13 March 2017

Gaia

R80.10

Installation and Upgrade Guide

Protected

Check Point
SOFTWARE TECHNOLOGIES LTD.

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.

Check Point R80.10

For more about this release, see the R80.10 home page http://supportcontent.checkpoint.com/solutions?id=sk111841.

More Information

Visit the Check Point Support Center http://supportcenter.checkpoint.com.

Latest Version of this Document

Download the latest version of this document http://downloads.checkpoint.com/dc/download.htm?ID=TBD.

To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

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 Gaia R80.10 Installation and Upgrade Guide.

Searching in Multiple PDFs

To search for text in all the R80.10 PDF documents, download and extract the complete R80.10 documentation package http://supportcontent.checkpoint.com/documentation_download?ID=TBD.
Use **Shift-Control-F** in Adobe Reader or Foxit reader.

Revision History

Date	Description
13 March 2017	First release of this document

Contents

Terms

Active Domain Server

The only Domain Management Server in a High Availability deployment that can manage a specified Domain.

Active Multi-Domain Server

The one Multi-Domain Server in a High Availability deployment that can work with global objects and global policies.

Administrator

A SmartConsole user with permissions to manage Check Point security products and the network environment.

ClusterXL

Check Point software-based cluster solution for Security Gateway redundancy and Load Sharing.

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.

Distributed Deployment

The gateway and the Security Management Server are deployed on different computers.

Domain

A network or a collection of networks related to an entity, such as a company, business unit or geographical location.

Domain Log Server

A log server for a specified Domain.

Domain Server

A virtual Security Management Server that manages Security Gateways for one Domain as part of a Multi-Domain Security Management environment.

Global Configuration

All Policies defined in the Global Domain that can be assigned to Domains, or to specified groups of Domains.

ICA

Internal Certificate Authority - A server component that issues certificates for authentication.

In-Place Upgrade

Upgrading a Security Management Server or Multi-Domain Server to the latest version on the existing computer.

Multi Domain Log Server

Physical server that contains the log database for all Domains.

Multi-Domain Security Management

A centralized management solution for large-scale, distributed environments with many different Domain networks.

Multi-Domain Server

A physical server that contains system information and Policy databases for all Domains in an enterprise environment.

Open Server

A computer made and distributed by a third party, such as Intel, and its operating system, such as RHEL or Windows, that is certified by Check Point to support Check Point products.

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.

Primary Multi-Domain Server

The first Multi-Domain Server that you define and log into, in a High Availability deployment.

Secondary Multi-Domain Server

All Multi-Domain Servers in a High Availability deployment created after the Primary Multi-Domain Server.

Security Gateway

A computer or an appliance that inspects traffic and enforces Security Policies for connected network resources.

Security Management Server

The server that manages, creates, stores, and distributes the security policy to Security Gateways.

Security Policy

A collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

SmartConsole

A Check Point GUI application used to manage security policies, monitor products and events, install updates, provision new devices and appliances, and manage a multi-domain environment.

SmartDashboard

A legacy Check Point client used to create and manage the security policy.

SmartUpdate

A SmartConsole client used to centrally upgrade and manage Check Point software and licenses.

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.

Standby Domain Server

All Domain Management Servers for a Domain that are not designated as the Active Domain Management Server.

Standby Multi-Domain Server

All Multi-Domain Servers in a High Availability deployment that cannot manage global policies and objects. Standby Multi-Domain Servers are synchronized with the active Multi-Domain Server.

Getting Started

In This Section:

Before you install or upgrade to R80.10:

1. Read the *R80.10 Release Notes* http://supportcontent.checkpoint.com/solutions?id=sk111841.
2. Create a backup file of the current system settings from the Gaia WebUI.
   For Multi-Domain Server run `mds_backup`

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.

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.

R80.10 Documentation

This guide is for security administrators responsible for installing R80.10 on appliances and open servers running Gaia.

To learn what is new in R80.10, see the *R80.10 Release Notes*. To find the release notes and the documentation, see the R80.10 home page http://supportcontent.checkpoint.com/solutions?id=sk111841.

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

Disk Space

When you install or upgrade R80.10, the installation or upgrade 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.

To learn how to remove old Check Point packages and files, see sk91060 http://supportcontent.checkpoint.com/solutions?id=sk91060.

After there is sufficient disk space, install or upgrade the product.

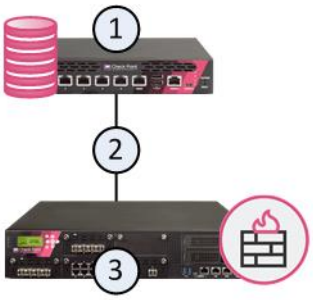
Product Deployment Scenarios

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	Security Management Server component
2	Standalone server
3	Security Gateway component

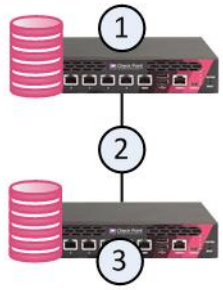
- **Distributed Deployment** - The Security Gateway and the Security Management Server are installed on different computers or appliances.



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

Management HA - A Primary and Secondary Security Management Server are configured. The databases of the Security Management Servers are synchronized, either manually or on a schedule, so they can back up one another. The administrator makes one Security Management

Server Active and the other(s) Standby. If the Active Security Management Server is down, the administrator can make the Standby server Active.



Item	Description
1	Primary Security Management Server
2	Direct or indirect Security Management Server to Security Management Server connection
3	Secondary Security Management Server

Backing Up

In This Section:

Gaia Snapshot Image Management

Before you upgrade a computer or appliance, back up with a snapshot. A snapshot saves the configuration of the Gaia operating system and, on a management server, the database. You can save snapshots on demand, or create a backup schedule.

You can revert to this snapshot to uninstall the new release.

Before you use snapshot image management, see sk91400 http://supportcontent.checkpoint.com/solutions?id=sk91400 and sk98068 http://supportcontent.checkpoint.com/solutions?id=sk98068.

A snapshot is a backup of the system settings and products:

- File system, with customized files
- System configuration (interfaces, routing, hostname, and similar)
- Software Blades
- Management database (on a Security Management Server or a Multi-Domain Server)

You can import a snapshot that was made on a different release or on this release. You must import it to the same appliance or open server hardware model.

IMPORTANT: After importing the snapshot, you must activate the device license from the WebUI or the User Center.

Snapshot options:

- **Revert** to a user created image.
- **Revert** to a factory default image, which is automatically created on Check Point appliances by the installation or upgrade procedure.
- **Delete** an image from the local system.
- **Export** an existing image. This creates a compressed version of the image. You can download the exported image to a different computer and delete the exported image from the Gaia computer. This saves disk space. You must not rename the exported image. If you rename a snapshot image, it is not possible to revert to it.
- **Import** an exported image.
- View a list of images that are stored locally.

IMPORTANT: Before using Snapshot image management, see the known limitations http://supportcontent.checkpoint.com/solutions?id=sk98068.

Note - During the snapshot creation, all the system processes and services continue to run, and the security policy enforcement does not get interrupted.

Working with Snapshot Management - WebUI

Before you create a snapshot image, make sure the storage computer or appliance fulfills the prerequisites.

To create a snapshot:

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**.

To restore a snapshot:

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 a snapshot:

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 a snapshot:

1. Make sure that there is enough disk space in: `/var/log`
2. In the tree view, click **Maintenance > Image Management**.
3. Select an image.
4. Click **Export**. The **Export Image (name)** window.
5. Click **Start Export**.

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**.

Note - You must not rename the exported image. If you rename a snapshot image, it is not possible to revert to it.

Working with Snapshot Management - CLI (snapshot)

Syntax

```
add snapshot <snapshot name> [desc <string>]
set snapshot {export | import} <snapshot name> path <export path> name <export file>
set snapshot revert <snapshot name>
show snapshot {{<snapshot name> all | date | desc | size} | snapshots}
delete snapshot <name>
```

Backing up the Configuration of the Gaia Operating System

You can back up the configuration of the Gaia operating system and of the Security Management Server database. 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 on a schedule. You can restore a previously saved configuration.

For more, see: sk91400 http://supportcontent.checkpoint.com/solutions?id=sk91400 and sk98068 http://supportcontent.checkpoint.com/solutions?id=sk98068.

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)

Description Create and save the system's configuration.

Syntax `add backup {local | tftp ip` *<ip>* `| {ftp | scp} ip` *<ip>* `username` *<name>* `password plain}`

Parameter	Description
`local`	Save the backup locally, to `/var/CPbackup/backups/`

