows' inability to support soft links.
4. Give FTP credentials to the folder, so the folder can be accessed via FTP.

Step 3: Installing the Package on the IP Appliance

1. Log in to the IP Appliance using a console.
2. Run `clish`
3. Install the IPSO to Gaia installation and upgrade package on the IPSO appliance using `clish` or using Network Voyager (see the Network Voyager Reference Guide (http://supportcontent.checkpoint.com/documentation_download?ID=10293)).

To use `clish`:

- If the IPSO to Gaia package is on an FTP server, run:

```
add package media ftp addr <FTP_IP> user <uname> password <pass> name  
<full_path>/Check_Point_Upgrade_Package_R75.40VS.IPSO6.2_to_Gaia.tgz
```

Note - If using anonymous ftp, change `ftp` to `anonftp`.

- If the IPSO to Gaia package is on the IP Appliance, go to the directory where the package is located, and run the `clish` command:

```
add package media local name  
./Check_Point_Upgrade_Package_R75.40VS.IPSO6.2_to_Gaia.tgz
```

The installation and upgrade package is installed.

```
Trying to install package: ./package_name.tgz
Package Information --
Name       : IPSO to Gaia Upgrade
Version    : <version>
Release    : <Release>
Description: IPSO to Gaia Upgrade Package (<package_version>)
Package will be installed under: /opt
Package installed and activated successfully.
End of package installation.
```

The installation success message is Package installed and activated successfully.

The package is reported to be activated, but there are no background processes running.

4. Show the installed and active packages:

```
show package active
```

Name	Ver	Rel	Dir	Desc
{Check Point CPinfo }	10	00	/opt/CPinfo-10	{Check Point CPinfo}
{Check Point R70}	R70	00	/opt/CPsuite-R70	{Check Point R70}
{IPSO to Gaia Upgrade}	<ver>	<rel>	/opt/<package_name>	{IPSO to Gaia Upgrade Package (<upgrade_package_version>)}

5. Exit clish. Run: exit

Step 4: Running the Installation and Upgrade Script

1. Go to the location of the package

```
cd /opt/<package_name>/
```

2. To upgrade, run

```
./run-upgrade-to-Gaia
```

To do a clean installation, run

```
./run-install-Gaia
```

If you are upgrading multiple appliances from a special upgrade package that was previously saved, the installation or upgrade runs automatically. Continue with [Step 9](#) ("[Step 9: Upgrade Runs Automatically](#)" on page [103](#)).

If you are upgrading or installing one appliance, continue here.

The script runs. The following shows an upgrade. If you do a clean installation, the IPSO configuration is not transferred to Gaia.

```

Welcome to the IPSO to Gaia Install/Upgrade procedure.

Checking platform...OK
Checking IPSO OS version ...OK
Checking hostname ...
Checking your configuration
Summary:
    Errors:      0
    Warnings:    0
    Information: 14
Total Grade: 94
Details in file "/var/tmp/verify-IPSO-for-Gaia.msgs".

A newer version of this script may be available.
Contact the Check Point UserCenter at https://usercenter.checkpoint.com
and see SK66569.

Do you want to continue with the upgrade ? [y] y

=====
The following types of information are needed to prepare
your IPSO appliance for the upgrade:

- info about downloading the Gaia image.
- info about transferring the verification reports (optional).
- info about transferring an IPSO backup (optional).
- info about transferring a special upgrade package with your answers
(optional).

Answer the prompts for this info and then the upgrade is performed.

Hit 'Enter' to continue or Ctrl-C to exit

```

3. Supply the information for downloading the Gaia image



Note - If you have run the upgrade script before, the previously entered values are shown in square brackets []. Press **Enter** to accept the values, or type in the new values and press **Enter**.

Step 5: Verifying the FTP Server

Enter the requested FTP server data and the path to the Gaia installation file.

	Required Directory Value
If ISO is mounted to a non-FTP directory	Enter full path to ISO. A relative path or shortcut link will not work. Example: if /home/uname/gaia , ./gaia will not work.
If ISO is mounted to /var/ftp , and FTP user account is used to install	Enter path to ISO. A shortened path will work. Example: if /var/ftp/gaia , gaia will work.
If ISO is mounted to /var/ftp , and non-FTP user account is used to install	Enter full path to ISO. A relative path or shortcut link will not work.

The script runs some tests to verify the FTP environment. If errors are detected, correct the FTP server configuration and then instruct the program to verify the FTP environment again.

Here is an example of a successful test:

```

Info for download of the Gaia image:
Info for download of the Gaia image:
IP address of FTP server [192.0.2.2]:
User name [gwhite]:
Password [*****]:
Directory [/mnt/fiber292]:
Performing tests of access to FTP server and Gaia ISO
Checking route to 192.0.2.2 ... OK
Interface: eth-s4p1 speed 100M, duplex full
Checking FTP access with given credentials ... OK
Checking FTP access to /mnt/fiber292 ... OK
Checking /mnt/fiber292 is Gaia ISO ... Yes
Checking multiple simultaneous connections to 192.0.2.2 ... OK
Checking timeout to 192.0.2.2 ... OK
Checking FTP access to files downloaded by Gaia boot-manager
    system/ramdisk.pxe ... OK
    system/base/stage2.img ... OK

```

Step 6 (Optional, Recommended): Supplying Reports and Backup Server Information

The script will request details of the FTP server to store reports and backup data. The same path-rules apply here as in *Step 5* ("[Step 5: Verifying the FTP Server](#)" on page 25). The backup creates two tgz files, for:

- IPSO operating system configuration files, user directories, and log files.
- Security Gateway backup files.

Here is an example:

```

A complete backup of the IPSO system can performed
including system configuration, user home directories,
log files and files from packages.

Do you want to perform this backup ? [y]

Use IP address '192.0.2.2' and user 'root' for the backup? [n]

Details for transferring the IPSO Backup:
IP address of FTP server []: 192.0.2.3
User name []: ftp
Password []: ***
Directory []: /backupdir

Checking FTP access to 192.0.2.3 (it may take a minute) ... done

```

Step 7: (Optional): Supplying Special Package Server Information

Enter data of the destination FTP server for the special upgrade package. Enter a destination directory, with the same rules as in *Step 5* ("[Step 5: Verifying the FTP Server](#)" on page 25).

```

A package with your answers to the previous prompts can be created.
This package can be used on other IPSO gateways for
unattended conversion to Gaia.

Do you want to create such a package? [y]

Details for transferring the package with your answers:
IP address of FTP server [192.0.2.3]:
User name [ftp]:
Password [***]:
Directory [packagedir]:
Checking FTP access to 192.0.2.3 (it may take a minute) ... done

```

Step 8: Confirming Your Selections

You see a summary of all your answers.

Information for download of the Gaia image:

```
FTP Server IP Address = 192.0.2.2
FTP Server user name = root
Directory on FTP Server = /imagedir
```

Information for transferring the IPSO Backup:

```
FTP Server IP Address = 192.0.2.3
FTP Server user name = ftp
Directory on FTP Server = /backupdir
```

Information for transferring the package with your answers:

```
FTP Server IP Address = 192.0.2.3
FTP Server user name = ftp
Directory on FTP Server = /packagedir
```

Are these values correct? [y]

1. Click **n** to change the selections you made before, or type **y** to start the upgrade.

The backup file and the special upgrade package file, if you chose to create them, are created.

```
Writing values to file
Performing IPSO backup (file <ipso_backup_file_name>.tgz) ... done
Performing Check Point Security Gateway backup (file <Security
Gateway_backup_file_name>.tgz) ... done
Transferring IPSO and Check Point Security Gateway backup files ... done
Creating a package with your answers (<package_name>_AUTO.tgz) ... done
Transferring package with your answers ... done
Installing Gaia Boot Manager ... done
```

2. You have 30 seconds to abort. To stop the upgrade, press **Enter**.

```
IP appliance reboots in 30 seconds to complete the upgrade.
Hit 'Enter' to abort.
```



Important - If you want to make changes, press **Enter** now.

This stops the upgrade to Gaia. To complete the upgrade to Gaia, reboot the IP Appliance.

Step 9: Upgrade Runs Automatically

The upgrade runs unattended.

- The IP Appliance reboots.
- The Gaia Boot Manager runs.



Important - It is possible that after the reboot the system will show the Boot Manager prompt. To complete the upgrade, type **INSTALL** at the Boot Manager prompt, and provide the requested information. The upgrade should continue from this point.

- The Gaia image is installed.



- The IPSO and R75.40VS configuration is imported into Gaia, including the SIC trust settings.

- You now see the Gaia prompt.

Congratulations. Gaia and R75.40VS are installed on the IP Appliance.



Important - The HTTPS port for the WebUI is set to 443 after an installation or upgrade. To change this, you must use SmartDashboard > **Gateway Properties** > **Portal Settings**.

Step 10: Making Sure the Upgrade Succeeded

To check the Security Gateway configuration:

1. At the Gaia prompt, log in with your IPSO credentials.
The system logs you in to the expert mode. That is, you will be in `csch` or `bash` depending on how the original IPSO system was configured.
2. Type `clish` to enter clish.
3. Run `fw ver` to see the Security Gateway version information.
4. Run `fw stat` to confirm that the default policy is enforced.
5. Launch R75.40VS SmartDashboard.
6. In the Security Gateway object:
 - a) Click **Test SIC status**. SIC status should be **Trust Established**.
 - b) Change the version to R75.40VS.
 - c) Install a policy on the Security Gateway.

Rollback from Gaia to IPSO

You can roll back from Gaia to IPSO 6.2. You can also restore the Check Point Security Gateway and/or Security Management server configuration.

Before doing a rollback from Gaia to IPSO:

Make sure that:

1. The IPSO boot manager installer is available. Download it from the R75.40VS home page (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
2. An IPSO image is available. Put the IPSO image on an FTP server, and make sure that the FTP server is accessible from the Gaia IP Appliance.
3. A backup of the Check Point Security Gateway on the Gaia IP Appliance is available. Put the backup tar file on an FTP server, and make sure the FTP server is accessible from the Gaia IP Appliance.

To roll back from Gaia to IPSO:

1. At the Gaia command line prompt, login as the administrator.
2. Go to expert mode. Type `expert` and supply the credentials.
3. Download the IPSO boot manager installer `Check_Point_R75.40VS_Install_IPSOBootmanager.sh` from the R75.40VS home page on the Support Center.
4. Copy the IPSO boot manager installer to a location of your choice on the Gaia IP Appliance. For example, to `/var/tmp`.
5. Change file attributes to give executable permissions. Run
`chmod 777 Check_Point_R75.40VS_Install_IPSOBootmanager.sh`
6. Install the IPSO boot manager. At the command prompt run
`./Check_Point_R75.40VS_Install_IPSOBootmanager.sh /dev/hda`
The script asks if you want to roll back to
 1. IPSO 4.2
 2. IPSO 6.2
7. Choose 2
8. Type `reboot`
After the reboot, the system is running the IPSO boot manager.
9. At the `BOOTMGR>` prompt, install the IPSO image. Run
`install`

10. Enter this data:

- IP address of the IP Appliance.
- Default gateway of the IP Appliance.
- IP address of the FTP server with the IPSO image.
- User credentials.
- Directory path.
- Various configuration questions (about the chassis serial number, whether the system is part of a VRRP cluster, and whether IGMP and BGP are enabled).

The system automatically reboots into IPSO.

11. Configure the IP Appliance:

- Hostname
- New password for `admin`
- Enable the management port physical interface
- IP address for the management interface
- Default gateway

To restore the Check Point Security Gateway configuration:

1. Log in to the newly installed and configured IPSO IP Appliance as `admin`
2. Use FTP to transfer the backup archive file containing the Check Point Security Gateway to the IP Appliance, and then uncompress the archive. In the following example,
 - The name of the backup archive is `CP_archive_nms71_20101124.tgz`
 - The IP address of the FTP server containing the backup archive is `192.0.2.3`.

```
cd /tmp
ftp ftp://192.0.2.3>/pub/CP_archive_nms71_20101124.tgz
tar xzf /tmp/CP_archive_nms71_20101124.tgz
```

3. Restore the IPSO backup file using the `set restore` CLI commands. In the following example,
 - The IP address of the FTP server containing the IPSO backup file is `192.0.2.2`
 - The IPSO backup file is in the `pub` directory.



Important - If the backup contains IPSO and Check Point configuration data, the Check Point packages must be installed first before trying to restore the backup; otherwise the restore will fail.

```
clish
set restore remote ftp-site ftp://192.0.2.2
set restore remote ftp-user <username e.g. anonymous>
set restore remote ftp-pass <password>
set restore remote ftp-dir pub
set restore remote filename i2g_backup_<hostname and timestamp>.tgz
```

IPSO automatically reboots.

4. Log out.
5. Log in as `admin`.

Verify the configuration has been restored.

Upgrading Security Gateways on Open Servers

Before you upgrade:

It is recommended to back up your current configuration (see "[Backing Up](#)" on page 66).

Gaia to Gaia

Upgrade Requirements:

Ensure you have at least 6 GB of disk space available to do the upgrade.

- Using the WebUI: Check the space available for images in the **Maintenance > Image Management** page.
- Using the CLI: In expert mode, run the `df -h` command and check the available space in `/var/log`.

To upgrade using the WebUI:

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>) to the Gaia WebUI client computer. The upgrade package has a name similar to `gaia_upg_R75.40VS.tgz`
2. Connect to the Gaia WebUI from a Web browser to `https://<management_IP_address>`
3. In the WebUI go to the **Maintenance > Upgrade** page. (Ensure the **View Mode** is **Advanced**.)
4. Click **Upload**.
5. Browse to the location of the upgrade package.
6. After the package is uploaded, either click **Done** to add the package to the **Upgrade Packages** repository, or click **Upgrade**.
If you added the package to the package repository, select the package, and click **Upgrade**.
The package is extracted.
7. After the package is extracted, click **OK**.
A console window opens.
You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer **Yes**.
8. You are asked if you want to start the upgrade. Select **Yes**.
9. After the upgrade, click **Reboot**.

To upgrade using the upgrade package, with CLI:

You can upload the TGZ to the WebUI, and upgrade Gaia with CLI commands.

1. Download the Gaia upgrade package from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R75.40VS.Gaia.tgz`
2. In the Gaia CLI, enter `expert` mode.
3. Use FTP, SCP or similar to transfer the upgrade package to the Gaia appliance or computer. We recommend that you place the package in `/var/log/upload`.
4. Exit `expert` mode.
5. In `clish`, register the file as an upgrade package. Run the command:
`add upgrade <version> package file <full path>`
6. Run:
`upgrade local <version>`
For example:
`upgrade local R75.40VS`
You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer **Yes**.
7. You are asked if you want to start the upgrade. Select **Yes**.
8. After the upgrade, type **OK** to reboot.

To upgrade using an ISO image on a DVD:

1. Download the Gaia ISO image from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
The upgrade package has a name similar to `Check_Point_R75.40VS_Gaia.iso`
2. Burn the ISO file on a DVD.
3. Connect an external DVD drive to a USB socket on the appliance or computer.
4. Run
`upgrade cd`

5. You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer *Yes*.
6. You are asked if you want to start the upgrade. Select *Yes*.
The upgrade takes place.
7. After the upgrade, before rebooting, remove the DVD from the drive.
8. Type *OK* to reboot.

SecurePlatform to Gaia

You can upgrade Security Gateways on SecurePlatform to R75.40VS Security Gateways on Gaia.

To upgrade an open server using the DVD:

1. Upgrade product licenses to R75 or higher, and attach the licenses to the computer.
2. Connect a DVD drive to the USB port on the computer.
3. Run: `patch add cd`
4. Select the Gaia upgrade package.
5. Confirm the MD5 checksum.
6. If relevant, when prompted, create a backup image for automatic revert.
7. After extracting files, the Installation program opens.
8. Accept the license agreement.
9. Select **upgrade**.
10. Configure your contract options.
You can also continue without contract information and configure it later using SmartUpdate.
11. Select a source for the upgrade utilities.
Wait for the pre-upgrade verifier to complete successfully.
12. Select **Stop Check Point processes**.
13. Select **Upgrade installed products**, or **upgrade installed products and add new products**, and confirm.
14. Wait while the required installation files are extracted.
 - a) Part one of the upgrade procedure saves data and upgrades the operating system.
 - b) Part two upgrades Check Point products.
15. After the upgrade completes successfully, remove the DVD from the drive.
16. Restart when prompted.
17. Install the Policy on the Security Gateway. This is highly recommended. The Security Gateway enforces the Initial Policy until you install the Policy:
 - a) Using SmartDashboard of the correct version, connect to the Security Management server.
 - b) Open the **General Properties** page of the Gateway object.
 - c) Click **Get** to update the **Platform** details.
 - d) Install the policy on the Gateway.

o upgrade a SecurePlatform Open Server using the WebUI:

1. Open Internet Explorer and log in to the SecurePlatform WebUI.
2. Select **Device > Upgrade**.
3. Click **Check Point Download Center**.
The Internet browser opens to the Check Point Support Center.
4. Search for and download the R75.40VS file for upgrades via the WebUI.
5. Click **Browse** and select the upgrade file:
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R76.Gaia.tgz`
6. Click **Upload package to device**.
The package is uploaded to the SecurePlatform computer.
After the **Upgrade Status** shows that the *Uploading* is *Completed* you can start the upgrade.

7. **Recommended:** In the **Safe Upgrade** section, click **Save snapshot of the current system before the upgrade**. The snapshot is used to revert the system if the upgrade is not successful.
8. Click **Start Upgrade**.
Follow the **Upgrade Status**. After the upgrade, the computer automatically reboots.



Note - The connection to the SecurePlatform WebUI closes after Gaia is installed.

9. Install the Policy on the Security Gateway. This is highly recommended. The Security Gateway enforces the Initial Policy until you install the Policy:
 - a) Using SmartDashboard of the correct version, connect to the Security Management server.
 - b) Open the **General Properties** page of the Gateway object.
 - c) Click **Get** to update the **Platform** details.
 - d) Install the policy on the Gateway.

SecurePlatform to SecurePlatform

Use this procedure to upgrade a SecurePlatform installation on the same computer. Upgrade the operating system and the installed products.

To upgrade a SecurePlatform Open Server using a DVD:

1. Insert R75.40VS DVD into the drive.
2. At the command prompt, enter: `patch add cd`
3. Select **SecurePlatform R75.40VS Upgrade Package** (`CPspupgrade_<version_number>.tgz`).
4. Press **y** to accept the checksum calculation.
5. Optional: When prompted, create a backup image so that you can restore the old version.



Note - Creating the snapshot image can take a long time. Check Point products are stopped during this time.

6. Press **N** at the welcome message.
7. Press **Y** to accept the license agreement.
8. In the next window, select **Upgrade** and then press **N**.
9. In the next window, press **N** to continue.
10. If prompted to download or import a valid support contract, select **Continue without contract information**. Press **N** to continue.
11. If a message shows that says your gateway is not eligible for upgrade, press **N** to continue.
You can safely ignore this message and use SmartUpdate to update your service contract later.
12. In the next window, select **Download most updated files**.
13. In the **Pre-Upgrade Verification Results** window, press **N** to continue.
If the Pre-Upgrade Verification fails, do the suggested steps to correct the problem. Start this procedure again from step 2.
14. When prompted, select **Stop Check Point processes** and press **N** to continue.
15. When prompted, select **Upgrade installed products** and press **N** to continue.
16. In the **Validation** window, press **N**.
17. When the upgrade completes successfully, restart the computer.

To upgrade a SecurePlatform Open Server using the WebUI:

1. Open Internet Explorer and log in to the SecurePlatform WebUI.
2. Select **Device > Upgrade**.
3. Click **Check Point Download Center**.
The Internet browser opens to the Check Point Support Center.
4. Search for and download the R75.40VS file for upgrades via the WebUI.
5. Click **Browse** and select the upgrade file:
`Check_Point_Upgrade_WEBUI_and_SmartUpdate_R75.40VS.SecurePlatform.tgz`
6. Click **Upload package to device**.

The package is uploaded to the SecurePlatform computer.

After the **Upgrade Status** shows that the *Uploading is Completed* you can start the upgrade.

7. **Recommended:** In the **Safe Upgrade** section, click **Save snapshot of the current system before the upgrade**. The snapshot is used to revert the system if the upgrade is not successful.

Your browser will automatically try to perform the first login immediately after the upgrade. To allow this, do not close the browser window or browse to another page.

8. Click **Start Upgrade**.

Follow the **Upgrade Status**. After the upgrade, the computer automatically reboots.

9. Install the Policy on the Security Gateway. This is highly recommended. The Security Gateway enforces the Initial Policy until you install the Policy:
 - a) Using SmartDashboard of the correct version, connect to the Security Management server.
 - b) Open the **General Properties** page of the Gateway object.
 - c) Click **Get** to update the **Platform** details.
 - d) Install the policy on the Gateway.

Windows

This section describes the upgrade process using the R75.40VS Installation DVD.

To upgrade a gateway in a Windows platform:

1. Insert the R75.40VS 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 R75.40VS 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 R75.40VS.
3. Install Policy on the upgraded gateway.

If you need to, you can restore the previous configuration (see "[Restoring Other Platforms](#)" on page 72).

Upgrading a VSX Gateway

The `vsx_util` command upgrades a VSX Gateway from an earlier version to R75.40VS.



Important - The `vsx_util` command cannot modify the management database if the database is locked. Make sure that no other administrators are connected to the management server. For a Multi-Domain Server configuration, make sure that no other administrators are connected to domains.

To upgrade a VSX Gateway to R75.40VS:

1. Install R75.40VS on the VSX Gateway ("[Installing VSX Gateways](#)" on page 44).
2. Reboot the VSX Gateway.
3. Close SmartDashboard.
4. Upgrade the VSX Gateways in the Security Management server.
 - a) From the Security Management server CLI, run `vsx_util upgrade`.
 - b) Do the on-screen instructions.
5. Push the configuration to the VSX Gateways. Do these steps for each VSX Gateway or cluster member.
 - a) Run `vsx_util reconfigure`.
 - b) Do the on-screen instructions.

The existing security policy is installed and configured on the upgraded VSX Gateway and this message is shown:

```
Reconfigure module operation completed successfully
```
 - c) Reboot the VSX Gateway.



Note - In a Multi-Domain Server environment, the operation skips any Domain Management Servers locked by an administrator. For all locked Domain Management Servers, when they are available, do steps 4 and 5 and then resume the upgrade.

6. Install the necessary licenses.

Upgrading Standalone Full High Availability

Full High Availability: The server and the gateway are in a standalone configuration and each has High Availability to a second standalone machine. If there is a failure, the server and the gateway failover to the secondary machine. In the standalone configuration the server and gateway can failover independently of each other. For example, if only the server has an issue, only that server fails over. There is no effect on the gateway in the standalone configuration.

To upgrade Full High Availability for cluster members in standalone configurations, there are different options:

- Upgrade one machine and synchronize the second machine with minimal downtime.
- Upgrade with a clean installation on one machine and synchronize the second machine with system downtime.

Upgrading with Minimal Downtime

You can do a Full High Availability upgrade with minimal downtime to the cluster members.

To upgrade Full High Availability with minimal downtime:

1. Make sure the primary cluster member is active and the secondary is standby: check the status of the members.
2. Start failover to the second cluster member.

The secondary cluster member processes all the traffic.
3. Log in with SmartDashboard to the management server of the secondary cluster member.
4. Click **Change to Active**.
5. Configure the secondary cluster member to be the active management server.



Note - We recommend to export the database using the Upgrade tools (on page 65).

6. Upgrade the primary cluster member to the appropriate version.
7. Log in with SmartDashboard to the management server of the primary cluster member.

Make sure version of the SmartDashboard is the same as the server.
8. Upgrade the version of the object to the new version.
9. Install the policy on the cluster object.

The primary cluster member processes all the traffic.



Note - Make sure that the **For Gateway Clusters install on all the members** option is cleared. Selecting this option causes the installation to fail.

10. Upgrade the secondary cluster member to the appropriate version.
11. Synchronize for management High Availability.

Upgrading with a Clean Installation

You can do a Full High Availability upgrade with a clean installation on the secondary cluster member and synchronize the primary cluster member. This type of upgrade causes downtime to the cluster members.

To upgrade Full High Availability with a clean installation:

1. Make sure the primary cluster member is active and the secondary is standby: check the status of the members.
2. Start failover to the second cluster member.
The secondary cluster member processes all the traffic.
3. Log in with SmartDashboard to the management server of the secondary cluster member.
4. Click **Change to Active**.
5. Configure the secondary cluster member to be the active management server.



Note - We recommend to export the database using the Upgrade tools (on page 65).

6. Upgrade the primary cluster member to the appropriate version.
7. Log in with SmartDashboard to the management server of the primary cluster member.
Make sure version of the SmartDashboard is the same as the server.
8. Upgrade the version of the object to the new version.
9. Install the policy on the cluster object.
The primary cluster member processes all the traffic.



Note - Make sure that the **For Gateway Clusters install on all the members** option is cleared. Selecting this option causes the installation to fail.

10. Install the secondary member.
11. From SmartDashboard, configure the cluster object.
 - a) Change the secondary details (if necessary).
 - b) Establish SIC.
12. Synchronize for management High Availability.
The primary management database synchronizes to the secondary management database.

Upgrading Clusters

If the appliance to upgrade was not the primary member of a cluster before, export its database before you upgrade. If it was the primary member before, you do not have to do this.

To upgrade an appliance and add it to a cluster:

1. If the appliance was not the primary member of a cluster, export the Security Management server database ("[Exporting the Database](#)" on page 146).
2. Upgrade the appliance ("[Upgrading Standalone Appliances](#)" on page 76).
3. If the appliance was not the primary member of a cluster, import the database ("[Importing the Database](#)" on page 147).
4. Using the WebUI, on the **Cluster** page, configure the appliance to be the primary member of a new cluster.

5. Connect a second appliance to the network.
 - If the second appliance is based on an earlier version: get the relevant upgrade package from the Download Center, save it to a USB stick, and reinstall the appliance as a secondary cluster member.
 - If the second appliance is upgraded: run the first-time wizard and select **Secondary Cluster Member**.

Chapter 7

Upgrading Multi-Domain Security Management

In This Chapter

Upgrade Multi-Domain Security Management Tools	113
Upgrade Best Practices	119
Upgrading a High Availability Deployment	124
Restarting Domain Management Servers	126
Restoring Your Original Environment	126
Removing Earlier Version Multi-Domain Server Installations	127
Changing the Multi-Domain Server Interfaces	127
IPS with Multi-Domain Security Management	128

This section includes procedures for upgrading Multi-Domain Security Management to R75.40VS.

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, `UnixInstallScript`, 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.

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 **Export current Multi-Domain Server** option in `UnixInstallScript` 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.

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.



Note - Before you migrate, delete all secondary management objects from the primary Security Management server.

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:

Install from CD:

```
# gtar xvfz /mnt/cdrom/linux/upgrade_tools/linux/pl_upgrade_tools.tgz -C
/var/opt/export_tools
```

Install from DVD:

```
# gtar xvfz /mnt/cdrom/Linux/linux/upgrade_tools/linux/pl_upgrade_tools.tgz -C
/var/opt/export_tools
```

The database to import is the database belonging to the primary Domain Management Server/Security Management server. Before you import, make sure that the database is synchronized.

If you want to migrate your current High Availability environment to a Domain Management Server High Availability on a different Multi-Domain Server, export the database. Then continue with a High Availability deployment (see the *High Availability* chapter in the *R75.40VS Multi-Domain Security Management Administration Guide*) (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

To export the management database:

```
<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.
- Run a "log switch" immediately before you export the Domain Management Server to export the log files.

Example:

```
# cd /opt/CPsuite-R75.40VS/fw1/bin/upgrade_tools/
# mdsenv dms1
# migrate export -l /var/opt/dms1_exported.tgz
```

This example assumes that you are upgrading using the distribution CD or DVD.

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.

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, it is a different procedure ("[Completing Migration to a New IP Address](#)" on page 148).

Syntax:

```
cma_migrate <source management tgz> <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>) 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 - You can run `mdscmd migratecma` to import files to a Domain Management Server, or you can use the SmartDomain Manager.