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

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
```

To monitor the creation of a backup: `show backup status`

To see the status of the last backup: `show backups`

Installing the Gaia Operating System

In This Section:

Changing Gaia Partition Sizes before the OS Installs

On Check Point appliances, the size of the disk partitions is predefined. On Smart-1 50/150/3050/3150 appliances, you can modify the default disk partitions in the first 20 seconds of an installation. The non-interactive installation then continues.

When installing Gaia on an open server, these partitions have default sizes:

- System-swap
- System-root
- Logs
- Backup and upgrade

You can change the System-root and the Logs partition sizes. The storage size assigned for backup and upgrade is updated accordingly.

To see the size of the system-root and log partitions on an installed system:

1. Enter `expert` mode.
2. Run: `df -h`

Most of the remaining space on the disk is reserved for backup images and upgrade.

To see the disk space assigned for backup images:

1. Connect to the Gaia WebUI.
2. Open **Maintenance > Image Management** page.

   On an Open Server, the available space in the **Image Management** page is less than the space you defined when installing Gaia. The difference is the space reserved for upgrades. The amount of reserved space equals the size of the system-root partition.

Note - The minimum recommended space in `/var/log` to support upgrade is 4 GB.

Installing the Gaia Operating System on an Open Server

When you start the Gaia installation, you must select Gaia and press **Enter** in 60 seconds, or the server tries to start from the hard drive. The timer countdown stops when you press **Enter**. There is no time limit for the next steps.

1. Start the server using the installation media.
2. When the first screen shows, select **Install Gaia on the system** and press **Enter.**
3. Press **OK** to continue with the installation.
4. Select a keyboard language. **English US** is the default.
5. Configure the hard disk partitions.
6. Enter and confirm the password for the **admin** account.
7. Select the management interface (default = `eth0`).
8. Configure the management IP address, net mask and default gateway.

   You can define the DHCP server on this interface.
9. Select **OK** to format the hard drive and installation the Gaia operating system.
10. **Reboot** to complete the installation.

Installing the Gaia Operating System on Appliances

You can clean install R80.10 on Gaia Check Point appliances. If the appliance does not have the R80.10 factory image, you can install it using a USB drive or DVD.

For a list of supported appliances, see the *R80.10 Release Notes*.

To install R80.10 on appliances that already have the R80.10 factory image:

1. Open the terminal emulation program.
2. Restart the appliance.
3. When prompted, press any key to enter the boot menu.
4. Select **Reset to factory defaults - Security Management Server** and press **Enter**.
5. Type **yes** and press **Enter**.

   The Security Management Server image is selected for the appliance and then the appliance resets.
6. Configure the Management IP Address ("Configuring the Management IP Address" on page 20).
7. Run the First Time Configuration Wizard ("Running the Gaia First Time Configuration Wizard" on page 21).

To install R80.10 Gaia on UTM-1. 2012 and 3000 series appliances that run an earlier version of Gaia:

1. Download the Gaia Operation System ISO file from the R80.10 Home SK (http://supportcontent.checkpoint.com/solutions?id=sk92965).
2. Create one of these removable installation media:
   - DVD - burn the ISO file onto it
   - Removable USB device - see sk65205 http://supportcontent.checkpoint.com/solutions?id=sk65205 to create it

3. Connect a computer to the console port on the front of the appliance through the supplied DB9 serial cable.
4. Connect to the appliance through a terminal emulation program, using these connection settings:
   a) The connection type - select or enter a serial port
   b) Define the serial port settings: 9600 BPS, 8 bits, no parity, 1 stop bit.
   c) From the **Flow control** list, select **None**.
5. Connect the installation media to the USB port on the appliance.
   For installation from a DVD, connect an external DVD drive, and insert the DVD into it.
6. Reboot the appliance.
   The appliance begins the boot process and status messages show in the terminal emulation window.
7. Redirect boot sequence to the installation media:
   - For installation from a DVD - Press **Enter** within 90 seconds to boot from the installation media.
     Note - If more time elapses, the appliance boots from the hard drive.
   - For intsallation from a removable USB device - In the boot screen, enter **serial** at the **boot** prompt and press *Enter*.

   The R80.10 ISO file is installed on the appliance, and the version and build number show in the terminal emulation window and on the LCD screen.
8. Reboot the appliance - press **CTRL+C**.
   The appliance reboots and shows the model number on the LCD screen.

To install the Gaia Operating System on an IP690, IP1280 and IP2450

R80.10 installations are supported on IP appliances with minimum of 2 cores and 4 GB RAM. To install, see: sk100686 http://supportcontent.checkpoint.com/solutions?id=sk100686.

Configuring the Management IP Address

The management interface is pre-configured with the IP address `192.168.1.1`. You can change the management IP address on a Check Point appliance before or after you run the First Time Configuration Wizard. If you must access the appliance over the network, update the interface before you connect the Gaia appliance to the network. Make sure the new address is on the same subnet as the management network.

You can also install a log server or Multi-Domain Log Server on a Check Point appliance ("Installing Other Servers" on page 35).

To change the Management address before you run the First Time Configuration Wizard:

1. Open a console connection.
2. Log in with the default username and password: `admin` and `admin`.
3. In clish, get the name of the management interface: `# show interfaces`
4. Set the management IP address:
   `# set interface mgmt ipv4-address` *<IPv4 address>* `subnet-mask` *<mask>*

5. Disable the static route to the default gateway that are not used:
   `# set static-route default nexthop gateway address` *<IPv4 address>* `off`
6. Open a browser to the WebUI and run the First Time Configuration Wizard.

To change the management IP address after you run the First Time Configuration Wizard:

1. Open a browser to the WebUI.
2. Open the **Network Management > Network interfaces** window.
3. In the **Management Interface** area, click **Set Management Interface**.
   The **Management Interface** window shows the interface that is configured as the management interface.
4. In the **Interfaces** table, select the management interface and click **Edit**.
5. Change the IP address of the interface.
   Note - This changes the settings of an interface to which the browser connected.
6. Click **OK**.

Running the Gaia First Time Configuration Wizard

The First Time Configuration Wizard helps you configure your appliance quickly. You can change the settings later, in the WebUI.

To start the First Time Configuration Wizard on Gaia:

1. Connect the appliance to your management network through the management interface, which is marked **MGMT**.
2. Open a connection from a browser to the management IP address:
   `https://<appliance_ip_address>`
   The login page opens.
3. Log in to the system with the default username and password: `admin` and `admin`
4. Click **Login**.
   The **First Time Configuration Wizard** runs.
5. In the **Deployment Options** page, click **Continue with Gaia configuration**. Click **Next**.
6. In the **Authentication Details** page, change the default administrator password. Click **Next**.
7. In the **Management Connection** page, enter the IPv4 management interface.
8. **Optional:** In the **Connection to UserCenter** page, configure an external interface to connect to the Check Point UserCenter. Use this connection to download a license and to activate it.
9. In the **Device Information** page:
   - Set the **Host Name** for the appliance.
   - If you configured an interface to the UserCenter, you must configure the IPv4 addresses of **DNS** servers.
   - If you configured an interface to the UserCenter and if you have a Proxy Server to reach the UserCenter, enter the IPv4 address and port for the **Proxy Server**.

   Click **Next**.
10. In the **Date and Time Settings** page, set the date and time manually, or enter the hostname and IPv4 address of the NTP server. Click **Next**.
11. In the **Products** page:
    - To install Multi-Domain Server, select **Multi-Domain Server** and **Primary**.

- To install Security Management Server, select **Security Management** and **Primary**.

You can select **Automatically download Blade Contracts and other important data**. Check Point highly recommends that you select Automatic Downloads (on page 134).

12. In the **Administrator** page, define the name and password of an administrator who can connect to the server with SmartConsole clients. Click **Next**.
13. In the **GUI Clients** page, define IPv4 addresses from which SmartConsole clients can log in. Click **Next**.
14. In the **Activation** page, get a license automatically from the UserCenter and activate it, or use the 15 day trial license. Click **Next**.

    Note: This page is only shown for open servers. The license activation is automatic on appliances.
15. In the **Summary** page, review your choices.

    You can select **Improve product experience by Sending Data to Check Point (on page 134).** Check Point recommends that you select this option. No data is made accessible to third parties.

    Click **Finish**.
16. To start the configuration, click **Yes**.

    A progress bar tracks the configuration of each task.
17. Click **OK**.

    Security Management Server or Multi-Domain Server is installed on the appliance.

Running an Unattended USB Installation of Gaia on Appliances

You can install a Gaia appliance using an ISO on a removable USB drive. To prepare a USB drive, see: sk65205 http://supportcontent.checkpoint.com/solutions?id=sk65205.

For version R77.20 and higher, the ISOmorphic tool lets an administrator run an unattended installation. In an unattended installation (appliances only):

1. An experienced Check Point system administrator prepares the installation media (USB) with these pre-configured settings for specified network interface:
   - IP address
   - Network mask
   - Default gateway
2. Sends the USB drive to an inexperienced administrator who inserts the drive into the appliance and reboots it.

   The tool installs R77.20 (or higher) and configures the appliance with the predefined settings. The LCD indicates a successful installation and interfaces blink in round-robin fashion.
3. The experienced administrator then:
   - Connects to the WebUI and runs the First Time Configuration Wizard, or
   - Opens a command line (SSH) connection to the appliance for further OS level configuration

Note: The ISOmorphic tool does not support unattended installation on open servers.

Installing Security Gateways

In This Section:

Installing Security Gateways on Open Servers

This procedure explains how to install a Security Gateway in a distributed deployment after you install the Operating System.

To install a Security Gateway on Gaia:

1. Open a Web browser to the WebUI:
   `https://`*<Gaia management IP address>*
2. In the Gaia Portal window, log in with the administrator name and password that you defined during the Gaia installation.
3. The WebUI shows the First Time Configuration Wizard.
4. Click **Next**.
5. Select **Continue with R80.10 configuration**, and click **Next**.
6. Configure the **Management Connection**.
7. Configure an **Internet Connection** (optional).
8. Enter the **Device information**:
   - Host Name
   - Domain Name
   - Primary DNS Server
   - Secondary DNS Server
   - Tertiary DNS Server
   - Proxy Settings
9. Configure the **Date and Time Settings** manually, or use the Network Time Protocol (NTP).
10. For the **Installation Type**, select **Security Gateway and/or Security Management**.
11. For the **Product**, make sure only **Security Gateway** is selected.

    Optional: Configure these settings if the Security Gateway is a cluster member:
    - Select **Unit is part of a cluster**
    - Select **ClusterXL** or **VRRP**
    - Select **Primary** or **Secondary**
    - **Log server/SmartEvent only**

    Click **Next**.
12. Answer yes or no to the **Dynamically Assigned IP** question.

13. Define the Secure Internal Communication (SIC) **Activation Key** that is used by the gateway object in SmartConsole.

    The Summary window shows the settings for the appliance.
14. Click **Finish**.

Installing Security Gateways on Appliances

After you install the Gaia operating system, install the Security Gateway.

For a list of supported appliances, see the *R80.10 Release Notes*.

Note - The management IP address can be changed before or after running the First Time Configuration Wizard ("Changing the Management Address Before or After Running the First Time Configuration Wizard" on page 25).

To start the First Time Configuration Wizard on Gaia:

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`

   Note - Make sure that the management interface on the computer is on the same network subnet as the appliance. For example: IP address `192.168.1.x` and Netmask `255.255.255.0`
   You can change the interface in the WebUI, after you complete the First Time Configuration Wizard.