To run the `cma_migrate` utility from the SmartDomain Manager:

1. Right-click a Domain Management Server and select **Options > Import Domain Management Server**.
2. When you enter the path to the exported database file, include the name of the exported database file at the end of the path.

cma_migrate and Certificates

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 more about CA on Multi-Domain Security Management, see 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.



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`.

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.

Syntax:

```
migrate_global_policies <path to exported tgz>
```

<path to exported tgz>: specifies the **fully qualified** path to the archive file created by the `migrate export` command.

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 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.

Syntax `mds_backup [-g -b {-d <target dir name>} -v -h]`

Parameter	Description
<code>-g</code>	Executes without prompting to disconnect GUI clients.
<code>-b</code>	Batch mode - executes without asking anything (<code>-g</code> is implied).
<code>-d</code>	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.
<code>-v</code>	Verbose mode - lists all files to be backed up, but do not perform the backup operation.
<code>-l</code>	Exclude logs from the backup.
<code>-h</code>	Help - displays help text.

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.



Note - The `mds_restore` command must use the script that was created in the directory into which the backup file was created.

Syntax `./mds_restore <backup file>`



Important - In Gaia, you have to run this command in expert mode and in the same directory as the backup file itself.

Upgrade Best Practices

Multi-Domain Server In-Place Upgrade

The in-place upgrade process takes place on an existing Multi-Domain Server machine. The Multi-Domain Server, together with all Domain Management Servers, are upgraded in one procedure.



Note - When upgrading Multi-Domain Security Management, all SmartUpdate packages on the Multi-Domain Server (excluding Edge firmware packages) are deleted from the SmartUpdate Repository.

Before doing an in-place upgrade to R75.40VS:

1. Run the **Pre-upgrade verification only** option from `UnixInstallScript`. In a multi-Multi-Domain Server environment, do this on all Multi-Domain Servers.
2. Make the changes required by the pre-upgrade verification, and if you have High Availability, start synchronizations.
3. Test your changes:
 - 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. Run `mds_backup` to back up your system.

Gaia to Gaia

Upgrade Requirements:

Ensure you have at least 6 GB of disk space available to do the upgrade.

- Using the WebUI: Check the space available for images in the **Maintenance > Image Management** page.
- Using the CLI: In expert mode, run the `df -h` command and check the available space in `/var/log`.

To upgrade using an ISO image on a DVD:

1. Download the Gaia ISO image from the Check Point Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
The upgrade package has a name similar to `Check_Point_R75.40VS_Gaia.iso`
2. Burn the ISO file on a DVD.
3. Connect an external DVD drive to a USB socket on the appliance or computer.
4. Run
`upgrade cd`
5. You are asked if you want to save a snapshot of the system before upgrade. We recommend that you answer `Yes`.
6. You are asked if you want to start the upgrade. Select `Yes`.
The upgrade takes place.
7. After the upgrade, before rebooting, remove the DVD from the drive.
8. Type `OK` to reboot.

SecurePlatform to SecurePlatform

Use a DVD to upgrade Multi-Domain Server on SecurePlatform.

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.

To upgrade Multi-Domain Server on SecurePlatform:

1. If necessary, create an upgrade DVD and do these steps:
 - a) Download the R75.40VS Multi-Domain Server ISO file (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).
 - b) Burn the ISO file on a DVD.
 - c) Connect an external DVD drive to the USB socket on the server.

Make sure that the DVD with the R75.40VS ISO file is in the DVD drive.
2. Log in to SecurePlatform (**expert** mode is necessary only for Smart-1 appliances).
3. Run: `patch add cd`
The SecurePlatform upgrade package is installed.
4. Select the **SecurePlatform R75.40VS Upgrade Package** and press **Enter**.
5. Type **yes** to verify the MD5 checksum.
6. If necessary, type **yes** to do a Safe Upgrade.
Multi-Domain Server is upgraded to R75.40VS.
7. Remove the DVD from the drive.
8. Restart the server.
9. Run this command to update the version of all Domain Management and Log Server objects located on this server: `/opt/CPmds-R75.40VS/scripts/mds_fix_cmas_clms_version -c ALL -n <Multi-Domain Server name>`

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 `UnixInstallScript` 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

Before you start the upgrade, consider these points:

- Make sure 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.
- 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.

Exporting a Multi-Domain Server Deployment

After you begin to export from the source Multi-Domain Server, avoid making configuration changes on that Multi-Domain Server. Changes made after export starts are not included in the tgz file. You will need to make such changes manually on the target after you complete the upgrade.

To export a Multi-Domain Server to a TGZ file:

1. Mount the Multi-Domain installation media to a subdirectory.
2. Change the directory to the mounted directory.
3. Browse to the directory which has the name of the operating system of your Multi-Domain Server.
4. Run: `UnixInstallScript`
5. Select the **Export current Multi-Domain Server** option.
6. Follow the instructions on the screen.
7. When prompted, choose whether or not you wish to save the log files to the tgz file.



Note - Exporting log files can 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. Run one of these:

- `mds_backup`
 - `UnixInstallScript` and select 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 same version as the existing Multi-Domain Server.
- 

Note - Make sure the target machine is 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`.
- 

Important - In Gaia, run this command from expert mode and exit after running the command. You must run this command from the folder that contains the backup file.

 1. Go to the folder that contains the backup file.
 2. Enter `./mds_restore`
4. If your target machine and the source machine have different IP addresses, change the IP Address of the restored Multi-Domain Server to the new IP address. If your target machine and the source machine have different interface names (for example: **hme0** and **hme1**), change the interface of the restored Multi-Domain Server to the new interface name.
 5. Test to confirm that the replication is successful:
 - a) Start the Multi-Domain Server.
 - b) Make sure 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. Stop the Multi-Domain Server on the target machine and upgrade.
 7. Run: `Container2MultiDomain`.
 8. Start the Multi-Domain Server.

Gradual Upgrade to Another Computer

In a gradual upgrade, you export Domain Management Servers one at a time from the source Multi-Domain Server to a target Multi-Domain Server of the latest version.

The gradual upgrade does not keep all data.

Data Not Exported	To get this data in the new environment:
Multi-Domain Security Management Administrators and management consoles	Redefine and reassign to Domains after the upgrade.
Policy assignment to Domains	Assign policies to Domains after the upgrade.
Status of global communities	Run: <code>mdsenv; fwm mds rebuild_global_communities_status all</code>

To run 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. Run: `migrate export`
The migrate export command exports the Domain Management Server database to a .tgz file on the Multi-Domain Server. It also transfers the licenses for the Domain Management Server.
4. Run: `cma_migrate <src tgz> <FWDIR on target>`
5. The `cma_migrate` (on page 116) command imports the Domain Management Server database (using the tgz created by the migrate export command) to the Multi-Domain Server.

6. Start the Domain Management Server.
7. Run: `mdsenv; mdsstart`
8. 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 Server to Domain Management Server

This section describes how to migrate the Security Management Server product of a standalone deployment to a Domain Management Server. Then you manage the former-standalone computer as a Security Gateway only from the Domain Management Server.



Note - To later undo the separation of the Security Management Server and Security Gateway on the standalone, back up the standalone computer before you migrate.

Before migrating:

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 computer already has 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 gateway participates in a VPN community, remove it from the community and erase its certificate. Note these changes, to undo them after the migration.
6. Save and close SmartDashboard. Do not install policy.

To migrate the management database to the Domain Management Server:

1. Go to the fully qualified path of the migrate export command.
2. Run: `migrate export [-l] <output file>`
3. Create a new Domain Management Server on the Multi-Domain Server, but do not start it.
4. 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.



Note - To run the `cma_migrate` utility from the SmartDomain Manager, right-click a Domain Management Server and select **Options > Import Domain Management Server**. In the **Import** window, when you enter the path to the exported database file, include the name of the exported database file at the end of the path.

You can also run `mdscmd migratecma` to import files to a Domain Management Server.

5. Restart the Domain Management Server and launch SmartDashboard.
6. 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 Server.
7. Edit the Primary Management Object and remove all interfaces (**Network Object > Topology > Remove**).
8. Create an object for the Security 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.
 - Enabled the installed Software Blades.
 - If the Security Gateway belonged to a VPN Community, add it back.
 - Do not initialize communication.
9. Run Domain Management Server on the primary management object and, in each location, consider changing to the new gateway object.
10. Install the policy on all other gateways, not the new one. If you see warning messages about this gateway because it is not yet configured, ignore them.
11. Uninstall the standalone deployment.
12. Install a Security Gateway on the previous standalone machine.
13. From the Domain Management Server SmartDashboard, edit the gateway object, define its topology, and establish trust between the Domain Management Server and the Security Gateway.
14. Install the policy on the Security Gateway.

Upgrading a High Availability Deployment



Note - The current version supports multiple Domain Management Servers for each Domain.

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.

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 `UnixInstallScript`. Upgrade the primary Multi-Domain Server only after you have fixed all errors and reviewed all warnings for all Multi-Domain Servers.

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, make sure they are upgraded to the same version.

To upgrade multiple Multi-Domain Servers:

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.

Upgrading Multi-Domain Servers and Domain Management Servers

To upgrade Multi-Domain Server and Domain Management Server:

1. Run pre-upgrade verification for all Multi-Domain Servers.
2. If a change to the global database is necessary, synchronize the Multi-Domain Servers immediately after making these changes. Update the database on one Multi-Domain Server and start synchronization. The other Multi-Domain Servers will get the database changes automatically.
3. If global database changes affect a global policy assigned to a Domain, assign the global policy again to all affected Domains.
4. If the verification command finds Domain Management Server level errors (for example, gateways that are no longer supported by the new version):
 - a) Make the required changes on the Active Domain Management Server.
 - b) Synchronize the Active Domain Management Server with all Standby Domain Management Servers.
5. If a Domain has Log Servers:
 - a) In the Domain SmartDashboard, manually install the new database: select **Policy > Install Database**.
 - b) Select all Log Servers.

- c) 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.

Change the active Multi-Domain Server and Domain Management Server, and then synchronize the Standby computers.

Updating Objects in the Domain Management Server Databases

After upgrading the Multi-Domain Servers and Domain Management Servers, you must update the objects in all Domain Management Server databases. This is necessary because upgrade does not automatically update the object versions attribute in the databases. If you do not manually update the objects, the standby Domain Management Servers and Log Servers will show the outdated versions.

Update the objects with these steps on each Multi-Domain Server.

To update Domain Management Server and Domain Log Server objects:

1. Make sure that all Domain Management Servers are up: `mdsstat`
If a Domain Management Server is down, resolve the issue, and start the Domain Management Server:
`mds_startcustomer`
2. Go to the top-level CLI: `mdsenv`
3. Run: `$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL`
Optional: update one Domain Management Server or Domain Log Server at a time with this command:
`$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n <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.

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 databases, 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: `mdsstart`

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.

To restore your original environment:

1. Remove the new installation:
 - a) For a **SecurePlatform** server, manually remove the new software packages. It can be easier to remove all installed Check Point packages and install the original version.
 - b) For all other servers, run the `mds_remove` utility.
2. Run the `mds_restore` command with the backup file.
3. The original environment is restored.



Important - In Gaia, run the `mds_restore` command from expert mode and exit after running the command. You must run this command from the folder that contains the backup file.

1. Go to the folder that contains the backup file.
2. Enter `./mds_restore`

Removing Earlier Version Multi-Domain Server Installations

After upgrading your Multi-Domain Server to the latest version, earlier version files are not automatically deleted from the disk. This lets you revert to the old version in the event there are problems with the upgrade. These files can take up a lot of disk space and cause performance degradation.

After you complete testing your upgrade, we recommend that remove these earlier version files. You can use the `mds_remove_version` tool to automatically remove old installations with no effect on the installed version.

To remove old installations:

1. Backup your system.
2. Download the tool.
3. Copy the `mds_remove_version.sh` script to the Multi-Domain Server
4. Run `mds_remove_version.sh`.
There are no parameters or arguments.
5. Confirm when prompted.
6. Make sure that the old files were successfully removed.



Important - This tool removes major releases and all minor releases installed over a major release. For example, if R71.50 is installed on your Multi-Domain Server, and you upgraded to R75.40VS, the tool removes R71 and R71.50 files.

Changing the Multi-Domain Server Interfaces

If your target machine and the source machine have different IP addresses, follow the steps listed below 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.

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 R75.40VS, 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**.
- If you manage IPS globally, you must reassign the global policy before installing the policy on Security Gateways.
- 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.

See the Global Policy Chapter in the *R75.40VS Multi-Domain Security Management Administration Guide* (<http://supportcontent.checkpoint.com/solutions?id=sk76540>) for detailed information.

Chapter 8

Upgrading with SmartUpdate

In This Chapter

Introducing SmartUpdate	129
Understanding SmartUpdate	130
SmartUpdate - Seeing it for the First Time	131
Common Operations	131
Upgrading Packages	132
Managing Licenses	135
Service Contracts	140
Generating CPInfo	140
The SmartUpdate Command Line	141

Introducing SmartUpdate

SmartUpdate automatically distributes applications and updates for Check Point and OPSEC Certified products, and manages product licenses. It provides a centralized means to guarantee that Internet security throughout the enterprise network is always up to date. SmartUpdate turns time-consuming tasks that could otherwise be performed only by experts into simple point and click operations.

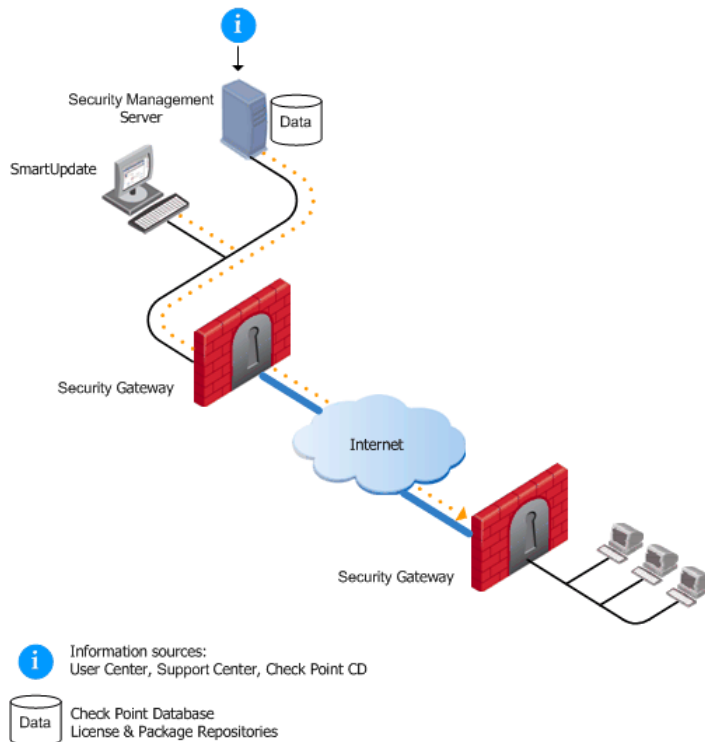
SmartUpdate extends your organization's ability to provide centralized policy management across enterprise-wide deployments. SmartUpdate can deliver automated software and license updates to hundreds of distributed security gateways from a single management console. SmartUpdate ensures security deployments are always up-to-date by enforcing the most current security software. This provides greater control and efficiency while dramatically decreasing maintenance costs of managing global security installations.