2. Open a connection from a browser to the management IP address.

   The login page opens.
3. Log in to the system with the default username and password: `admin` and `admin`
4. Click **Login**.

   The **First Time Configuration Wizard** runs.
5. Follow the instructions on the screen.

   Note - Settings that you configure in the First Time Configuration Wizard, can be changed later in the WebUI, from an Internet browser go to `https://<appliance_ip_address>`

To configure Gaia Security Gateway appliances:

1. Open a Web browser to the WebUI:

   `https://`*<Gaia management IP address>*
2. In the Gaia Portal window, log in with the administrator name and password that you defined during the Gaia installation.
3. The WebUI shows the First Time Configuration Wizard.
4. Click **Next**.
5. Select **Continue with R80.10 configuration**, and click **Next**.
6. Configure the **Management Connection**.
7. Configure an **Internet Connection** (optional).
8. Enter the **Device information**:
   - Host Name
   - Domain Name

- Primary DNS Server
- Secondary DNS Server
- Tertiary DNS Server
- Proxy Settings

9. Configure the **Date and Time Settings** manually, or use the Network Time Protocol (NTP).
10. For the **Installation Type**, select **Security Gateway and/or Security Management**.
11. For the **Product**, make sure only **Security Gateway** is selected.

    Optional: Configure these settings if the Security Gateway is a cluster member:
    - Select **Unit is part of a cluster**
    - Select **ClusterXL** or **VRRP**
    - Select **Primary** or **Secondary**
    - **Log server/SmartEvent only**

    Click **Next**.
12. Answer yes or no to the **Dynamically Assigned IP** question.
13. Define the Secure Internal Communication (SIC) **Activation Key** that is used by the gateway object in SmartConsole.

    The Summary window shows the settings for the appliance.
14. Click **Finish**.

To change the management IP address after running the First Time Configuration Wizard:

1. Open the WebUI.
2. Open the **Network Management > Network interfaces** window.
3. In the **Management Interface** area, click **Set Management Interface**.
4. The Management interface window shows which interface is configured as the management interface.
5. In **Interfaces** table, select the management interface and click **Edit**.
6. Change the IP address of the interface.

   Note - This changes the settings of an interface the browser is currently connecting to.
7. Click **OK**.

Changing the Management Address Before or After Running the First Time Configuration Wizard

Use the console connection to configure the management interface before connecting the Gaia appliance to the network. Once the management interface has this address, you can connect through a browser over the network and run the First Time Configuration Wizard.

To change the Management address before running the First Time Configuration Wizard:

1. Open a console connection.
2. Log in using the default username and password: `admin` and `admin`.
3. Run the `show interfaces` command to get the name of the management interface.

4. In clish, set the management interface using:
   `set interface mgmt ipv4-address <IPv4 address> subnet-mask <mask>`
5. Set the static route to the default gateway using:
   `set static-route default nexthop gateway address <ip address> on`
6. Through a browser, connect to the WebUI and run the First Time Configuration Wizard.

To change the management IP address after running the First Time Configuration Wizard:

1. Open the WebUI.
2. Open the **Network Management > Network interfaces** window.
3. In the **Management Interface** area, click **Set Management Interface**.
4. The Management interface window shows which interface is configured as the management interface.
5. In **Interfaces** table, select the management interface and click **Edit**.
6. Change the IP address of the interface.
   Note - This changes the settings of an interface the browser is currently connecting to.
7. Click **OK**.

Configuring a Standalone Appliance

You can configure a Check Point Standalone appliance using the Check Point First Time Configuration Wizard in one of these modes:

- Standard - supported on all appliances running all R80.10 Gaia versions
- Quick Setup - supported only on these appliances

Appliances	Model Numbers
2012 Series	4200,4400,4600,4800,12200,12400,12600,21400,13500,21700,13500,13800,21800
3000 Series	3200,5200,5400,5600,5800,15400,15600,23500,23800

For more on Gaia Quick Standalone Setup, see: sk102231
http://supportcontent.checkpoint.com/solutions?id=sk102231.

To configure Check Point products on an appliance running Gaia Operating System, the administrator uses the IP address of the management interface on the appliance. The default is 192.168.1.1, but you can change it. If you change the management interface IP address, make sure it is on the same subnet as the management network, so that you can access the appliance from a remote computer over the network. You can change the management IP address before, during, or after running the First Time Configuration Wizard. If you change the management IP address during the First Time Configuration Wizard, the warning shows: Your IP address has been changed. In order to maintain the browser connection, the old IP address will be retained as a secondary IP address.

To change the management IP address before running the First Time Configuration Wizard:

1. Open a console connection to the appliance using the default management IP address.

2. Log in using the default credentials:
   - username - `admin`
   - password - `admin`
3. Run the `show interfaces` command to get the name of the management interface.
4. In clish, run this command to set the management interface:
   `set interface mgmt ipv4-address <IPv4 address> subnet-mask <mask>`
5. Run this command to configure the static route to the default gateway:
   `set static-route default nexthop gateway address <ip address> on`

Now, you can use the configured management IP address to connect through a browser with the WebUI and to run the First Time Configuration Wizard.

Note - On a UTM-1 appliance, the internal interface (INT) is used as an interface.

To change the management IP address after running the First Time Configuration Wizard:

1. Open a browser connection to the default management IP address.
2. In WebUI, go to **Network Management > Network interfaces**.
3. In the **Management Interface** area, click **Set Management Interface**.
4. The **Management interface** window shows which interface is configured as the management interface.
5. In **Interfaces** table, select the management interface and click **Edit**.
6. Change the IP address of the interface.

   Note - The connection will drop, because the settings of an interface the browser is currently connecting to are changed.
7. Click **OK**.

To configure a Standalone appliance using First Time Configuration Wizard in the standard mode:

1. Connect the appliance to the management network through the management interface (**MGMT**).
2. On a computer that is connected to the management network, open a web browser to the management IP address on the appliance.

   The login page opens.
3. Log in with the default credentials:
   - username - `admin`
   - password - `admin`
4. Click **Login**.

   The First Time Configuration Wizard starts and the **Welcome** screen shows.
5. Click **Next**.
6. In the **Setup** section of **Deployment Options** view, select **Continue with Gaia R80.10 configuration** and click **Next**.
7. Change the default **administrator password** and click **Next**.
8. Configure the **Management Connection** settings:
   - **IPv4 address** and **Subnet mask** of the management interface

Note - You can leave the IP address and the subnet mask unchanged. It is either the factory default address or the latest address that the administrator configured.

- IPv4 address of the **Default Gateway**
- **Configure IPv6** (optional) -
  - Select **On** from the drop-down menu (by default, it is off)
  - Enter the **IPv6 address** and **Subnet** mask of the management interface
  - Enter the IPv6 address of the **Default Gateway**

9. Click **Next**.
10. Configure **Connection to UserCenter** settings (optional) - an additional interface for remote management:
    - **Interface** - select an interface on the appliance
    - Configure IPv4 -
      - Select **On** from the drop-down menu (by default, it is off)
      - Enter the **IPv4 address** and **Subnet mask** of the interface
    - Configure IPv6 -
      - Select **On** from the drop-down menu (by default, it is off)
      - Enter the **IPv6 address** and **Subnet** mask of the interface
11. Click **Next**.
12. Configure the **Date and Time Settings** in one of these ways:
    - **Manually**
    - **Configure the NTP server** - define the **hostname** and the **IP address** (IPv4 or IPv6)
13. Click **Next**.
14. In the **Products** window, select **Security Gateway** and **Security Management**

    If the unit is part of a cluster:
15. Select the cluster type: **ClusterXL** or **VRRP Cluster**
    - Define the **Management** as **Primary**, **Secondary**, or **Log Server/SmartEvent Only**
    - Enter the **Cluster Global ID** - only on versions R77.30 and later
16. Click **Next**.
17. Define login credentials for the Security Management Server administrator account - **Name** and **New Password**
18. Click **Next**.
19. Define SmartConsole clients that can log in to the Security Management Server:
    - For **This machine** or **Network** - an IPv4 or an IPv6 address
    - Range of IPv4 addresses
20. Click **Next**.
21. For 2012 series only -

    a) Get a license automatically from the UserCenter and activate it, or use the trial license.

    b) If there is a proxy server between the appliance and the Internet, enter its IP address and port.

    c) Click **Next**.
22. Review the summary, make sure it is correct, and click **Finish**.
23. On 2012 models only, click **Yes t**o start the configuration process.

    A progress bar tracks the configuration of each task.

24. Click **OK** to finish the installation.

    If the **Help Check Point Improve Upgrades (CPUSE)** window shows, click **Yes** or **No**.

After Gaia R80.10 is installed on the appliance, you can also download the SmartConsole using the Gaia WebUI.

To download the SmartConsole:

1. Open a web browser and connect to: `https://<management_ip_address>`
2. In the **Overview** page of the WebUI, click **Download Now!**

When you configure a Standalone appliance in **Quick Setup** mode, these products settings are configured:

- Security Gateway - in bridge or monitor mode
- Security Management Server with these blades:
  - Firewall Software Blade - with Any-Any-Accept default policy and logging of a few common protocols
  - IPS Software Blade - set to inspect all traffic and has troubleshooting turned on by default
  - Application Control and URL Filtering Software Blades - each with Any-Any-Log policy, set to run in the background, and with fail-open mode turned on
  - Anti-Bot Software Blade
  - Anti-Virus Software Blade
  - Threat Emulation Software Blade - in ThreatCloud mode
  - SmartEvent Software Blade - with detect-only policy, set to scan all file types in both directions, and set to run in the background

    Note - Anti-Bot, Anti-Virus, and Threat Emulation are not installed on 2200 series appliances

To configure a Standalone appliance using First Time Configuration Wizard in the Quick Setup mode:

1. Connect the appliance to the management network through the management interface (**MGMT**).
2. On a computer that is connected to the management network, open a web browser to the management IP address on the appliance.

   The login page opens.
3. Log in with the default credentials:
   - username - `admin`
   - password - `admin`
4. Click **Login**.

   The First Time Configuration Wizard starts and the **Welcome** screen shows.
5. Click **Next**.
6. In the **Setup** section of **Deployment Options** view, select **Quick Standalone setup of Gaia <latest_version>** and click **Next**.
7. In the **Quick Setup** window, configure settings in these sections:
   - **Management** - New **IPv4 address** and **Subnet mask**

Note - You can leave the IP address and the subnet mask unchanged. It is either the factory default address or the latest address that the administrator configured.

- **Authentication** - **New Password** (make sure to **Confirm Password**) for the Gaia OS and the Security Management Server *admin* account
- **Networking** -
  - **IPv4 Address (<int>)** and **Subnet mask** (optional) of the additional interface for remote access
  - **Default gateway** - make sure it is in the same subnet as the **Management** IP address (if you use the new interface for management, the address of the default gateway must be in the same subnet as the address of the new interface)
  - **DNS** server IP address (optional)
  - Proxy server (optional) - select **Proxy server** and enter the **Address** and the **Port number**
  - **Topology** - select **Monitor mode** or **Bridge mode**
  - To verify connectivity, click **Test Connectivity**.

8. Click **Next**.
9. Review the summary, make sure it is correct, and click **Finish**.

Note - In **Quick Setup** mode, date and time are automatically synchronized with those on the PC that is used to run the First Time Configuration Wizard.

After the First Time Configuration Wizard runs in **Quick Setup** mode, the latest R80.10 version of the Security Checkup is installed and can be used with R77.30 or a later version of SmartConsole.

If you want to convert the standalone appliance into a gateway only, and manage it with an existing Security Management Server, you can download and run this script on the appliance:

```
# /bin/standlone_to_gw_registry_update.sh
$CPDIR/registry/HKLM_registry.data
```

Notes -

- Quick Setup cannot be used to reconfigure Security Gateways of different versions
- Quick Setup does not automatically activate the Standalone configuration products - the 15 days trial license is used until the products are activated
- After the Quick Setup configuration runs, to activate Threat Emulation Software Blade, you must activate the Standalone on the appliance

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* http://www.bluecoat.com/user/login/customer_portal (password required).

To install a VSX Gateway:

1. Install and configure the R80.10 ISO file on the VSX Gateway.

   The steps are different if the VSX Gateway is on an appliance ("Installing Security Gateways on Appliances" on page 24) or an Open Server ("Installing Security Gateways on Open Servers" on page 23).

   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. Complete the on-screen instructions.
6. Install the necessary licenses on the VSX Gateway.

Installing a Security Management Server

In This Section:

Installing a Security Management Server using CPUSE

With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself. The software update packages and full images are for major releases, minor releases and Hotfixes. All of the CPUSE processes are handled by the Deployment Agent daemon (DA).

Gaia automatically locates and shows the available software update packages and full images that are relevant to the Gaia operating system version installed on the computer, the computer's role (gateway, Security Management Server, standalone), and other specific properties. The images and packages can be downloaded from the Check Point Support center and installed.

For more about CPUSE, see sk92449 http://supportcontent.checkpoint.com/solutions?id=sk92449.

Software Update Requirements

- At least 4 GB free disk space in `/var/log`
- Un-partitioned free disk space should be at least the size of root partition. To find out the:
  - Amount of un-partitioned free disk space, run: `pvs`
  - Size of the root partition, run: `df -h`

To update the Gaia Software Updates agent:

1. Make sure the proxy and the DNS server are configured.
2. In the WebUI, go to **Upgrades (CPUSE) > Software Updates Policy**.
3. In the **Software Deployment Policy** section. select one of these options:
   - **Manually** – Do the procedure described in the CPUSE sk http://supportcontent.checkpoint.com/solutions?id=sk92449
   - **Scheduled** or **Automatic** – the latest Deployment Agent is downloaded and automatically installed.
   - **Periodically update new Deployment Agent version** - Updates only the DA according to the configured time period.
4. Click **Apply**.

To install R80.10 using Upgrades (CPUSE) - WebUI:

1. Open **Upgrades (CPUSE)** > **Status and Actions**.
2. Click **Major Versions**.
3. Select the R80.10 image.

4. Click **Download**.
5. To make sure the installation is allowed, click **Actions > Verifier.**
6. Click **OK**.

   The Installation **verified - Installation is allowed** window shows. Verification is complete.
7. Click **Clean Install**.
8. Reboot.

Configuring a Security Management Server on Gaia

To install and configure Check Point products on Gaia, use the First Time Configuration Wizard ("Running the Gaia First Time Configuration Wizard" on page 21) or configure the operating system and install the products in the WebUI.

To configure Security Management Server on Gaia:

1. Open a browser to the WebUI: `https://`*<Gaia management IP address>*
2. In the **Gaia Portal** window, log in with the administrator name and password that you defined during Gaia installation.
3. The WebUI shows the **First Time Configuration Wizard**. Click **Next**.
4. Select **Continue with R80.10 configuration**. Click **Next**.
5. If you did not change the default administrator password, do it now. Click **Next**.
6. Set an 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.
7. Optional: Configure an **Internet Connection**.
8. Enter the **host name** of the server.

   Optional:

   - Enter the **domain name**, and IPv4 addresses for the **DNS servers**.
   - Set the IP Address and Port for a Proxy Server.

   Click **Next**.
9. Configure the **Date and Time Settings** manually, or enter the hostname and IPv4 address of the NTP server. Click **Next**.
10. Select **Security Gateway and/or Security Management**. Click **Next**.
11. Make sure **Security Management** is the only product selected. Click **Next**.
12. Use the Gaia administrator account, or define a new administrator for the Security Management Server administrator account. Click **Next**.
13. Define IPv4 addresses from which SmartConsole clients can log in to the Security Management Server. Click **Next**.
14. Review the summary and then click **Finish**.
15. Click **Yes** when prompted to start the configuration process.

    A progress bar tracks the configuration of each task.
16. Click **OK**.
17. If the **Help Check Point Improve Upgrades (CPUSE)** window shows, click **Yes** or **No**. Check Point recommends that you click Yes. Your data is never shared with third parties.

Installing a Security Management Server on Linux

To install a Security Management Server on Red Hat Enterprise Linux, see sk98760
http://supportcontent.checkpoint.com/solutions?id=sk98760

Installing Other Servers

In This Section:

This section explains how to install secondary management server, log servers, and SmartEvent servers.

Installing Endpoint Security

The Network Security Management Server can also be an Endpoint Security Management Server.

Installing Endpoint Security Servers

Use the installation instructions in this guide to install Security Management Servers. You can enable the Endpoint Security Management Server after the Security Management Server installation is completed.

To enable an Endpoint Security Management Server:

1. Use the instructions in this guide to install a Security Management Server.
2. In SmartDashboard, open the Security Management Server object.
3. Enable the **Endpoint Policy Management** blade.
4. In SmartConsole, install policy.

Check Point Cloud Services for Endpoint

After the Endpoint Security Management Server is enabled on the Security Management Server, these components communicate with the Check Point cloud services:

- Endpoint Anti-Malware Software Blade – Downloads updates from the Check Point Malware Update Server. These updates are mandatory for the correct functioning of the Anti-Malware Software Blade. Preventing them causes severe security issues, because the blade does not operate with the latest malware information database.
- Endpoint Anti-Malware Software Blade – Sends suspected malware to the Check Point ThreatCloud Server. These updates increase the accuracy of malware detection by Check Point Endpoint Security clients and Check Point Security Appliances. To turn them off, modify the Anti-Malware rule in the Organizational Security Policy in SmartEndpoint.
- Endpoint Application Control Software Blade – Downloads information about classified known applications from the Check Point ThreatCloud Server and sends unknown applications for analysis. These updates are mandatory for the correct functioning of the Endpoint Application Control Software Blade. Without these updates, the blade is unable to classify malicious applications and automatically distinguish between them and non-malicious ones.

To enable an Endpoint Policy Server:

1. Use the instructions in this guide to install a **Log Server**.
2. Connect from SmartConsole to the Endpoint Security Management Server.
3. Create a new Log Server object.
4. Enable the **Endpoint Policy Management** and **Logging & Status** management Software Blades.
5. Install policy

When the Endpoint Policy Management blade is enabled, the Gaia WebUI port changes from 443 to 4434. If you disable the blade, the port changes back to 443.

Disk Space for Endpoint Security

We recommend that you have at least 10 GB available for Endpoint Security in the Root disk partition. Client packages and release files are stored under the Root partition.

The files include:

- 4 GB - Security Management Server installation files.
- 2 GB or more - Client files (each additional version of client packages requires 1GB of disk space).
- 1 GB - Logs.
- 1 GB - High Availability support (more can be required in large environments).

Note - To make future upgrades easier, we recommend that you use a larger disk size than necessary in this deployment.

Installing a Log Server for Security Management Server

You can install a dedicated log server on a Gaia appliance or open server. 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:

1. In the First Time Configuration Wizard **Products** page, select **Security Management**.
2. Define the Security Management as a **Log Server**.

Installing a SmartEvent Server

You can install a dedicated SmartEvent server on Gaia appliances or open servers.

To install a SmartEvent server:

- In the First Time Configuration Wizard **Products** page, select **Log Server/SmartEvent only**.
- In the **Secure Internal Communication (SIC)** page, define the **Activation Key**. Use this key to configure the dedicated server for SmartEvent object in SmartDashboard.

Minimum Disk Space

The Security Management Server or Log Server with log indexing enabled, creates and uses index files for fast access to log file content. Index files are located by default at `$RTDIR/log_indexes`.

To make sure that there is always sufficient disk space on the server, the server that stores the log index deletes the oldest index entries when the available disk space is less than a specified minimum. The default minimum value is 5000 MB, or 15% of the available disk space.

To change the minimum available disk space for Logs and indexes:

1. In SmartConsole, edit the Security Management Server or Log Server or SmartEvent network object.
2. Open **Logs > Storage**.
3. Select **When disk space is below <number> Mbytes, start deleting old log files**.
4. Change the disk space value.

   Note - In a Multi-Domain Security Management environment, the disk space for logs and indexes is controlled by the Multi-Domain Server, and applies to all Domain Management Servers. Configure the disk space on the Multi-Domain Server object.

Installing Multi-Domain Security Management

In This Section:

Installing Multi-Domain Server on Smart-1 Appliances

Install a Multi-Domain Server on supported Smart-1 models.

To install Multi-Domain Server on an appliance:

1. Install the Gaia operating system on the appliance using Upgrades(CPUSE) ("Installing a Security Management Server using CPUSE" on page 32). Alternatively, follow the procedure for UTM-1 and 2012 Models.
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 a Multi-Domain Server on Smart-1 appliances:

1. **This step applies to R77.10 and higher.** For other Gaia releases, configure these options in the Gaia WebUI, in the **Image Management** page.

   In the **Deployment Options** page, select **Continue with Gaia configuration**. Other options are:

   Clean install

- Install a version from the Check Point Cloud.
- Install from a USB device.

Recovery

- Automatic version recovery from the Check Point Cloud.
- Import an existing snapshot.

Click **Next**.

2. In the **Authentication Details** page, change the default administrator password.
   Click **Next**.
3. In the **Management Connection** page, set an IPv4 and an IPv6 address for the management interface, or set one IP address (IPv4 or IPv6).
   You can change the Management IP address. Gaia automatically creates a secondary interface to keep connectivity when the management interface is not available. After you complete the First Time Configuration Wizard, you can remove this interface in the **Interface Management > Network Interfaces** page.
4. **Optional:** In the **Connection to UserCenter** page, configure an external interface to connect to the Check Point UserCenter. Use this connection to download a license and activate it. Alternatively, use the trial license. To connect to the UserCenter, you must also configure DNS and (if applicable) a Proxy Server, in the **Device Information** page of the Wizard.
5. In the **Device Information** page, set the **Host Name** for the appliance.
   Optional:
   - Set the domain name, and IPv4 or IPv6 addresses for the DNS servers.
   - To connect to the UserCenter, set the IP Address and Port for a Proxy Server. Do this if you want to activate the appliance by downloading a license from the UserCenter.

   Click **Next**.
6. In the **Date and Time Settings** page, set the date and time manually, or enter the hostname, IPv4 address or IPv6 address of the NTP server.
   Click **Next**.
7. **This step does not apply to R77.20 and higher or Smart-1 205/210/225/3050/3150:**
   In the **Appliance Type** page, select **Smart-1 appliance**.
   Click **Next**.
8. In the **Products** page, select **Multi-Domain Server** and **Primary.**
   For R77.10 and higher: **Automatically download Blade Contracts and other important data**. Check Point highly recommends that you select Automatic Downloads (on page 134).
9. In the **Security Management Administrator** page, define the name and password of a Superuser administrator that can connect to the Multi-Domain Server using SmartConsole clients.
   Click **Next**.
10. In the **Multi-Domain Server GUI Clients** page, define IP addresses from which SmartConsole clients can log in to the Multi-Domain Server.
    Click **Next**.
11. In the **Appliance Activation** page, get a license automatically from the UserCenter and activate it, or use the 15 day trial license.
    Click **Next**.
12. In the **Summary** page, review your choices
    Optional: Improve product experience by Sending Data to Check Point (on page 134).
    Click **Finish**.

13. To start the configuration, click **Yes**.

    A progress bar tracks the configuration of each task.

14. Click **OK**.

    The Multi-Domain Server is installed on the appliance.

15. If necessary, download SmartConsole from the Gaia WebUI.

    a) Open a connection from a browser to the WebUI: `https://<management_ip_address>`

    b) In the **Overview** page, click **Download Now**.

16. In the **Products** page, select **Multi-Domain Server** and **Primary.**

    For R77.10 and higher: **Automatically download Blade Contracts and other important data**. Check Point highly recommends that you select Automatic Downloads (on page 134).

17. In the **Security Management Administrator** page, define the name and password of a Superuser administrator that can connect to the Multi-Domain Server using SmartConsole clients.

    Click **Next**.

18. In the **Multi-Domain Server GUI Clients** page, define IP addresses from which SmartConsole clients can log in to the Multi-Domain Server.

    - If you select **This machine** or **Network**, define an IPv4 or an IPv6 address.
    - You can also select a range of IPv4 addresses.

    Click **Next**.

19. In the **Appliance Activation** page, get a license automatically from the UserCenter and activate it, or use the 15 day trial license.

    Click **Next**.

20. In the **Summary** page, review your choices

    Optional: Improve product experience by Sending Data to Check Point (on page 134).

    Click **Finish**.

21. To start the configuration, click **Yes**.

    A progress bar tracks the configuration of each task.

22. Click **OK**.

23.

    The Multi-Domain Server is installed on the appliance.

24. If necessary, download SmartConsole from the Gaia WebUI.

    a) Open a connection from a browser to the WebUI: `https://<management_ip_address>`

    b) In the **Overview** page, click **Download Now!**

To configure a secondary Multi-Domain Server on appliances:

Use the same procedure as for the primary Multi-Domain Server with these changes:

- Use a different IP address for the management interface on the secondary appliance.
- 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.

Installing Multi-Domain Server on Gaia Open Servers

To install and configure Check Point products on Gaia, use the First Time Configuration Wizard ("Running the Gaia First Time Configuration Wizard" on page 21) or configure the operating system and install the products in the WebUI.

To install Multi-Domain Server on a Gaia open server:

1. Open a browser to the WebUI: `https://`*<Gaia management IP address>*
2. In the **Gaia Portal** window, log in with the administrator name and password that you defined during Gaia installation.
3. The WebUI shows the **First Time Configuration Wizard**. Click **Next**.
4. Select **Continue with R80.10 configuration**. Click **Next**.
5. Set an 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.

   Click **Next**.
6. Enter the **host name** of the server.

   Optional:

   - Enter the **domain name**, and IPv4 addresses for the **DNS servers**.
   - Set the IP Address and Port for a Proxy Server.

   Click **Next**.
7. Set the date and time manually, or enter the hostname and IPv4 address of the NTP server. Click **Next**.
8. Enter the username and password for the Security Management Server administrator account. Click **Next**.
9. For **Installation Type**, select **Multi-Domain Server**. Click **Next**.
10. For the type of server, select **Primary Multi-Domain Server**.
11. Select the **Leading VIP Interfaces**.

    Leading interfaces are physical interfaces that connect to the external network. These interfaces are for Domain Management Server virtual IP addresses. Each leading VIP interface can have up to 250 virtual IP addresses (250 Domain Management Servers).
12. Configure the GUI clients that can log into the Multi-Domain Server. Click **Next**.
13. Set the **Name** and **Password** for the Multi-Domain Server administrator account. Click **Next**.
14. Review the summary and then click **Finish**.
15. Click **Yes** when prompted to start the configuration process.

    A progress bar tracks the configuration of each task.
16. Click **OK**.
17. If the **Help Check Point Improve Upgrades (CPUSE)** window shows, click **Yes** or **No**. Check Point recommends that you click Yes. Your data is never shared with third parties.

Installing a Multi-Domain Log Server

You can install a dedicated Multi-Domain Log Server on a Gaia appliance or open server. Start to install the products as for a Multi-Domain Server, but stop at the step where you select components.

To install a Multi-Domain Log Server:

1. In the First Time Configuration Wizard **Products** page, select **Multi-Domain Log Server**.
2. In the **Secure Internal Communication (SIC)** page, define the **Activation Key**.

Post-Installation Configuration

You can use the Check Point configuration tool (`cpconfig` for Security Management Server or `mdsconfig` for Multi-Domain Security Management) 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.

  Make sure that no firewall blocks port 19009 between the management server and 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.

Enabling IPv6 on Gaia

IPv6 is automatically enabled if you configure IPv6 addresses in the First Time Configuration Wizard.

If you did not do this, enable IPv6 in one of the following ways:

To enable IPv6 using clish:

```
# set ipv6-state on
# save config
# reboot
```

To enable IPv6 using the WebUI:

1. In the WebUI navigation tree, select **System Management > system Configuration**.
2. For **IPv6 Support**, select **On**.
3. When prompted, select **Yes** to reboot.

Installing SmartConsole Clients

In This Section:

SmartDashboard and SmartConsole are used to manage the Security Management Server and Security Gateways.

For SmartConsole requirements, see the *Release Notes*.

To install the SmartConsole clients on Windows platforms:

1. Insert the R80.10 distribution media or download the SmartConsole application from the *Support Center* http://supportcontent.checkpoint.com/solutions?id=sk111841.
2. Run the **SmartConsole** executable.
3. Continue with the instructions on the screen.

Logging in to SmartConsole

To log in to SmartConsole clients:

1. Open the SmartConsole application.
2. Enter the host name or IP address of the Security Management Server or Multi-Domain Server.

   The management server authenticates the connection when you log in for the first time. Multiple administrators can be logged in at one time.
3. Enter your administrator credentials or select the certificate file.
4. Click **Login**.
5. 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.

Troubleshooting SmartConsole

If you disable control connections for implicit rules (**Global Properties** > **FireWall**), you must open ports for SmartConsole to communicate with the Security Management Server.

Make sure the SmartConsole computer can access these ports on the server:

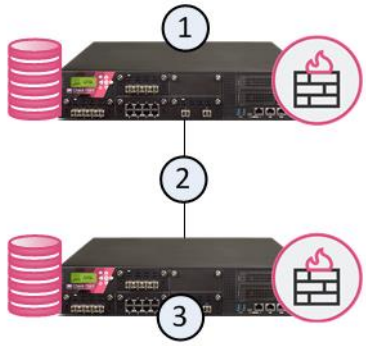
- 18190
- 18264

High Availability

In This Section:

Understanding Standalone Full High Availability on Appliances

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 - active
2	Direct appliance to appliance connection
3	Backup appliance - standby

- 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 operating system, 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.

Note - SmartEvent Server and SmartReporter are not supported in Management High Availability and ClusterXL Full High Availability environments. For these environments, install SmartEvent Server and SmartReporter on dedicated machines.

For more, see sk25164 http://supportcontent.checkpoint.com/solutions?id=sk25164

Installing Standalone Full High Availability on Gaia Appliances

Installing Standalone Full High Availability on Gaia appliances.

To configure the primary management:

1. Connect the appliance to your management network through the management interface, which is marked **MGMT**.
2. Open a connection from a browser to the management IP address:
   `https://<appliance_ip_address>`
   The login page opens.
3. Log in to the system with the default username and password: `admin` and `admin`
4. Click **Login**.
   The **First Time Configuration Wizard** runs.
5. Select **Continue with configuration of Gaia R80.10**.
6. Click **Next**.
7. Set the username and password for the administrator account and then click **Next**.
8. Click **Next**.
9. Set an IPv4 address for the management interface.
   The IP address is automatically taken from the Gaia operating system. 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.
10. Internet Connection -- optionally define a second interface for the appliance.
11. Set the **host name** for the appliance.
    Optional:
    - Set the **domain name**, and IP addresses for the **DNS servers**.
    - Set the IP Address and Port for a Proxy Server
12. Click **Next**.
13. Set the date and time manually, or enter the hostname and IPv4 address of the NTP server.
14. Click **Next**.
15. Select **Security Gateway** and **Security Management**.
16. Configure these **Advanced** settings:
    - Select **Unit is part of a cluster**
    - Select **ClusterXL**
    - Select **Primary**

    Click **Next**.
17. Set the username and password for the Security Management Server administrator account and then click **Next**.
18. Define IP addresses from which SmartConsole clients can log in to the Security Management Server.
    - Any IP Address
    - If you select **This machine** or **Network**, define an IPv4 address.
    - You can also select a range of IPv4 addresses.

19. Click **Next**.
20. Click **Next**.
21. Review the summary and, if correct, click **Finish**.
22. To start the configuration process, click **Yes**.

    A progress bar tracks the configuration of each task.
23. When prompted to reboot, click **OK**.

    Gaia R80.10 is installed on the appliance.
24. Log in to the Gaia WebUI with the new management IP address that you entered in the First Time Configuration Wizard.
25. Double-click the **SYNC** or **eth1** interface and configure the settings. This interface is used to synchronize with the other appliance. Click **Apply**.
26. Configure the settings for other interfaces that you are using.
27. Use a cross-over cable to connect the **SYNC** or **eth1** interfaces on the two appliances.
28. If necessary, download SmartConsole from the Gaia WebUI.

    a) Open a connection from a browser to the WebUI: `https://<management_ip_address>`

    b) In the **Overview** page, click **Download Now!**

To configure the secondary management:

1. Connect the appliance to your management network through the management interface, which is marked **MGMT**.
2. Open a connection from a browser to the management IP address: `https://<appliance_ip_address>`

   The login page opens.
3. Log in to the system with the default username and password: `admin` and `admin`
4. Click **Login**.

   The **First Time Configuration Wizard** runs.
5. Select **Continue with configuration of Gaia R80.10**.
6. Click **Next**.
7. In the First Time Configuration Wizard, set the username and password for the administrator account and then click **Next**.
8. Set an IPv4 address for the management interface.

   The primary and secondary management servers must have different IP addresses.
9. Internet Connection -- optionally define a second interface for the appliance.
10. Set the **host name** for the appliance.

    Optional:

    - Set the **domain name**, and IPv4 addresses for the **DNS servers**.
    - Set the IP Address and Port for a Proxy Server
11. Click **Next**.
12. Set the date and time manually, or enter the hostname and IPv4 address of the NTP server.
13. Click **Next**.
14. Select **Security Gateway** and **Security Management**.
15. Configure these **Advanced** settings:
    - Select **Unit is part of a cluster**
    - Select **ClusterXL**

- Select **Secondary**

Click **Next**.

16. Define the Secure Internal Communication (SIC) **Activation Key** that is used by the gateway object in SmartConsole and then click **Next**.
17. Review the summary and, if correct, click **Finish**.
18. To start the configuration process, click **Yes**.

    A progress bar tracks the configuration of each task.
19. Click **OK**.

    Gaia R80.10 is installed on the appliance.
20. Log in to the Gaia WebUI with the new management IP address that you entered in the First Time Configuration Wizard.
21. Double-click the **SYNC** or **eth1** interface and configure the settings. This interface is used to synchronize with the other appliance.

    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.

    Click **Apply**.
22. Configure the settings for other interfaces that you are using.
23. Make sure a cross-over cable connects the **SYNC** or **eth1** interfaces on the two appliances.
24. If necessary, download SmartConsole from the Gaia WebUI.

    a) Open a connection from a browser to the WebUI: `https://<management_ip_address>`

    b) In the **Overview** page, click **Download Now!**

Upgrading Standalone Full High Availability Gaia Appliances

After upgrading a Full High Availability deployment to R80.10, you must re-establish SIC between the active and standby members.

Configuring Standalone Full High Availability on Appliances

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 a Log Server for Security Management Server" on page 36).

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.

Configuring Management High Availability

You can install a Primary and Secondary server on two Smart-1 appliances or two open servers. The databases are synchronized. If the Primary is Active and goes down, the Secondary server becomes Active.

Prerequisites for Management High Availability

- The Primary and Secondary servers must be R80.10 clean installed from the same ISO. If they are open servers, they must have the same operating system (Gaia).
- To enable SmartEvent, see sk25164 http://supportcontent.checkpoint.com/solutions?id=sk25164

High-Level Workflow to install and configure Management High Availability:

1. Configure the primary server with the First Time Configuration Wizard.
2. Configure the secondary server with the First Time Configuration Wizard:
   - In the **Management Connection** page, use a different IP address for the management interface on the secondary appliance.
   - In the **Products** page, select **Secondary**.

     If prompted to install a Primary Multi-Domain Server, enter **no**.
   - In the **Secure Internal Communication (SIC)** page, define the **Activation Key**. Use this key to configure the secondary server object in SmartDashboard.
3. From SmartConsole:

   a) Log in to the primary server.

   b) Create a Check Point Host object for the secondary server.

   c) Initialize SIC with the secondary server.

   Note - For more about configuring High Availability for Security Management Servers, see the R80.10 *Security Management Guide*.

   For information about how to configure High Availability for a Multi-Domain Server deployment, see the R80.10 *Multi-Domain Server Administration Guide*.

Deleting the IPv4 Address from Management High Availability

You can remove the IPv4 address from one member in a management High Availability environment and keep the IPv6 and IPv4 addresses on the second member.

To remove the IPv4 address from a management HA member:

1. Open the WebUI.
2. In the **Network Management > Network Interfaces** page, delete the IPV4 address.
3. Open SmartDashboard.
4. Reset SIC.
5. Install the database (**Policy > Install Database**).
6. Reboot.

7. Synchronize the databases of the Security Management Servers.

Using Monitor Mode

Configure Monitor Mode on Security Gateway interfaces, to monitor traffic from a mirror port or span port on a switch. Use Monitor Mode to analyze network traffic without changing the production environment. The mirror port on a switch duplicates the network traffic and sends it to the monitor interface on the gateway to record the activity logs.

You can use mirror ports:

- To monitor the use of applications as a permanent part of your deployment
- To evaluate the capabilities of the Application Control and IPS blades before you buy them

The mirror port does not enforce a policy or run active operations (prevent, drop, reject) on network traffic. It can be used only to evaluate the monitoring and detecting capabilities of the Software Blades. All duplicated packets that arrive at the monitor interface of the gateway are terminated and will not be forwarded. The Security Gateway does not send traffic through the monitor interface.

Supported Software Blades for Monitor Mode

These Software Blades support Monitor mode for Security Gateway deployment:

Supported Blade	Supports Gateways in Monitor Mode	Supports Virtual System in Monitor Mode
Firewall	Yes	Yes
IPS	Yes	Yes
URL Filtering	Yes	Yes
DLP	Yes	No
Anti-Bot	Yes	Yes
Application Control	Yes	Yes
Identity Awareness	Yes	No
Threat Emulation	Yes	Yes

Unsupported Software Blades for Monitor Mode

These features, Software Blades and deployments are not supported in Monitor mode:

- NAT
- IPsec VPN
- HTTPS Inspection
- Mobile Access

- DLP with FTP
- HTTP/HTTPS proxy
- Anti-Spam and Email Security
- QoS
- Traditional Anti-Virus
- User Authentication
- Client Authentication

Unsupported Deployments for Monitor Mode

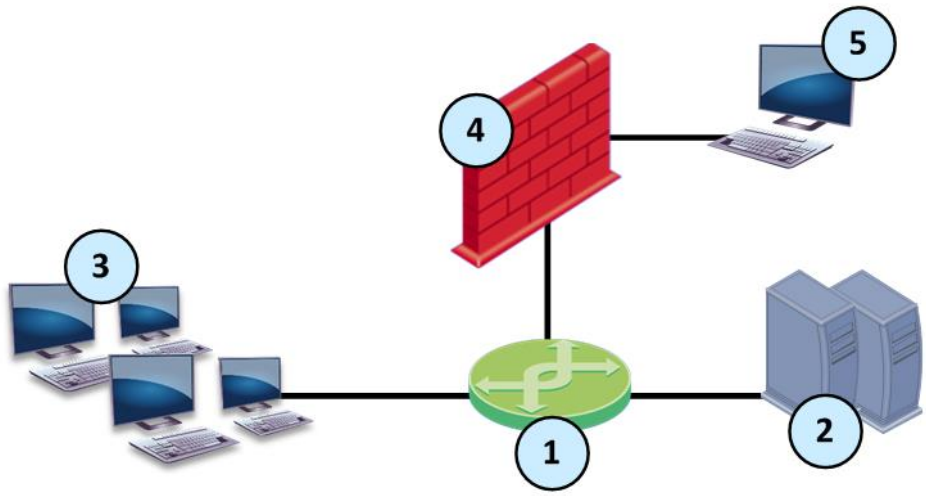
These are deployments do not support Monitor Mode:

- Access to Portals
- Multiple TAP interfaces when the same traffic is monitored

Configuring Monitor Mode

You can configure a mirror or TAP port to duplicate network traffic that is sent to a Security Gateway. The gateway inspects the traffic but does not drop packets.

Connect the Security Gateway to a mirror port on the switch that duplicates the ports and VLANs.



Item	Description
1	Switch with mirror port
2	Servers
3	Computers
4	Security Gateway in monitor mode
5	Management for Security Gateway

Note - Make sure that one mirror port on the switch is connected to one interface on the Security Gateway.

To enable monitor mode on the Security Gateway from the WebUI:

1. From the navigation tree, click **Network Interfaces**.
2. Select the interface and click **Edit**.
3. Click the **Ethernet** tab.
4. Click **Monitor Mode**.
5. Click **OK**.

To enable monitor mode on the Security Gateway from the clish:

```
set interface <interface name> monitor-mode on
```

Upgrading Prerequisites

In This Section:

Before Upgrading

Before you upgrade:

- For information about supported upgrade paths, see the *R80.10 Release Notes*.
- Make sure that you have the latest version of this document.

If you use Mobile Access Software Blade and you edited the configurations, review the edits before you upgrade to R80.10!

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 R80.10.
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 R80.10 files with your customized files!

Contract Verification

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/ngx/upgrade/contract/index.html.

Upgrade Tools

Before you upgrade appliances or servers, get the upgrade tools. There is a different package of tools for each source platform.

Important! To make sure you have the latest version of the upgrade tools, download the appropriate package from the **Tools** section in the Check Point R80.10 Support site http://supportcontent.checkpoint.com/solutions?id=sk111841.

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

Package	Description
migrate.conf	Holds configuration settings for Advanced Upgrade / Database Migration.
migrate	Runs Advanced Upgrade or migration. On Windows, this is **migrate.exe**.
pre_upgrade_verifier	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. On Windows this is **pre_upgrade_verifier.exe** `pre_upgrade_verifier -p $FWDIR -c` *<Current Version>* `-t` *<Target Version>*
migrate export	Backs up all Check Point configurations, without operating system information. On Windows, this is **migrate.exe export**
migrate import	Restores backed up configuration.

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)

Parameter	Description
-c	Currently installed version
-t -i	Target version 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, consult the Support Center http://supportcontent.checkpoint.com/solutions?id=sk111841 or contact your Reseller.

Service Contract Files

Introduction

Before upgrading a gateway or Security Management Server to R80.10, you need to have a valid support contract that includes software upgrade and major releases registered to your Check Point User Center account. The Security Management Server stores the contract file and downloads it to Security Gateways during the upgrade. By verifying your status with the User Center, the contract file enables you to easily remain compliant with current Check Point licensing standards.

Working with Contract Files

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

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

Installing a Contract File On Security Management Server

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.

Installing a Contract File 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.

Upgrading Security Management Servers and Security Gateways

In This Section:

Using the Upgrade Verification Service

The Upgrade Verification Service helps you upgrade successfully to R80.10.

We evaluate your environment and send you an email that shows if you are ready to upgrade, or what you must do first. For more details, see sk110267 http://supportcontent.checkpoint.com/solutions?id=sk110267.

Upgrading with CPUSE

With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself. The software update packages and full images are for major releases, minor releases and Hotfixes. All of the CPUSE processes are handled by the Deployment Agent daemon (DA).

Gaia automatically locates and shows the available software update packages and full images that are relevant to the Gaia operating system version installed on the computer, the computer's role (gateway, Security Management Server, standalone), and other specific properties. The images and packages can be downloaded from the Check Point Support center and installed.

Upgrade Limitations

- Personal files saved outside of the `/home` directories are erased during the upgrade process. If you created a snapshot immediately before upgrading, you can revert to the snapshot to recover personal files saved outside of the `/home` directory.
- Open servers that were upgraded from SecurePlatform to Gaia cannot be upgraded.
- Upgrading using Full Images:
  - IP Appliances are not supported.
  - UTM-1 Appliances are not supported.
  - To upgrade the secondary Security Management Server of a Full High Availability deployment, use the procedure in this guide for upgrading with a clean installation.

- The ssh key is not migrated to the new version.
- The Mobile Access Software Blade custom configuration is not upgraded.
- Virtual Systems Mode is not supported.
- Endpoint Policy Servers cannot be upgraded.

Software Update Requirements

- At least 4 GB free disk space in `/var/log`
- Un-partitioned free disk space should be at least the size of root partition. To find out the:
  - Amount of un-partitioned free disk space run: `pvs`
  - Size of the root partition, run: `df -h`

To update the Gaia Software Updates agent:

1. Make sure the proxy and the DNS server are configured.
2. In the WebUI, go to **Upgrades (CPUSE) > Software Updates Policy**.
3. In the **Software Deployment Policy** section. select **Periodically update new Deployment Agent version**. This option updates the DA according to the configured time period.
4. Click **Apply**.

To upgrade to R80.10 using CPUSE:

See the procedures in sk92449 http://supportcontent.checkpoint.com/solutions?id=sk92449.

Upgrading Security Gateways

You can upgrade Security Gateways using one of these methods:

- **CPUSE:** Do a local upgrade on the Security Gateway itself using CPUSE
- **SmartUpdate**: Centrally upgrade and manage Check Point software and licenses from a SmartConsole client.

Best Practice:

Before you upgrade, back up your configuration (see "Backing Up" on page 14).

Upgrading Security Gateways using CPUSE

The WebUI uses Upgrades (CPUSE) for upgrading.

For more about CPUSE, see sk92449 http://supportcontent.checkpoint.com/solutions?id=sk92449.

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.

Upgrading a VSX Gateway

The `vsx_util` command upgrades a VSX Gateway from an earlier version to R80.10.

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 R80.10:

1. Install R80.10 on the VSX Gateway ("Installing VSX Gateways" on page 30).
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 Security Management Server and Standalone

This section explains how to upgrade Gaia standalone and Security Management Server. A Security Management Server upgraded to R80.10 can enforce and manage Gateways from earlier versions. Some new features are not available on earlier versions

See the R*80.10 Release Notes f*or the supported features (in the "Compatibility Tables" section) and deployments.

Upgrade Notes

Upgrading Standalone Appliances	You can upgrade a Standalone deployment on UTM-1 appliances, certain 2012 Models, and IP appliances.
Upgrading Open Servers	Before you upgrade: • Back up your current configuration (see "Backing Up" on page 14). • See the *R80.10 Release Notes* to make sure that you have enough disk space.
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 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 57). 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 with Database Migration" on page 94) **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 and open servers.

To upgrade using CPUSE

See the procedures in sk92449 http://supportcontent.checkpoint.com/solutions?id=sk92449.

To Upgrade Endpoint Security on the Security Management Server:

To upgrade to R77 with E80.50 from E80.40 or higher, use the upgrade or advanced upgrade and migration procedures for Security Management Servers in this guide.

Upgrading Standalone Full High Availability

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 that you export the database using the Upgrade tools (on page 57).
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 that you export the database using the Upgrade tools (on page 57).
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 on Appliances

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 Current Security Management Server Database" on page 100).
2. Upgrade the Appliance.
3. If the appliance was not the primary member of a cluster, Import the database ("Importing the Security Management Server Database" on page 101).
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**.

Changing to an IPv6-Only Management IP Address

To remove the IPv4 management address from a Security Management Server with a dual-IP management addresses (IPv4 and IPv6):

1. Open SmartDashboard using the IPv6 address.
2. Edit the Security Management Server object.
3. In the **General Properties** page, delete the IPv4 address.
4. Go to the **Topology** page, **Interface Properties** window, and delete the IPv4 address.
5. Save.
6. Open the Gaia WebUI by connecting to the IPv6 address https://<IPv6 address>.
7. Delete the management IPV4 address from these pages:
   - **Network Interfaces**
   - **IPv4 Static routes**

Deleting the IPv4 Address from Management High Availability

You can remove the IPv4 address from one member in a management High Availability environment and keep the IPv6 and IPv4 addresses on the second member.

To remove the IPv4 address from a management HA member:

1. Open the WebUI.
2. In the **Network Management > Network Interfaces** page, delete the IPV4 address.
3. Open SmartDashboard.
4. Reset SIC.
5. Install the database (**Policy > Install Database**).
6. Reboot.
7. Synchronize the databases of the Security Management Servers.

Upgrading Multi-Domain Security Management

In This Section:

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 Tool

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
   ```