SmartUpdate enables remote upgrade, installation and license management to be performed *securely* and *easily*. A system administrator can monitor and manage remote gateways from a central location, and decide whether there is a need for software upgrade, new installations and license modification. It is possible to remotely upgrade:

- Check Point Security Gateways
- Hotfixes, Hotfix Accumulators (HFAs) and patches
- Third party OPSEC applications
- UTM-1 Edge
- Check Point IPSO Operating System
- SecurePlatform

All operations that can be performed via SmartUpdate can also be done via the command line interface. See The SmartUpdate Command Line (on page [141](#)) for more information.

Understanding SmartUpdate



SmartUpdate installs two *repositories* on the Security Management server:

- **License & Contract Repository**, which is stored on all platforms in the directory `$FWDIR\conf\`.
- **Package Repository**, which is stored:
 - on Windows machines in `C:\SUroot`.
 - on UNIX machines in `/var/suroot`.

The **Package Repository** requires a separate license, in addition to the license for the Security Management server. This license should stipulate the number of nodes that can be managed in the **Package Repository**.

Packages and licenses are loaded into these repositories from several sources:

- the Download Center web site (packages)
- the Check Point DVD (packages)
- the User Center (licenses)
- by importing a file (packages and licenses)
- by running the `cplic` command line

Of the many processes that run on the Check Point Security Gateways distributed across the corporate network, two in particular are used for SmartUpdate. Upgrade operations require the `cprid` daemon, and license operations use the `cpd` daemon. These processes listen and wait for the information to be summoned by the Security Management server.

From a remote location, an administrator logged into the Security Management server initiates operations using the SmartUpdate tool. The Security Management server makes contact with the Check Point Security Gateways via the processes that are running on these gateways in order to execute the operations initiated by the system administrator (e.g., attach a license, or upload an upgrade). Information is taken from the repositories on the Security Management server. For instance, if a new installation is being initiated, the information is retrieved from the **Package Repository**; if a new license is being attached to remote gateway, information is retrieved from the **License & Contract Repository**.

This entire process is Secure Initial Communication (SIC) based, and therefore completely secure.

SmartUpdate - Seeing it for the First Time

SmartUpdate has two tabs:

- **Packages** tab shows the packages and Operating Systems installed on the Check Point Security Gateways managed by the Security Management server. Operations that relate to packages can only be performed in the **Packages** tab.
- **Licenses** tab shows the licenses on the managed Check Point Security Gateways. Operations that relate to licenses can only be performed in the **Licenses** tab.

These tabs are divided into a tree structure that displays the packages installed and the licenses attached to each managed Security Gateway.

The tree has three levels:

- Root level shows the name of the Security Management server to which the GUI is connected.
- Second level shows the names of the Check Point Security Gateways configured in SmartDashboard.
- Third level shows the Check Point packages (in the **Packages** tab) or installed licenses (in the **Licenses** tab) on the Check Point Security Gateway.

Additionally, the following panes can be displayed:

- **Package Repository** - shows all the packages available for installation. To view this pane, select **Packages > View Repository**.
- **License & Contract Repository** - shows all licenses (attached or unattached). To view this pane, select **Licenses > View Repository**.
- **Operation Status** - shows past and current SmartUpdate operations. To view this pane, select **Operations > View Status**. In this pane you can read about:
 - Operations performed (e.g., Installing package <X> on Gateway <Y>, or Attaching license <L> to Gateway <Y>).
 - The status of the operation being performed, throughout all the stages of its development (for instance, operation started, or a warning).
 - A progress indicator.
 - The time that the operation takes to complete.

Common Operations

Drag and Drop - Packages and licenses can be dragged and dropped from the Repositories onto the Security Gateways in the **Package/Licenses Management** tree. This drag and drop operation will invoke the **distribute** or **attach** operation respectively.

Search - To search for a text string: select **Tools > Find**. In **Find what**, enter a string to search for. Select search location: **Network Objects License & Contract** tab or **Package Repository**.

Sort - To sort in ascending or descending order, click the column title in the **Licenses** or **Packages** tab.

Expand or Collapse - To expand or collapse the Check Point Security Gateways tree structure, right-click on the tree root and choose **Expand/Collapse**.

Change view - To change the Repository view, right-click on a blank row or column in the **Repository** window and select an option. For example, in the **Licenses Repository** you can select to see only the attached licenses.

Clear Repository of completed operations - To clear a single operation, select the line in the **Operation Status** window and press the **Delete** key, or right-click and select **Clear**. To clear all completed operations from the **Operation Status** window, select **Status > Clear all completed operations**.

See operation details - To view operation details, in the **Operation Status** window, double-click the operation entry. The **Operation Details** window shows the operation description, start and finish times, and progress history. The window is resizable. To copy the Status lines to the clipboard, select the line, right-click and choose **Copy**.

Print views - To print a view, select **File > Print**. The **Choose Window** is displayed. Select the window that you would like to print, e.g., Operation Status or License & Contract Repository. Optionally, you can adjust the print setup settings, or preview the output.

See logs -

- Log of SmartUpdate package operations - `$SUROOT\log\su.elg`.
- Audit log of SmartUpdate operations - SmartView Tracker Audit View.

Upgrading Packages

The latest management version can be applied to a single Check Point Security Gateway, or to multiple Check Point Security Gateways simultaneously. Use the **Upgrade all Packages** operation to bring packages up to the most current management version.

When you perform **Upgrade all Packages** all products are upgraded to the latest Security Management server version. This process upgrades both the software packages and its related HFA (that is, the most up to date HFA is installed). Once the process is over, the software packages and the latest HFA will exist in the **Package Repository**.

To upgrade Check Point packages to versions earlier than the latest available version, they must be upgraded one-by-one. Use the **Distribute** operation to upgrade packages to management versions other than the most current, or to apply specific HFAs.

In addition, SmartUpdate recognizes gateways that do not have the latest HFA. When you right-click an HFA in the **Package Repository** and select **Distribute** for that specific HFA, you will receive a recommendation to install a new HFA on the gateways that do not have it.

Prerequisites for Remote Upgrades

- Make sure that SmartUpdate connections are allowed. Go to **SmartDashboard > Policy > Global Properties > FireWall Implied Rules**, and make sure that **Accept SmartUpdate Connections** is selected.
- Secure Internal Communication (SIC) must be enabled between the Security Management server and remote Check Point Security Gateways.

Retrieving Data from Check Point Security Gateways

In order to know exactly what OS, vendor and management version is on each remote gateway, you can retrieve that data directly from the gateway.

- To retrieve data on a specific Check Point Security Gateway, right-click on the gateway in the **Package Management** window and select **Get Gateway Data**.
- If you are installing or upgrading multiple Check Point Security Gateways, from the **Packages** menu select **Get Data From All**.

Adding New Packages to the Package Repository

To distribute (that is, install) or upgrade a package, you must first add it to the **Package Repository**. You can add packages to the **Package Repository** from the following three locations:

Download Center

1. Select **Packages > New Package > Add from Download Center**.
2. Accept the Software Subscription Download Agreement.
3. Enter your user credentials.
4. Select the packages to be downloaded. Use the `Ctrl` and `Shift` keys to select multiple files. You can also use the **Filter** to show just the packages you need.
5. Click **Download** to add the packages to the Package Repository.

User Center

Use this procedure for adding OPSEC packages and Hotfixes to the Package Repository.

1. Open a browser to the Check Point Support Center (<http://supportcenter.checkpoint.com>).
2. Select the package you want to upgrade.
3. Enter your user credentials.
4. Accept the Software Subscription Download Agreement.
5. Choose the appropriate platform and package, and save the download to the local disk.
6. Select **Packages > New Package > Import File**.
7. In the **Add Package** window, navigate to the desired .tgz file and click **Open** to add the packages to the **Package Repository**.

Check Point DVD

1. Select **Packages > New Package > Add from CD/DVD**.
2. Browse to the optical drive, and click **OK**.
A window opens, showing the available packages on the DVD.
3. Select the packages to add to the **Package Repository** (Ctrl-select for more than one package).
4. Click **OK**.

Verifying the Viability of a Distribution

Verify that the distribution (that is, installation) or upgrade is viable based upon the Check Point Security Gateway data retrieved. The verification process checks that:

- the Operating System and currently distributed packages are appropriate for the package to be distributed,
- there is sufficient disk space,
- the package is not already distributed,
- the package dependencies are fulfilled.

To manually verify a distribution, select **Packages > Pre-Install Verifier....**

Transferring Files to Remote Devices

When you are ready to upgrade or distribute packages from the **Package Repository**, it is recommended to transfer the package files to the devices to be upgraded. Placing the file on the remote device shortens the overall installation time, frees Security Management server for other operations, and reduces the chance of a communications error during the distribute/upgrade process. Once the package file is located on the remote device, you can activate the distribute/upgrade whenever it is convenient.

Transfer the package file(s) to the directory `$SUROOT/tmp` on the remote device. If this directory does not exist, do one of the following:

- For Windows gateways, place the package file in the directory `SYSTEMDRIVE\temp` (SYSTEMDRIVE is usually `C:\`)
- For UNIX gateways, place the package file in the directory `/opt/`.

Distributions and Upgrades

You can upgrade all packages on one remote gateway, or you can distribute specific packages one-by-one for all gateways.

Upgrading All Packages on a Check Point Remote Gateway

All Check Point packages on a single remote gateway, other than the operating system, can be remotely upgraded in a single operation. The **Upgrade all Packages** function allows you to simultaneously distribute or upgrade multiple packages to the latest management version. Proceed as follows:

1. Select **Packages > Upgrade all Packages**.
2. From the **Upgrade All Packages** window, select the Check Point Security Gateways that you want to upgrade. Use the **Ctrl** and **Shift** keys to select multiple devices.



Note - The **Reboot if required...** option (checked by default) is required in order to activate the newly distributed package.

3. If one or more of the required packages are missing from the **Package Repository**, the **Download Packages** window opens. Download the required package directly to the **Package Repository**.
4. Click **Upgrade**.
The installation proceeds only if the upgrade packages for the selected packages are available in the **Package Repository**.

Updating a Single Package on a Check Point Remote Gateway

Use this procedure to select the specific package that you want to apply to a single package. The **distribute** function allows you to:

- Upgrade the OS on an IP appliance or on SecurePlatform
- Upgrade any package to a management version other than the latest
- Apply Hot Fix Accumulators (HFAs)

Proceed as follows:

1. In the **Package Management** window, click the Check Point Security Gateway you want to upgrade.
2. Select **Packages > distribute**.
3. From the **distribute Packages** window, select the package that you want to distribute. Use the **Ctrl** and **Shift** keys to select multiple packages, and then click **distribute**.

The installation proceeds only if the upgrade packages selected are available in the **Package Repository**.

Upgrading UTM-1 Edge Firmware with SmartUpdate

The UTM-1 Edge gateway firmware represents the software that is running on the appliance. The UTM-1 Edge gateway's firmware can be viewed and upgraded using SmartUpdate. This is a centralized management tool that is used to upgrade all gateways in the system by downloading new versions from the download center. When installing new firmware, the firmware is prepared at the Security Management server, downloaded and subsequently installed when the UTM-1 Edge gateway fetches for updates. Since the UTM-1 Edge gateway fetches at periodic intervals, you will notice the upgraded version on the gateway only after the periodic interval has passed.

If you do not want to wait for the fetch to occur you can download the updates with the **Push Packages Now (UTM-1 Edge only)** option in the **Packages** menu. With this option it is possible to create a connection with UTM-1 Edge in order to access new (that is, the latest) software package(s). The distribution is immediate and avoids the need to wait for the fetch to get the package.

Canceling and Uninstalling

You can stop a distributed installation or upgrade while in progress.

To cancel a SmartUpdate operation:

- Select **Status > Stop Operation**.

At a certain point in any operation, the **Stop Operation** function becomes unavailable. You can cancel the operation after this point. This will uninstall changes made. Use this also to uninstall distributed installations or upgrades.

To uninstall:

1. Wait for the operation to complete.
2. Select **Packages > Uninstall**.



Note - Uninstallation restores the gateway to the last management version distributed.

Uninstalling Installations and Upgrades

If you want to cancel an operation and you have passed the point of no return, or the operation has finished, you can uninstall the upgrade by selecting **Packages > Uninstall**.



Note - Uninstallation restores the gateway to the last management version distributed.

Restarting the Check Point Security Gateway

After you distribute an upgrade or uninstall, reboot the gateway.

To restart the gateway:

- Select **Reboot if required** at the final stage of upgrade or uninstall.
- Select **Packages > Reboot Gateway**.

Recovering from a Failed Upgrade

If an upgrade fails on SecurePlatform, SmartUpdate restores the previously distributed version.

SecurePlatform Automatic Revert

If an upgrade or distribution operation fails on a SecurePlatform device, the device will reboot itself and automatically revert to the last version distributed.

Snapshot Image Management

Before performing an upgrade, you can use the command line to create a Snapshot image of the SecurePlatform OS, or of the packages distributed. If the upgrade or distribution operation fails, you can use the command line to revert the disk to the saved image.

- To create a Snapshot file on the gateway, type:
`cprinstall snapshot <object name> <filename>`
- To show the available Snapshot files, type:
`cprinstall show <object name>`
- To revert to a given Snapshot file, type:
`cprinstall revert <object name> <filename>`



Note - Snapshot files are stored at `/var/CPsnapshot` on the gateway.

Deleting Packages from the Package Repository

To clear the **Package Repository** of extraneous or outdated packages, select a package, or Ctrl-select multiple packages and select **Packages > Delete Package**. This operation cannot be undone.

Managing Licenses

With SmartUpdate, you can manage all licenses for Check Point packages throughout the organization from the Security Management server. SmartUpdate provides a global view of all available and installed licenses, allowing you to perform such operations as adding new licenses, attaching licenses and upgrading licenses to Check Point Security Gateways, and deleting expired licenses. Check Point licenses come in two forms, Central and Local.

- The *Central* license is the preferred method of licensing. A Central license ties the package license to the IP address of the Security Management server. That means that there is one IP address for all licenses; that the license remains valid if you change the IP address of the gateway; and that a license

can be taken from one Check Point Security Gateway and given to another with ease. For maximum flexibility, it is recommended to use Central licenses.

- The *Local* license is an older method of licensing, however it is still supported by SmartUpdate. A Local license ties the package license to the IP address of the specific Check Point Security Gateway, and cannot be transferred to a gateway with a different IP address.

When you add a license to the system using SmartUpdate, it is stored in the **License & Contract Repository**. Once there, it must be installed to the gateway and registered with the Security Management server. Installing and registering a license is accomplished through an operation known as *attaching* a license. Central licenses require an administrator to designate a gateway for attachment, while Local licenses are automatically attached to their respective Check Point Security Gateways.

Licensing Terminology

• Add

Licenses received from the User Center should first be added to the **License & Contract Repository**. Adding a local license to the **License & Contract Repository** also attaches it to the gateway.

Licenses can be conveniently imported to the **License & Contract Repository** via a file and they can be added manually by pasting or typing the license details.

• Attach

Licenses are attached to a gateway via SmartUpdate. Attaching a license to a gateway involves installing the license on the remote gateway, and associating the license with the specific gateway in the **License & Contract Repository**.

• Central License

A **Central License** is a license attached to the Security Management server IP address, rather than the gateway IP address. The benefits of a **Central License** are:

- Only one IP address is needed for all licenses.
- A license can be taken from one gateway and given to another.
- The new license remains valid when changing the gateway IP address. There is no need to create and install a new license.

• Certificate Key

The **Certificate Key** is a string of 12 alphanumeric characters. The number is unique to each package. For an evaluation license your certificate key can be found inside the mini pack. For a permanent license you should receive your certificate key from your reseller.

• CPLIC

A command line for managing local licenses and local license operations. For additional information, refer to the *R75.40VS Command Line Interface Reference Guide* (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

• Detach

Detaching a license from a gateway involves uninstalling the license from the remote gateway and making the license in the **License & Contract Repository** available to any gateway.

• State

Licenses can be in one of the following states:

The license state depends on whether the license is associated with the gateway in the **License & Contract Repository**, and whether the license is installed on the remote gateway. The license state definitions are as follows:

- **Attached** indicates that the license is associated with the gateway in the **License & Contract Repository**, and is installed on the remote gateway.
- **Unattached** indicates that the license is not associated with the gateway in the **License & Contract Repository**, and is not installed on any gateway.
- **Assigned** is a license that is associated with the gateway in the **License & Contract Repository**, but has not yet been installed on a gateway.
- **Upgrade Status** is a field in the **License & Contract Repository** that contains an error message from the User Center when the Upgrade process fails.

- **Get**
Locally installed licenses can be placed in the **License & Contract Repository**, in order to update the repository with all licenses across the installation. The **Get** operation is a two-way process that places all locally installed licenses in the **License & Contract Repository** and removes all locally deleted licenses from the **License & Contract Repository**.
- **License Expiration**
Licenses expire on a particular date, or never. After a license has expired, the functionality of the Check Point package may be impaired.
- **Local License**
A **Local License** is tied to the IP address of the specific gateway and can only be used with a gateway or a Security Management server with the same address.
- **Multi-License File**
Licenses can be conveniently added to a gateway or a Security Management server via a file, rather than by typing long text strings. **Multi-license files** contain more than one license, and can be downloaded from the Check Point User Center (<http://usercenter.checkpoint.com>).
Multi-license files are supported by the `cplic put`, and `cplic add` command-line commands.
- **Features**
A character string that identifies the features of a package.

License Upgrade

One of the many SmartUpdate features is to upgrade licenses that reside in the License & Contract Repository. SmartUpdate will take all licenses in the License & Contract Repository, and will attempt to upgrade them with the use of the Upgrade tool.

The License Attachment Process

Introducing the License Attachment Process

When a Central license is placed in the **License & Contract Repository**, SmartUpdate allows you to *attach* it to Check Point packages. Attaching a license installs it to the remote gateway and registers it with the Security Management server.

New licenses need to be attached when:

- An existing license expires.
- An existing license is upgraded to a newer license.
- A Local license is replaced with a Central license.
- The IP address of the Security Management server or Check Point Security Gateway changes.

Attaching a license is a three step process.

1. Get real-time license data from the remote gateway.
2. Add the appropriate license to the **License & Contract Repository**.
3. Attach the license to the device.

The following explains the process in detail.

Retrieving License Data from Check Point Security Gateways

To know exactly what type of license is on each remote gateway, you can retrieve that data directly from the gateway.

- To retrieve license data from a single remote gateway, right-click on the gateway in the **License Management** window and select **Get Check Point Security Gateway Licenses**.
- To retrieve license data from multiple Check Point Security Gateways, from the **Licenses** menu and select **Get All Licenses**.

Adding New Licenses to the License & Contract Repository

To install a license, you must first add it to the **License & Contract Repository**. You can add licenses to the **License & Contract Repository** in the following ways:

Download From the User Center

1. Select **Network Objects License & Contract** tab > **Add License > From User Center**
2. Enter your credentials.
3. Perform one of the following:
 - Generate a new license - if there are no identical licenses, the license is added to the **License & Contract Repository**.
 - Change the IP address of an existing license, that is, Move IP.
 - Change the license from Local to Central.

Importing License Files

1. Select **Licenses & Contract > Add License > From File**.
2. Browse to the location of the license file, select it, and click **Open**.

A license file can contain multiple licenses. Unattached Central licenses appear in the **License & Contract Repository**, and Local licenses are automatically attached to their Check Point Security Gateway. All licenses are assigned a default name in the format **SKU@ time date**, which you can modify at a later time.

Add License Details Manually

You may add licenses that you have received from the Licensing Center by email. The email contains the license installation instructions.

1. Locate the license:
 - If you have received a license by email, copy the license to the clipboard. Copy the string that starts with `cplic putlic...` and ends with the last SKU/Feature. For example: `cplic putlic 1.1.1.1 06Dec2002 dw59Ufa2-eLLQ9NB-gPuyHzvQ-WKreSo4Zx CPSUITE-EVAL-3DES-NGX CK-1234567890`
 - If you have a hard copy printout, continue to **step 2**.
2. Select the **Network Objects License & Contract** tab in SmartUpdate.
3. Select **Licenses > Add License > Manually**. The **Add License** window appears.
4. Enter the license details:
 - If you copied the license to the clipboard, click **Paste License**. The fields will be populated with the license details.
 - Alternatively, enter the license details from a hard-copy printout.
5. Click **Calculate**, and make sure the result matches the validation code received from the User Center.
6. You may assign a name to the license, if desired. If you leave the **Name** field empty, the license is assigned a name in the format **SKU@ time date**.
7. Click **OK** to complete the operation.

Attaching Licenses

After licenses have been added to the **License & Contract Repository**, select one or more licenses to attach to a Check Point Security Gateway.

1. Select the license(s).
2. Select **Network Objects License & Contract** tab > **Attach**.
3. From the **Attach Licenses** window, select the desired device.

If the attach operation fails, the Local licenses are deleted from the Repository.

Detaching Licenses

Detaching a license involves deleting a single *Central* license from a remote Check Point Security Gateway and marking it as unattached in the **License & Contract Repository**. This license is then available to be used by any Check Point Security Gateway.

To detach a license, select **Network Objects License & Contract** tab > **Detach** and select the licenses to be detached from the displayed window.

Deleting Licenses from the License & Contract Repository

Licenses that are not attached to any Check Point Security Gateway and are no longer needed can be deleted from the **License & Contract Repository**.

To delete a license:

1. Right-click anywhere in the **License & Contract Repository** and select **View Unattached Licenses**.
2. Select the unattached license(s) to be deleted, and click **Delete**.

Viewing License Properties

The overall view of the **License & Contract Repository** displays general information on each license such as the name of the license and the IP address of the machine to which it is attached. You can view other properties as well, such as expiration date, SKU, license type, certificate key and signature key.

To view license properties, double-click on the license in the **Licenses** tab.

Checking for Expired Licenses

After a license has expired, the functionality of the Check Point package will be impaired; therefore, it is advisable to be aware of the pending expiration dates of all licenses.

To check for expired licenses, select **Licenses > Show Expired Licenses**.

To check for licenses nearing their dates of expiration:

1. In the **License Expiration** window, set the **Search for licenses expiring within the next x days** property.
2. Click **Apply** to run the search.

To delete expired licenses from the **License Expiration** window, select the detached license(s) and click **Delete**.

Exporting a License to a File

Licenses can be exported to a file. The file can later be imported to the **License & Contract Repository**. This can be useful for administrative or support purposes.

To export a license to a file:

1. In the **Licenses Repository**, select one or more licenses, right-click, and from the menu select **Export to File....**
2. In the **Choose File to Export License(s) To** window, name the file (or select an existing file), and browse to the desired location. Click **Save**.

All selected licenses are exported. If the file already exists, the new licenses are added to the file.

Managing Multi-Domain Security Management Licenses with 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 **Past License** to enter the data.

You can now see the license in the repository.

To attach a license to a component:

1. In the SmartDomain Manager, select **SmartUpdate**.
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.

For more about license management tasks in SmartUpdate, see the *R75.40VS Security Management Administration Guide* (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

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

Service Contracts

Before upgrading a gateway or Security Management server, 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 Check Point 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.

For more on service contracts, see the Service Contract Files Web page (<http://www.checkpoint.com/nginx/upgrade/contract/index.html>).

Generating CPInfo

CPInfo is a support tool that gathers into one text file a wide range of data concerning the Check Point packages in your system. When speaking with a Check Point Technical Support Engineer, you may be asked to run CPInfo and transmit the data to the Support Center. Download the tool from the Support Center (<http://supportcontent.checkpoint.com/solutions?id=sk30567>).

To launch CPInfo, select **Tools > Generate CPInfo**.

1. Choose the directory to which you want to save the output file.
2. Choose between two methods to name the file:
 - based on the SR number the technician assigns you, or
 - a custom name that you define.
3. Optionally, you may choose to add:
 - **log files** to the CPInfo output.
 - the **registry** to the CPInfo output.

The SmartUpdate Command Line

All management operations that are performed via the SmartUpdate GUI can also be executed via the command line. There are three main commands:

- `cppkg` to work with the Packages Repository.
- `cprinstall` to perform remote installations of packages.
- `cplic` for license management.

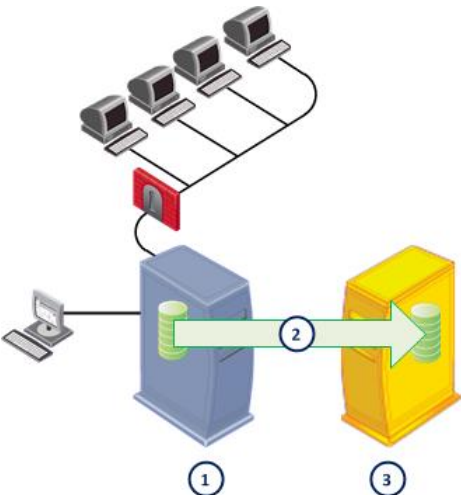
For details on how to use these commands, see the *R75.40VS Command Line Interface Reference Guide* (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

Chapter 9

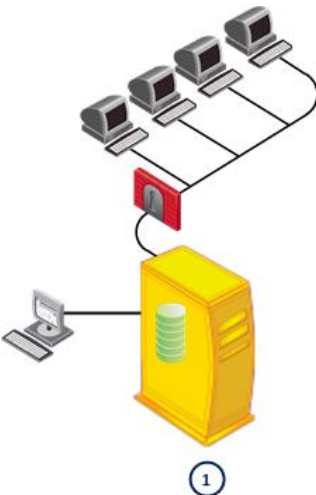
Advanced Upgrade and Database Migration

In This Chapter	
Supported Upgrade Paths, Platforms and Products	142
Legacy Hardware Platforms	142
Migration Workflow	143
Migrate Command Reference	152

Before Database Migration



After Database Migration



Item	Description	Item	Description
1	Source computer	1	Target R75.40VS computer connected to network
2	Management database migration path		
3	R75.40VS target computer, not connected to the network		

Supported Upgrade Paths, Platforms and Products

Make sure 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 R75.40VS Release Notes.

Legacy Hardware Platforms

A legacy platform is a hardware platform unsupported for new installations but still supported for database migration.

Solaris

Although Solaris is a legacy platform (unsupported for new installations), you can migrate the Solaris database to Windows, SecurePlatform, and Gaia. But only from Check Point versions in the supported upgrade path. See the R75.40VS *Release Notes* (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

- **For Security Management Server**

The database migration procedure for Solaris is the same as for SecurePlatform and Gaia, as described in this chapter.

- **For SmartDomain Manager**

To export the SmartDomain Manager database from a legacy platform, use the R75.40VS SecurePlatform CD. Only two menu options are available:

- preupgrade verification
- mds export

Migration Workflow

In this section:

General Workflow	144
Preparing the Source Server for New IP Address	145
Getting the Migration Tools Package	145
Using the Pre-Upgrade Verification Tool	145
Exporting the Database	146
Importing the Database	147
Migrating the Database of a Secondary Security Management Server	148
Completing Migration to a New IP Address	148
Migrating to a Server with a Different Platform	149
SmartReporter Database Migration	149
SmartEvent Events Database Migration	150

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

- A secondary Security Management server
- To a server with a different IP address
- SmartReporter
- SmartEvent

Migration Workflow



General Workflow

First read the Release Notes to make sure that your upgrade path is supported.