   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 Tool

The **Export current Multi-Domain Server** option in `mds_setup` 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.

Run `mds_setup` from the DVD, from the `linux/p1_install/` directory

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 one 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 using `migrate export`, in a Management High Availability environment:

- In Security Management - In SmartDashboard, delete all secondary management objects from the primary Security Management Server.
- In Multi-Domain Security Management - When you migrate Domain Management Servers one at a time, in the SmartDashboard of the primary Domain Management Server, delete the secondary Management Server object.

To install the migrate utility:

1. Locate the `p1_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/p1_upgrade_tools.tgz -C
/var/opt/export_tools
```

Install from DVD:

```
# gtar xvfz
/mnt/cdrom/Linux/linux/upgrade_tools/linux/p1_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 *R80.10 Multi-Domain Security Management Administration Guide* http://supportcontent.checkpoint.com/documentation_download?ID=46532).

To export the management database:

```
<fully qualified path to command> migrate export [-l] <output file>
```

The optional `-l` flag includes closed log files and SmartLog data 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-R80.10/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{Do not change to a variable}.

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 Data

The `cma_migrate` process does not change the Certificate Authority or key data. The R80.10 Domain Management Server has SIC with Security Gateways. If the IP address of the R80.10 server is not the same as the IP address of the R77.xx server, you must establish trust between the new server and the gateways.

Before you begin, see sk17197 http://supportcontent.checkpoint.com/solutions?id=sk17197 to make sure the environment is prepared.

To initialize a Domain Management Server Internal Certificate Authority:

1. Remove the current Internal Certificate Authority for the specified environment, run:

   ```
   # mdsstop_customer <DomainServer NAME>
   # mdsenv <DomainServer NAME>
   # fwm sic_reset
   ```

2. Create a new Internal Certificate Authority, run:

   ```
   # mdsconfig -ca <DomainServer NAME> <DomainServer IP>
   # mdsstart_customer <DomainServer NAME>
   ```

Resolving Issues with IKE Certificates

With a VPN tunnel that has an externally managed, third-party gateway and a Check Point Security Gateway, sometimes there is an issue with the IKE certificates after you migrate the management database.