If the target Security Management Server will not use the IP address of the source, prepare the environment to recognize the new IP address ("[Preparing the Source Server for New IP Address](#)" on page 145). Do this before you do the steps below.

On the source server:

1. Get the migration tools package ("[Getting the Migration Tools Package](#)" on page 145).
2. Extract the downloaded package.



Important - Put all extracted files in the same directory, and run the tools from this directory.

3. Make sure the files have executable permissions. For example, In the temporary directory, run `chmod 777 *`
4. Run `fw logswitch` to close the SmartView Tracker log files. Only closed logs are migrated.
5. Close all Check Point GUI clients that are connected to the Security Management server.
Alternatively, if this is a computer that is not in production, run `cpstop` on the source computer.



Important - If you do not close the GUI clients or run `cpstop`, the exported management database can become corrupted.

6. Make sure the source server and the target server have network access.
 - The source and target servers must be connected to a network.
 - The connected network interface must have an IP address.
 - On SecurePlatform, the `ifconfig` command output must show that the interface is UP.
 - On Windows, the interface must be enabled in the **Network Connections** window.
7. Run the `pre_upgrade_verifier` command (see "[Using the Pre-Upgrade Verification Tool](#)" on page 145).
8. Correct all errors before continuing.
9. If the target server must have a different IP address than the source server, make the necessary changes on the source server (see "[Completing Migration to a New IP Address](#)" on page 148).
10. Export the management database ("[Exporting the Database](#)" on page 146).
 - If SmartReporter is installed on the source server, export the Log Consolidation database ("[Exporting the SmartReporter Database](#)" on page 149).
 - If SmartEvent is installed on the source server, export the Events database ("[SmartEvent Events Database Migration](#)" on page 150).

On the target server:

1. Install the R75.40VS Security Management server or a standalone deployment. Configure as required.
2. Get the most updated migration tools package ("[Getting the Migration Tools Package](#)" on page 145) 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. Import the management database from the source server to the target ("[Importing the Database](#)" on page 147).
 - If SmartReporter is installed on the source server, import the Log Consolidation database (see "[Importing the SmartReporter Database](#)" on page 150).
 - If SmartEvent is installed on the source server, import the SmartEvent Events database ("[SmartEvent Events Database Migration](#)" on page 150).
4. If the target server has a different IP address than the source server, make the necessary changes to the license and target computer ("[Completing Migration to a New IP Address](#)" on page 148).
If the target server is a different platform than the source server, edit the database ("[Migrating to a Server with a Different Platform](#)" on page 149).
5. Test the target installation.
6. Disconnect the source server from the network.
7. Connect the target server to the network.

Preparing the Source Server for New IP Address

Licenses are related to the Security Management server IP address. If you migrate the Security Management server database to a server with a new IP address, licensing issues can arise. We recommend that you keep the same IP address for the target Security Management server. If this is not possible, you must prepare the source database before the export and edit the target database after the import ("[Completing Migration to a New IP Address](#)" on page 148).

There are additional steps for a Security Management server that manages VSX Gateways in these configurations:

- From a Security Management server to a new Domain Management Server or Security Management server
- From a Domain Management Server to a new Domain Management Server

On the source computer before migration:

1. Create a new host object in SmartDashboard with the IP address of the target Security Management server.
2. Define a firewall rule that lets this new Security Management server connect to Security Gateways.

Source	Destination	Service
<i>new server</i>	any	FW1 (TCP 256) CPD (TCP 18191) FW1_CPRID (TCP 18208)

3. Install the new security policy on all gateways.
4. For configurations that include VSX Gateways, to these steps:
 - a) Define the previous firewall rule again for the VSX policy.
 - b) Install the policy on the VSX Gateways.

Getting the Migration Tools Package

It is important that you use the correct migration tools package. Download the latest version of the migration tools from the Support Center (<http://supportcenter.checkpoint.com>). This is the best way to make sure that you get the most recent version.

Alternatively, you can get the migration tools package from the target computer.

To get the migration tools package from the target computer:

1. Install R75.40VS on the target computer.
2. Copy the complete directory from the **target** computer to the **source** computer:
 - SecurePlatform / Gaia - \$FWDIR/bin/upgrade_tools
 - Windows - %FWDIR%\bin\upgrade_tools

Use FTP, SCP or similar. The source directory can be anywhere, such as /var/tmp.

The migration tool files are contained in a compressed package. The files in the package are:

- migrate
- migrate_conf
- upgrade_export
- upgrade_import

Using the Pre-Upgrade Verification Tool

We recommend that you run the pre-upgrade verifier (see "[Using the Pre-Upgrade Verifier Tool](#)" on page 65) on the Security Management server source computer before exporting 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 migration.

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

Go to the migration tools directory. The **pre_upgrade_verifier** tool is in the downloaded package, and is in the extracted directory. All files from the package must be in the same extracted directory.

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.

Exporting the Database

On Gaia and SecurePlatform - CLI

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

1. Log in to the **expert** mode.
2. Get the R75.40VS 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.

On Gaia and SecurePlatform - GUI on DVD

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

1. Insert the R75.40VS DVD into source computer drive.
2. At the command prompt, run: `patch add cd`
3. Select **SecurePlatform R75.40VS Upgrade Package**.
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 backup image can take up to twenty minutes, during which time Check Point products are stopped.

6. The **welcome** screen opens. Press **n**.
7. Press **Y** to accept the license agreement.
8. From the **Security Management Upgrade Option** screen, select **Export Security Management configuration**. Press **N** to continue.
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.

On IP Appliance

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

1. Get the R75.40VS 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.

On Windows - CLI

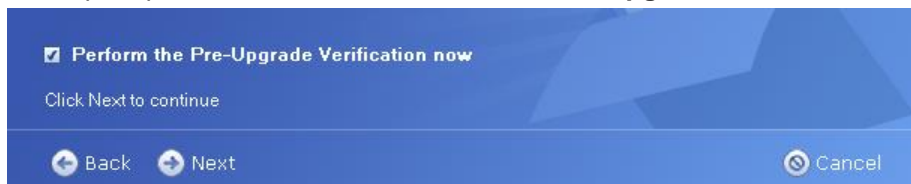
To create a management database export file on the source computer:

1. Get the R75.40VS 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.

On Windows - GUI on DVD

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

1. Log in to Windows using **Administrator** credentials.
2. Insert the R75.40VS 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 Support center (<https://support.checkpoint.com>).
 - Use the upgrade utilities that you downloaded to your local disk.
 - Use the upgrade utilities on the DVD.
7. When prompted, **do not disable** the **Perform Pre-Upgrade verification now** option.



8. If there are pre-upgrade verification errors, correct them and start this procedure again from step 3. Otherwise, click **Next** to continue.
9. Enter path and management database export file name. The default is:
`c:\temp\cp_db_configuration.tgz.`
10. When the export completes, click **OK**.

Importing the Database

To SecurePlatform

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. Use FTP, SCP or similar.
3. Run:
`<path to migration tools directory>/migrate import <path to the file>/<exported database name>.tgz.`
4. Do the instructions on the screen to import the management database.

To IP Appliance

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. Use FTP, SCP or similar.
2. Run:
`<path to migration tools directory>/migrate import <path to the file>/<exported database name>.tgz.`
3. Do the instructions on the screen to import the management database.

To Windows

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. Use FTP, SCP or similar.
2. From the Windows command prompt, run:
`<path to migration tools directory>\migrate.exe import <path to the file>\<exported database name>.tgz.`
3. Do the instructions on the screen to import the management database.

Migrating the Database of a Secondary Security Management Server

To do an advanced upgrade for a Secondary Security Management server:

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. To get assistance with this step, contact Check Point Technical Support or your vendor.
2. Install a new primary Security Management server.
3. Import the management database file to the new primary Security Management server.
4. Install new secondary R75.40VS Security Management server.
5. Establish SIC with the secondary Security Management Server.
6. Synchronize the new secondary Security Management server with the new primary Security Management server.

Completing Migration to a New IP Address

Licenses are related to the Security Management server IP addresses. You must update the license and configure the environment to recognize the new Security Management server.

1. Update the Security Management server licenses with the new IP address. If you use central licenses, they must also be updated with the new IP Address.
2. Run `cpstop`
3. Run `cpstart`
4. Connect to the new IP address with SmartDashboard.
 - a) Remove the host object and the rule that you created before migration ("[Preparing the Source Server for New IP Address](#)" on page 145).
 - b) Update the primary Security Management server object to make the IP Address and topology match the new configuration.
 - c) Reset SIC for all SmartEvent distributed servers.
5. Run `evstop` and `evstart` on SmartEvent and SmartReporter distributed servers.
6. On the DNS, map the target Security Management server host name to the new IP address.

Migrating to a Server with a Different Platform

If you migrate the management database to a server with a platform or operating system that is different from the source server, you must update the primary management object's properties accordingly.



Warning - Failure to do so may cause security issues.

After migration:

1. Connect with the SmartDashboard to the target Security Management Server.
2. Edit the primary object:
 - Update the target computer platform.
 - Update the target computer operating system.
3. Save the database.

Example:

If you migrate from a Windows Security Management server to an appliance:

1. Change **OS** from **Windows** to **SecurePlatform**.
2. Change **Hardware** from **Open server** to **UTM-1**.

SmartReporter Database Migration

While the database migration procedure automatically migrates the SmartReporter *management* database to the target server, it does not migrate the SmartReporter database. If you have SmartReporter installed on the source server, you must do several additional steps to migrate the database to the target.

Exporting the SmartReporter Database

To create the SmartReporter database export file on the source server:

1. Run `cpstop`.
2. Find and open the MySQL configuration file using a text editor:
 - On SecurePlatform: `$RTDIR/Database/conf/my.cnf`.
 - On Windows: `%RTDIR%\Database\conf\my.ini`

Use this file to locate directory names for use in the next steps.
3. Delete the contents of the directory specified in the **innodb_log_group_home_dir= <xxx>** setting.
4. Create the 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.
This directory contains the database files.
 - b) Use GNU tar/gzip utilities to create an archive file containing all files in the directory specified by the **datadir=<xxx>** setting. For example on SecurePlatform use:


```
tar zcvf datadir.tgz <datadir setting>
```
5. 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`). After copying the file to a backup device, rename the file by appending a `.old` suffix to the file name. For example, rename file `my.cnf` to `my.cnf.old`. (Import scripts require this suffix.)
 - 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).

Importing the SmartReporter Database

On the target server:

1. If you have not already done so, install R75.40VS and SmartReporter, on the target server.
2. Run `cpstop`.
3. Copy:
 - **For SecurePlatform:** `my.cnf.old` to `$RTDIR/Database/conf/`
 - **For Windows:** `my.ini.old` to `%RTDIR%\Database\conf`.



Note - If you are migrating to a platform where the name of configuration file is different (for example, migrating from Windows to SecurePlatform) rename the configuration file accordingly.

4. Copy these files from the backup device to the target server:
 - The SmartReporter exported database file (`datadir.tgz`) to the one of these locations:
 - **SecurePlatform:** `$RTDIR/bin`
 - **Windows:** `%RTDIR%\bin`
 - Company logo image files to the `$RTDIR/bin` (`%RTDIR%\bin` on Windows) directory.
 - Custom distribution scripts to the `$RTDIR/DistributionScripts` (`%RTDIR%\DistributionScripts` on Windows) directory.

Completing the SmartReporter Upgrade

To complete the SmartReporter upgrade:

1. When upgrading from a version before R75.40VS:
 - a) Run `cpstop`
 - b) Run:


```
cpprod_util_CPPPROD_SetValue_ "Reporting Module" DefaultDatabase 1 "MySQL" 1
```
2. Run:


```
./EVR_DB_Upgrade -mysql "<absolute path to file>/<SmartReporter database export file>.tgz"
```

For example, if **datadir.tgz** is located in `$RTDIR/bin`, run:

```
EVR_DB_Upgrade -mysql "$RTDIR/bin/datadir.tgz"
```
3. 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=
```
4. Run `cpstart`
5. In SmartDashboard, from the **Policy** menu, select **Install Database**.
6. In SmartReporter, from the **Consolidation** tab, remove the existing consolidation session and create a new one.

SmartEvent Events Database Migration

While the database migration procedure automatically migrates the SmartEvent *management* database to the target computer, it does not migrate the SmartEvent *events database*. If you have SmartEvent installed on the source server, you must do more to migrate the events database to the target.



Note - The Events Database can be very large, and the manual migration take time.

These steps explain how to use the `eva_db_backup` and `eva_db_restore` scripts with the default options. By default, the commands are run without options. You must have write permissions for the current directory.

To see more options:

- On SecurePlatform, run: `$RTDIR/bin/eva_db_backup.csh --help`
- On Windows, run: `%RTDIR%\bin\eva_db_backup.exe --help`

When upgrading from R70.20 and higher:

1. On the source machine, go to `$RTDIR/bin` or `%RTDIR%\bin`.
2. Run the backup tool:
 - On SecurePlatform, run: `./eva_db_backup.csh`
 - On Windows, run: `eva_db_backup.exe`
3. Copy the backup file created by the tool to the destination machine. By default, the name of a backup file is: `<current date>-events_db.backup`.
4. Run `cpstop` on the destination machine.
5. Run the restore tool:
 - On SecurePlatform, run: `$RTDIR/bin/eva_db_restore.csh -filename <path to the backup file>`
 - On Windows, run: `%RTDIR%\bin\eva_db_restore.exe -filename <path to the backup file>`
6. Open the `eventia_upgrade.C` file in `$RTDIR/conf` or `%RTDIR%\conf`.
If it has **DONE** in **online_status** or **background_status** attribute of the **Database** section, delete **DONE** and save the file.
7. Run: `cpstart`

When upgrading from a version older than R70.20:**On Source server:**

Copy the database file (`$RTDIR/events_db/events.sql` or `%RTDIR%/events_db/events.sql` file by default) from source machine to the destination machine.

On Destination server:

1. Run: `cpstop`
2. Run the PostgreSQL daemon:
 - SecurePlatform: `$CPDIR/database/postgresql/util/PostgreSQLCmd start`
 - Windows: `"%CPDIR%\database\postgresql\util\PostgreSQLCmd.exe" start`
3. Drop the previous PostgreSQL database content.
 - a) Log in to the postgres database:
 - SecurePlatform: `$CPDIR/database/postgresql/bin/psql -U cp_postgres -p 18272 postgres`
 - Windows: `"%CPDIR%\database\postgresql\bin\psql.exe" -U cp_postgres -p 18272 postgres`
 - b) Run: `drop database events_db;`
If you get an error that the database does not exist, ignore it.
 - c) Run `"\q"` to exit the database.
4. Run the database upgrade tool twice:
 - `DbUpgradeSqliteToPostgres online <full path to events.sql file>`
 - `DbUpgradeSqliteToPostgres background <full path to events.sql file>`

The second action may take a long time, depending on the Source machine database size.
5. Stop the PostgreSQL daemon:
 - SecurePlatform: `$CPDIR/database/postgresql/util/PostgreSQLCmd stop`
 - Windows: `"%CPDIR%\database\postgresql\util\PostgreSQLCmd.exe" stop`
6. Open the `eventia_upgrade.C` file in `$RTDIR/conf` or `%RTDIR%\conf`
If it shows **DONE** in the **online_status** or **background_status** attribute of the **Database** section, delete **DONE** and save the file.

7. Run: `cpstart`
8. Delete the `events.sql` file from destination machine.

Migrate Command Reference

The migrate command exports a source Security Management server database to a file, or imports the database file to a target Security Management server. Use absolute paths in the command, or relative paths from the current directory.

Before you run this command for export, close all SmartConsole clients or run `cpstop` on the Security Management Server.

Before you run this command for import, run `cpstop` on the Security Management Server.

Syntax:

```
migrate (export | import) [-l] [-n] <filename>
```

Parameters:

Value	Description
export import	One of these actions must be used. Make sure services are stopped.
-l	Optional. 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 export.
-n	Optional. Run silently (non-interactive) using the default options for each setting. Important note: If you export a management database in this mode, to a directory with a file with the same name, it will be overwritten without prompting. If you import using this option, the command runs <code>cpstop</code> automatically.
filename	Required. Enter the name of the archive file that contains the Security Management server database. The path to the archive must exist.

Chapter 10

Upgrading ClusterXL Deployments

In This Chapter

Planning a Cluster Upgrade	153
Minimal Effort Upgrade on a ClusterXL Cluster	154
Zero Downtime Upgrade on a ClusterXL Cluster	154
Zero Downtime Upgrade of SecurePlatform ClusterXL to Gaia ClusterXL	155
Converting a Security Gateway Cluster to VSX	155
VSX Cluster Optimal Service Upgrade	156
Full Connectivity Upgrade on a ClusterXL Cluster	158

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.



Note - During the upgrade procedure, standby members are upgraded first. When upgrade on the final active member begins, the active member fails over to the standby member (or members, depending on the deployment: High Availability or Load Sharing). At this point, since connection tables between cluster members are not synced, all open connections are lost. Only a full connectivity upgrade (between minor versions) preserves open connections.

- **Full Connectivity Upgrade:** Choose this option if your gateway needs to remain active and all open connections must be maintained. 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 158) and the *R75.40VS Release Notes* (<http://supportcontent.checkpoint.com/solutions?id=sk76540>).

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 32/64-bit Cluster Members

High Availability cluster deployments support 32/64-bit configurations. A cluster that contains 32-bit and 64-bit members, the 64-bit member changes to Ready state and does not synchronize with other members. When you are upgrading or replacing cluster members, make sure that all the cluster members are configured to the same version (32-bit or 64-bit).

Upgrading OPSEC Certified Cluster Products

- When upgrading IP appliance clusters (VRRP and IP Clusters), use the Zero Downtime or the Minimal Effort procedure.
- When upgrading third-party clustering products, use the Minimal Effort procedure.
- If the third party vendor has an alternative for a zero downtime upgrade, refer to their documentation before upgrading.

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.

Zero Downtime Upgrade on a ClusterXL Cluster

This section includes the procedure doing a zero downtime upgrade. 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 guide.

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

We recommend that you do not install a new policy on the cluster until the last member is upgraded. If you must do this, see *Installing a Policy during Cluster Upgrade*.

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. Assume cluster member A is the active member, and members B and C are standby members.
 - a) In **Load Sharing** mode, randomly choose one of the cluster members to upgrade last.
 - b) Make sure that the previously upgraded software blade 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 them.

5. In SmartDashboard:
 - a) From the **Install Policy** 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) In the **Gateway Cluster General Properties** window, change the Cluster version to the new version.
 - c) Install the security policy on the cluster.
The policy successfully installs on cluster members B and C. Policy install fails on member A and generates a warning. The warning can be safely ignored.
6. 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.
7. Upgrade Cluster member A by:
 - Using SmartUpdate
 - In Place

During the upgrade, `cpstop` runs automatically, causing A to fail over to members B and/ or C depending on whether this is a Load Sharing or High Availability configuration.
8. Reboot cluster member A.
9. Run `cphaconf set_ccp multicast` 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.

Zero Downtime Upgrade of SecurePlatform ClusterXL to Gaia ClusterXL

In this procedure, the gateway cluster has an active member (A), and two backup members (B and C). First upgrade B and C, and then upgrade A.

To do a zero down-time upgrade of a ClusterXL gateway cluster:

1. Upgrade the backup members (B and C). See [Upgrading an Open Server from SecurePlatform to Gaia](#) or [Upgrading an Appliance from SecurePlatform to Gaia](#).
2. Verify that active member (A) is Active, and that B and C are Ready: On each member, run the command `cphaprob stat`.
3. Transfer traffic to members B and C by stopping traffic on A. On A, run `cphastop`
4. Upgrade member A, as above.
5. Install the policy on A.

Converting a Security Gateway Cluster to VSX

Use the VSX Gateway Conversion wizard in SmartDashboard to convert a Gaia High Availability cluster of Security Gateways to a VSX cluster ("[Converting Gateways to VSX Gateways](#)" on page 44). The settings of each Security Gateway are applied to the VSX Gateway (VS0). For more about using the Conversion wizard, see sk79260 (<http://supportcontent.checkpoint.com/solutions?id=sk79260>).

You can only convert a cluster that uses the Gaia operating system.



Important - There is no loss of connectivity during the conversion process. You cannot use the conversion wizard to convert a Load Sharing cluster of Security Gateways.

VSX Cluster Optimal Service Upgrade

Use the Optimal Service Upgrade feature to upgrade a VSX cluster from R67.10 to R75.40VS with a minimum loss of connectivity. New connections that are opened during the upgrade procedure are maintained after the upgrade is finished. Connections that were opened on the old version are discarded after the upgrade.

You will also be able to use this feature to upgrade a Security Gateway or VSX cluster from R75.40VS to future major releases. For more about upgrading to R67.10, see the *R67.10 Release Notes*.

For more about the Optimal Service Upgrade and to download the upgrade hotfix, go to sk74300 (<http://supportcontent.checkpoint.com/solutions?id=sk74300>).

Upgrade Workflow

Use the Optimal Service Upgrade feature to upgrade a VSX cluster from R67.10 to R75.40VS without losing connectivity. When you upgrade the cluster, use two cluster members to process the network traffic.

- Old cluster member with hotfix - The R67.10 VSX Gateway on which you install the Optimal Service Upgrade hotfix.
- New cluster member - VSX Gateway that you upgraded to R75.40VS. This cluster member processes new connections.

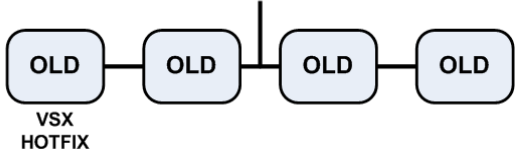
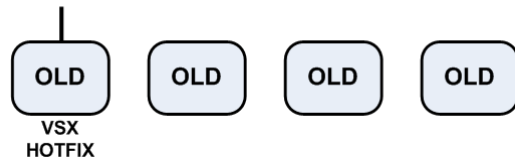
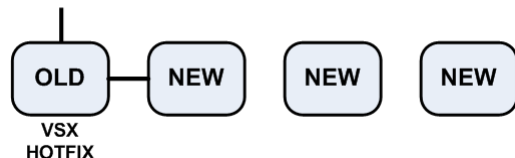
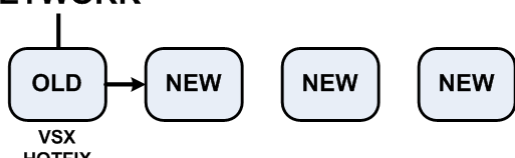
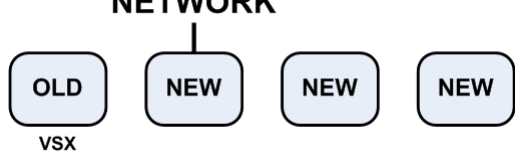
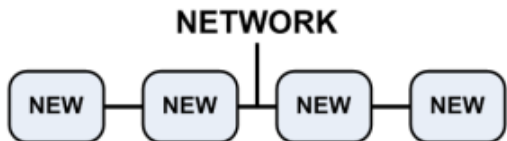
Diagram of Cluster Members	Summary
<p>NETWORK</p> 	<ul style="list-style-type: none"> • VSX cluster with four R67.10 VSX Gateways (OLD). • Install the Optimal Service Upgrade hotfix on the cluster member that is connected to the network.
<p>NETWORK</p> 	<ul style="list-style-type: none"> • Disconnect all the cluster members from the network, except for the member with the hotfix. • Configure the <code>fwaha_mac_magic</code> parameter on the member with the hotfix.
<p>NETWORK</p> 	<ul style="list-style-type: none"> • Upgrade the cluster members to R75.40VS (NEW), except for the old hotfix cluster member. • On the old cluster member, run the hotfix.
<p>NETWORK</p> 	<ul style="list-style-type: none"> • Connect one new cluster member to the network. • On the new cluster member, run <code>cphaosu start</code>. <p>All new connections are processed on the new cluster member.</p>
<p>NETWORK</p> 	<ul style="list-style-type: none"> • Disconnect the old cluster member from the network.

Diagram of Cluster Members	Summary
	<ul style="list-style-type: none"> • Connect all the cluster members to the network. • Upgrade the old member to R75.40VS

Upgrading the Cluster R67.10 VSX

Two cluster members are used to maintain connectivity, while you upgrade all the other cluster members.

The default value for the `fwha_mac_magic` parameter is 254. If your configuration uses a different value, make sure that you configure the applicable `fwha_mac_magic` parameter on all the cluster members. For more about the `fwha_mac_magic` parameter, see the *R75.40VS ClusterXL Administration Guide*.

To use the Optimal Service Upgrade to upgrade the R67.10 VSX cluster members:

1. Install the Optimal Service Upgrade hotfix on a cluster member
(http://downloads.checkpoint.com/fileserver/ID/18641/FILE/fw1_HOTFIX_ELSA_HFA_OSU_076.tgz).
This is the old cluster member with hotfix.
Run `fw1_HOTFIX_ELSA_HFA_OSU_076_843076007_1`
2. Disconnect all old cluster members from the network, except for one cluster member.
Make sure that the management interfaces are not connected to the network.
3. Configure the `fwha_mac_magic` parameter on the old cluster member, run `fw ctl set int fwha_mac_magic <value>`
Make sure that the old and new cluster members use the same value for the `fwha_mac_magic` parameter.
4. Install R75.40VS on all the cluster members that are not connected to the network.
5. On the old cluster member, run `cphaosu start`
6. Reconnect the SYNC interface of one new cluster member to the network.
7. Move traffic to the new cluster member that is connected to the network. Do these steps:
 - a) Make sure the new cluster member is in ready state.
 - b) Connect the other new cluster member interfaces to the network.
 - c) On the new cluster member, run `cphaosu start`
 - d) On the old cluster member, run `cphaosu stat`
The network traffic statistics are shown.
 - e) When the old cluster member does not have many connections, run `cphaosu finish`
8. On the new cluster member, run `cphaosu finish`
9. Disconnect the old cluster member from the network.
10. Reconnect the other new cluster members to the network one at a time. Do these steps on each cluster member:
 - a) Run `cphastop`
 - b) Connect the new cluster member to the network.
 - c) Run `cphastart`
11. Upgrade the old cluster member and reconnect it to the network.

Troubleshooting the Upgrade

Use these `cphaosu` commands if there are problems during the upgrade process.

- If it is necessary to rollback the update, run `cphaosu cancel` on the new member. The old member processes all the traffic.

- After you run `cpshaosu finish` on the old member, you can continue to process the old traffic on the old member and the new traffic on the new member. Run `cphaosu restart` on the old member.

Limitations

1. Upgrade procedure should be implemented when there is minimal network traffic.
2. If there is a member failure during the upgrade, the Optimal Service Upgrade procedure does not provide redundancy.
3. Do not apply configuration changes during the upgrade process.
4. These connections do not survive the upgrade process:
 - a) Complex connections, for example:
 - DCE RPC
 - SUN RPC
 - Back Web
 - DHCP
 - IIOP
 - FreeTel
 - WinFrame
 - NCP
 - VPN
 - b) Dynamic routing
 - c) Bridge mode (L2) configurations

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 R75.40VS 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 Upgrade Scenarios

FCU when upgrading and also changing the OS.

Check Point Clustering Solution			
OS Type Changing from:	ClusterXL	IP clustering	VRRP
SecurePlatform to Gaia	No FCU	No FCU	No FCU
Not Changing	FCU	FCU	FCU
IPSO to Gaia	No FCU	No FCU	No FCU

IPSO to SecurePlatform	No FCU	No FCU	No FCU
------------------------	--------	--------	--------

- Legacy High Availability is not supported in FCU.
- For other third-party support, refer to the third-party documentation.

Full Connectivity Upgrade Prerequisites

Make sure that the new member (NM) and the old member (OM) have the same policy and product installation. During the upgrade, do not change the policy from the last policy installed before this upgrade.

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:

```
Registered connections modules:
No. Name      Newconn Packet End      Reload Dup Type Dup Handler
0: Accounting 00000000 00000000 d08ff920 00000000 Special d08fed58
1: Authentication d0976098 00000000 00000000 00000000 Special d0975e7c
3: NAT        00000000 00000000 d0955370 00000000 Special d0955520
4: SeqVerifier d091e670 00000000 00000000 d091e114 Special d091e708
6: Tcpstreaming d0913da8 00000000 d09732d8 00000000 None
7: VPN        00000000 00000000 d155a8d0 00000000 Special d1553e48
```

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 154). 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:

Do the steps outlined in Zero Downtime Upgrade on a ClusterXL Cluster (on page 154). Before you do step 7 in this section, run this 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.

To upgrade a cluster with three or more members, do one these:

- Upgrade the two New Members (NMs) by doing the steps in Zero Downtime Upgrade on a ClusterXL Cluster (on page 154). Before you do the "Upgrade cluster member" A step, run this command on all

upgraded members:

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

Continue with the **Upgrade cluster member A** step on the single Old Member (OM).

or

- First upgrade one member by doing the steps in Zero Downtime Upgrade on a ClusterXL Cluster (on page 154). Before you do the "Upgrade cluster member A" step, run this command on all upgraded members:

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

Continue with **Upgrade cluster member A** on the remaining Old Members (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. After `cphastop` is executed, do not run `cpstart` or `cphastart` and do not reboot the machine.

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:

```
During FCU..... yes
Number of connection modules..... 23
Connection module map (remote -->local)
0 --> 0 (Accounting)
1 --> 1 (Authentication)
2 --> 3 (NAT)
3 --> 4 (SeqVerifier)
4 --> 5 (SynDefender)
5 --> 6 (Tcpstreaming)
6 --> 7 (VPN)
Table id map (remote->local)..... (none or a specific list,
depending on configuration)
Table handlers .....
78 --> 0xF98EFFF0 (sip_state)
8158 --> 0xF9872070 (connections)
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 Upgrade Scenarios" on page 158).

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

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 marked as non-synchronized.

Syntax:

```
fw tab -t connections -u [-s]
```

Options:

-t - table

-u - unlimited entries

-s - (optional) summary of the number of connections

For more on the `fw tab -t connections` command, see the *Command Line Interface Guide*.

You can 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 table handlers that deal with the upgrade are only created during policy installation, and `cpstart` installs policy.

Index

A

- Action Items • 146
- Add License Details Manually • 138
- Add Packages to the Package Repository • 92
- Adding a New Appliance to a High Availability Cluster • 51
- Adding Licenses using the SmartDomain Manager • 62
- Adding New Licenses to the License & Contract Repository • 138
- Adding New Packages to the Package Repository • 132
- Advanced Upgrade and Database Migration • 142
- Attaching Licenses • 138

B

- Backing Up • 66
- Backing Up the System - CLI (Backup) • 66
- Backing Up the System - WebUI • 66
- Backup and Restore • 117
- Basic Architecture • 56

C

- Canceling and Uninstalling • 134
- Certificate Authority Information • 116
- Changing the Multi-Domain Server Interfaces • 127
- Check Point DVD • 133
- Checking Compatibility • 45
- Checking for Expired Licenses • 139
- cma_migrate • 115
- cma_migrate and Certificates • 116
- Common Operations • 131
- Compatibility Tables • 12
- Completing Migration to a New IP Address • 148
- Completing the Conversion • 45
- Completing the SmartReporter Upgrade • 150
- Configuring Image Management - CLI (snapshot) • 68
- Configuring Image Management - WebUI • 67
- Configuring Standalone Full High Availability • 50
- Configuring the Security Management Server for SmartUpdate • 92
- Container2MultiDomain • 113
- Contract Verification • 64
- Converting a Security Gateway • 44
- Converting a Security Gateway Cluster to VSX • 155
- Converting a Security Management Server to Multi-Domain Server • 59
- Converting a VSX Gateway • 45
- Converting Gateways to VSX Gateways • 44
- Converting the Security Management Server • 59

D

- Deleting Licenses from the License & Contract Repository • 139
- Deleting Packages from the Package Repository • 135
- Demo Mode • 53, 62
- Deploying Bridge Mode Security Gateways • 52
- Deployment Options • 15
- Detaching Licenses • 139
- Disk Partitions in a Gaia Clean Installation • 17, 34
- Disk Space • 14
- Display the Connections Table • 160
- Displaying Upgrade Statistics (cphaprob fcustat) • 160
- Distributions and Upgrades • 133
- Download Center • 132
- Download From the User Center • 138
- Downloading R75.40VS • 10

E

- Export • 114
- Exporting a License to a File • 139
- Exporting a Multi-Domain Server Deployment • 121
- Exporting and Importing a Multi-Domain Server • 120
- Exporting the Database • 146
- Exporting the SmartReporter Database • 149

F

- For New Check Point Customers • 10
- Full Connectivity Upgrade Limitations • 159
- Full Connectivity Upgrade on a ClusterXL Cluster • 158
- Full Connectivity Upgrade Prerequisites • 159

G

- Gaia • 19, 20, 30, 35, 37, 40, 42, 52
- Gaia Appliances • 47
- Gaia Automatic Software Updates • 14
- Gaia Backup • 66
- Gaia Snapshot Image Management • 67
- Gaia to Gaia • 76, 79, 80, 85, 87, 93, 95, 105, 119
- Gateway Upgrade - SmartUpdate • 92
- General Workflow • 144
- Generating CPInfo • 140
- Getting Started • 9
- Getting the Migration Tools Package • 145
- Glossary • 10
- Gradual Upgrade to Another Computer • 122
- Gradual Upgrade with Global VPN Communities • 123

I

- ICA Considerations • 73
- Important Information • 3
- Importing a Multi-Domain Server deployment • 121
- Importing License Files • 138
- Importing the Database • 147
- Importing the SmartReporter Database • 150
- Installation Procedure Overview • 22

- Installing a Contract File • 74
- Installing Full High Availability Appliances • 47
- Installing Gateways • 61
- Installing Log Server • 39
- Installing Multi-Domain Security Management • 56
- Installing Multi-Domain Security Management GUI Clients • 61
- Installing Multi-Domain Server • 58
- Installing Security Gateway • 40
- Installing Security Gateway on Appliances • 40
- Installing Security Gateway on Open Servers • 42
- Installing Security Management Server • 34
- Installing Security Management Server and Security Gateways • 16
- Installing Security Management Server on Appliances • 35
- Installing Security Management Server on Open Servers • 37
- Installing SmartConsole Clients • 53
- Installing Standalone • 17
- Installing Standalone on Appliances • 18
- Installing Standalone on Open Servers • 30
- Installing VSX Gateways • 44
- Introducing SmartUpdate • 129
- Introducing the License Attachment Process • 137
- Introduction • 74
- IP Appliances • 20, 42, 79, 95
- IPS with Multi-Domain Security Management • 128
- IPSO to Gaia • 96

L

- Legacy Hardware Platforms • 142
- License Upgrade • 137
- Licensing • 13
- Licensing Multi-Domain Security Management • 13
- Licensing Terminology • 136
- Limitations • 158
- Logging in to SmartConsole • 54

M

- Managing Domain Management Servers During the Upgrade Process • 126
- Managing Licenses • 135
- Managing Multi-Domain Security Management Licenses with SmartUpdate • 139
- mds_backup • 118
- mds_restore • 118
- Migrate Command Reference • 152
- migrate export • 115
- migrate_global_policies • 117
- Migrating from Security Management Server to Domain Management Server • 123
- Migrating the Database of a Secondary Security Management Server • 148
- Migrating to a Server with a Different Platform • 149
- Migration Workflow • 143
- Minimal Effort Upgrade on a ClusterXL Cluster • 154

- Multi-Domain Server High Availability • 125
- Multi-Domain Server In-Place Upgrade • 119

O

- On Gaia and SecurePlatform - CLI • 146
- On Gaia and SecurePlatform - GUI on DVD • 146
- On Gaia, SecurePlatform and Windows • 74
- On IP Appliance • 147
- On IP Appliances • 74
- On Security Gateways • 75
- On Windows - CLI • 147
- On Windows - GUI on DVD • 147
- Open Servers • 60

P

- Performing a Full Connectivity Upgrade • 159
- Permanent Kernel Global Variables • 153
- Planning a Cluster Upgrade • 153
- Planning the Upgrade • 120
- Post-Installation Configuration • 54, 61
- Preparing for Installation • 21
- Preparing for Upgrade • 96
- Preparing the Source Server for New IP Address • 145
- Preparing to Convert • 59
- Prerequisites for Remote Upgrades • 132
- Pre-Upgrade Verification and Tools • 125
- Pre-Upgrade Verifiers and Correction Utilities • 113

R

- R75.40VS Documentation • 9
- Ready State During Cluster Upgrade/Rollback Operations • 153
- Recommended Logging Options for High Availability • 51
- Recovering from a Failed Upgrade • 135
- Removing a Cluster Member • 50
- Removing Earlier Version Multi-Domain Server Installations • 127
- Replicate and Upgrade • 121
- Resolving Issues with IKE Certificates • 117
- Restarting Domain Management Servers • 126
- Restarting the Check Point Security Gateway • 135
- Restoring a Deployment • 71
- Restoring Other Platforms • 72
- Restoring Your Original Environment • 126
- Retrieving Data from Check Point Security Gateways • 132
- Retrieving License Data from Check Point Security Gateways • 137
- Rollback from Gaia to IPSO • 28, 104
- Running Container2MultiDomain • 114

S

- SecurePlatform • 19, 31, 36, 38, 41, 42, 53
- SecurePlatform Appliances • 49
- SecurePlatform Automatic Revert • 135
- SecurePlatform Backup • 69
- SecurePlatform Restore • 72
- SecurePlatform Revert • 71

- SecurePlatform Snapshot Image Management • 70
- SecurePlatform to Gaia • 78, 82, 86, 89, 94, 107
- SecurePlatform to SecurePlatform • 78, 83, 87, 90, 95, 108, 119
- Service Contract Files • 74
- Service Contracts • 140
- Setting Up Multi-Domain Security Management Networking • 57
- Smart-1 • 35
- Smart-1 and 2012 Models • 85
- Smart-1 Appliances • 58
- SmartDashboard Toolbar • 14
- SmartEvent Events Database Migration • 150
- SmartReporter Database Migration • 149
- SmartUpdate - Seeing it for the First Time • 131
- Snapshot Image Management • 135
- Software Licensing • 13
- Step 1
 - Getting the Upgrade Package and the Gaia Image • 23, 99
- Step 10
 - Making Sure the Upgrade Succeeded • 104
 - Selecting Check Point Products • 28
- Step 2
 - Putting the Gaia ISO on an FTP Server • 23, 99
- Step 3
 - Installing the Package on the IP Appliance • 23, 99
- Step 4
 - Running the Installation and Upgrade Script • 24, 100
- Step 5
 - Verifying the FTP Server • 25, 101
- Step 6 (Optional, Recommended)
 - Supplying Reports and Backup Server Information • 26, 102
- Step 7 (Optional)
- Supplying Special Package Server Information • 26, 102
- Step 8
 - Confirming Your Selections • 26, 103
- Step 9
 - Installation Runs Automatically • 27
 - Upgrade Runs Automatically • 103
- Supported Upgrade Paths, Platforms and Products • 142
- Supported Upgrade Scenarios • 158

T

- The License Attachment Process • 137
- The pre_upgrade_verifier command • 146
- The SmartUpdate Command Line • 141
- To an Earlier Version on a Windows Open Server • 73
- To an Earlier Version on an IP Appliance • 72
- To IP Appliance • 148
- To SecurePlatform • 147
- To Windows • 148
- Transferring Files to Remote Devices • 133
- Troubleshooting the Upgrade • 157

U

- Understanding a Full Connectivity Upgrade • 158
- Understanding SmartUpdate • 130
- Uninstalling Installations and Upgrades • 135
- Uninstalling Multi-Domain Security Management • 62
- Uninstalling Packages • 66
- Uninstalling R75.40VS • 54
- Updating a Single Package on a Check Point Remote Gateway • 134
- Updating Objects in the Domain Management Server Databases • 126
- Upgrade Best Practices • 119
- Upgrade Multi-Domain Security Management Tools • 113
- Upgrade Procedure Overview • 98
- Upgrade Tools • 65
- Upgrade Workflow • 156
- Upgrading 32/64-bit Cluster Members • 154
- Upgrading a High Availability Deployment • 124
- Upgrading a VSX Gateway • 109
- Upgrading All Packages on a Check Point Remote Gateway • 133
- Upgrading Clusters • 111
- Upgrading ClusterXL Deployments • 153
- Upgrading Gateways using SmartUpdate • 91
- Upgrading Multi-Domain Security Management • 113
- Upgrading Multi-Domain Servers and Domain Management Servers • 125
- Upgrading OPSEC Certified Cluster Products • 154
- Upgrading Packages • 132
- Upgrading Prerequisites • 64
- Upgrading Security Gateways • 91
- Upgrading Security Gateways on Appliances • 93
- Upgrading Security Gateways on Open Servers • 105
- Upgrading Security Management Server and Security Gateways • 76
- Upgrading Security Management Server on Appliances • 85
- Upgrading Security Management Server on Open Servers • 87
- Upgrading Standalone • 76
- Upgrading Standalone Appliances • 76
- Upgrading Standalone Full High Availability • 110
- Upgrading Standalone Open Servers • 80
- Upgrading Successfully • 66
- Upgrading the Cluster R67.10 VSX • 157
- Upgrading the Security Management Server • 84
- Upgrading UTM-1 Edge Firmware with SmartUpdate • 134
- Upgrading with a Clean Installation • 111
- Upgrading with Minimal Downtime • 110
- Upgrading with SmartUpdate • 129
- USB Installation • 10
- User Center • 133
- Using the Pre-Upgrade Verification Tool • 145
- Using the Pre-Upgrade Verifier Tool • 65

UTM-1 and 2012 Models • 18, 76
UTM-1, Power-1, and 2012 Models • 40, 93

V

Verifying the Viability of a Distribution • 133
Viewing License Properties • 139
VSX Cluster Optimal Service Upgrade • 156

W

Web Security License Enforcement • 140
Welcome • 9
Where To From Here? • 63
Where to Go From Here • 54
Windows • 32, 38, 43, 109
Windows and IP Appliance Export • 71
Windows to Windows • 84, 91
Working with Contract Files • 74

Z

Zero Downtime Upgrade of SecurePlatform
ClusterXL to Gaia ClusterXL • 155
Zero Downtime Upgrade on a ClusterXL Cluster
• 154