The Security Gateway presents its IKE certificate to its peer. The third-party gateway uses the FQDN of the certificate to retrieve the host name and IP address of the Certificate Authority. If the IKE certificate was issued by a Check Point Internal CA, the FQDN contains the host name of the original management server. The peer gateway will fail to contact the original server and will not accept the certificate.

To fix:

- Update the external DNS server to resolve the host name to the IP address of the relevant Domain Management Server.
- Revoke the IKE certificate for the gateway and create a new one.

migrate_global_policies Command

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 polices 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

Before you upgrade, back up the management server, to restore it later if necessary.

- In a Single Domain Security Management Server environment, use the `add backup` and `set backup restore` commands.
- In Multi-Domain Security Management, use the `mds_backup` and `mds_restore` commands.

It is best practice to store the backup on an external computer or storage.

mds_backup

The `mds_backup` command backs up the complete Multi-Domain Server, including all the Domain Management Servers, binaries, and user data. If the Multi-Domain Security Management environment has multiple Multi-Domain Servers, backup runs on all of them at the same time.

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 the `$MDSDIR/conf/mds_exclude.dat` file. The collected data is stored in a single .tgz file, in the current working directory, named with the *date-time*. For example: `13Sep2002-141437.mdsbk.tgz`

To back up a Multi-Domain Server:

1. Go to a path outside the product directory. This is the working directory.

   It is important that you not run `mds_backup` from a directory that will be backed up, to avoid a circular reference. For example, do not run `mds_backup` from `/opt/CPmds-R80.10`.
2. Run: `mds_backup`
3. When the process is done, copy the `.tgz` file, with the `mds_restore`, `gtar` and `gzip` command files, to an external backup location.

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

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

Comments When using the `-g` or `-b` options, make sure that no GUI clients or log servers are connected. If there are client connections, the backup can be corrupted if changes are made during the backup process.

Active log files are not backed up, to avoid read-during-write inconsistencies. It is best practice to run a log switch before backup.

You can back up the Multi-Domain Server without log files. The .tgz will be must smaller. To make sure all logs are excluded:

1. Open: `$MDSDIR/conf/mds_exclude.dat`
2. Add: `log/*`
3. Save the file.

mds_restore

Use this command to restore a Multi-Domain Server that was backed up with `mds_backup`. It is best practice to restore to a clean install of the previous version. Use the *Installation and Upgrade Guide* for major versions, or the *Release Notes* for minor versions or hotfixes.

If the Multi-Domain Security Management environment has multiple Multi-Domain Servers, restore all Multi-Domain Servers at the same time.

To restore a Multi-Domain Server:

1. Go to the directory where the backup was created.
2. Log in to expert mode.
3. Run: `./mds_restore <backup_file>`
4. If you restore a Multi-Domain Server to a new IP address, configure the new address ("Migrating a License to a New IP Address (Security Management Server)" on page 102).

Upgrading Multi-Domain Security Management with Migration

We recommend that you use database export/import to upgrade. This procedure migrates all system databases, Domain Management Servers, Rule Bases, logs and Global Domains to a target Multi-Domain Server.

Important - In R80, the order that you import servers is important. First you must import the Primary Multi-Domain Server, then Secondary Multi-Domain Servers and Multi-Domain Log Servers. If there is no Primary Multi-Domain Server, you must first promote a secondary Multi-Domain Server to be the primary.

Exporting the Multi-Domain Server Databases

Before you begin:

- Export one database at a time. Start with the Primary Multi-Domain Server.
- Make sure the Global Domain Management Server is active on the Primary Multi-Domain Server.

To create the export file on a source Multi-Domain Server:

1. Stop all Check Point services: `# mdsstop`
2. Switch to the Multi-Domain Server context:
   `# mdsenv`

```
# mcd
```

3. Mount the ISO file:

   ```
   # mount -o loop /path_to/Check_Point_R80.10_Gaia.iso /mnt/cdrom
   ```

4. Go to the installation folder:

   ```
   # cd /mnt/cdrom/linux/p1_install
   ```

5. Run the installation script:

   ```
   # ./mds_setup
   ```

6. Run the **Pre-Upgrade Verifier**: enter 1 when this menu shows:

   ```
   (1) Run Pre-upgrade verification only [recommended before upgrade]
   (2) Upgrade to R80.10
   (3) Backup current Multi-Domain Server
   (4) Export current Multi-Domain Server
   Or 'Q' to quit.
   ```

   The pre-upgrade verifier analyzes compatibility of the management database and its current configuration. A detailed report shows the steps to do before and after the upgrade.

   Note: The pre-upgrade verifier can only verify a database that is intended for import into a different major version (for example, R77.xx to R80.10). It cannot be used on a database that is intended for import to the same major version.

7. Read the Pre-Upgrade Verifier output and fix all errors according to the instructions.
8. After fixing errors, open SmartConsole and reassign the Global Policy on all Domains.
9. Stop the services again: `# mdsstop`
10. Run the installation script `# ./mds_setup`
11. Export the current Multi-Domain Server configuration: enter **4** when this menu shows:

    ```
    (1) Run Pre-upgrade verification only [recommended before upgrade]
    (2) Upgrade to R80.10
    (3) Backup current Multi-Domain Server
    (4) Export current Multi-Domain Server
    Or 'Q' to quit.
    ```

12. Answer the interactive questions:

    ```
    Would you like to proceed with the export now [yes/no] ? yes
    Please enter target directory for your Multi-Domain Server export (or 'Q'
    to quit): /var/log
    Do you plan to import to a version newer than R80.10 [yes/no] ? no
    Using migrate_tools from disk.
    Do you wish to export the log database [yes/no] ? yes or no
    ```

    If you enter **no** to export the logs, the configuration is still exported.

13. Make sure this export file is created:

    ```
    # ls -l /var/log/exported_mds.DDMMYYY-HHMMSS.tgz
    ```

14. Calculate the MD5 for this file:

    ```
    # md5sum /var/log/exported_mds.DDMMYYY-HHMMSS.tgz
    ```

Importing the Database to the Primary Multi-Domain Server

Import the Multi-Domain Server configuration that you exported.

Important - When you transfer the exported database from the source to the target, use **binary mode** during the transfer.

Before you begin, install R80.10 Multi-Domain Security Management and the latest R80.10 Jumbo Hotfix on the target Multi-Domain Server ("Installing Multi-Domain Security Management" on page 38).

Note - When you complete the upgrade process for the Primary Multi-Domain Server, the Multi-Site upgrade is not finished. You can only access objects that are stored on other Multi-Domain Security Management servers when the upgrade process for the other Multi-Domain Servers is complete.

To import the Multi-Domain Server configuration:

1. Log in to **expert** mode.
2. Transfer (with FTP, SCP, or similar) the exported configuration file collected from the source to the new server: `exported_mds.`*DDMMYYY-HHMMSS*`.tgz`
3. Calculate the MD5 for the transferred file and compare to the MD5 that was calculated on original server:

   `# md5sum /<directory>/exported_mds.`*DDMMYYY-HHMMSS*`.tgz`
4. Import the configuration: `$MDSDIR/scripts/mds_import.sh` *<path_exported_database>*`/exported_mds.`*DDMMYYY-HHMMSS*`.tgz`
5. Test the target installation.
6. Disconnect the source server from the network.
7. Connect the target server to the network and run `mdsstart`

To update the version of the Domain Management Server and Domain Log Server objects on this Multi-Domain Server:

On each Domain Management Server and Domain Log Server that you import, run:
`$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n <`*Multi-Domain Server name*`>`

Importing the Database to Secondary Multi-Domain Servers

Import the Multi-Domain Server configuration that you exported to a Secondary Multi-Domain Server or Multi-Domain Log Server. If you have multiple servers, import the database to one server at a time.

Important: When you transfer the exported database from the source to the target, use **binary mode** during the transfer.

Before you begin:

- In the primary Multi-Domain Server, log into expert mode and run this command to back it up:
  `# mds_backup -b -d /var/log`
- Install R80.10 Multi-Domain Security Management on the target Multi-Domain Server ("Installing Multi-Domain Security Management" on page 38).
- Make sure the Primary Multi-Domain Server is running.
- Make sure that the Primary Multi-Domain Server has the correct license to work in Multi-Site environment.
- Make sure that there is good connectivity between all the servers. System databases, logs, and Global domains are upgraded only on the Primary Multi-Domain Server. The connection is necessary to synchronize the other Multi-Domain Servers and Multi-Domain Log Servers.

- The IP address of the source and target Secondary Multi-Domain Servers and Multi-Domain Log Servers must be the same.

To import the Multi-Domain Server configuration:

1. Log in to **expert** mode.
2. Transfer (with FTP, SCP, or similar) the exported configuration file collected from the source to the new server: `exported_mds.`*DDMMYYY-HHMMSS*`.tgz`
3. Calculate the MD5 for the transferred file and compare to the MD5 that was calculated on source Multi-Domain Server:
   `# md5sum /<directory>/exported_mds.`*DDMMYYY-HHMMSS*`.tgz`
4. Make sure that there is connectivity to the newly upgraded primary Multi-Domain Server.
5. Import the configuration: `$MDSDIR/scripts/mds_import.sh -secondary -primaryip` *<IP_primary_server>* *<path_exported_database>*`/exported_mds.DDMMYYYY-HHMMSS.tgz`
6. On the Primary Multi-Domain Server, make sure that the Full Sync task completes successfully.
7. Test the target installation.
8. Disconnect the source server from the network.
9. Connect the target server to the network and run `mdsstart`.

To update the version of the Domain Management Server and Domain Log Server objects on this Multi-Domain Server:

1. On each Domain Management Server and Domain Log Server that you import, run: `$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n <`*Multi-Domain Server name*`>`
2. Open SmartConsole and make sure that the version for each of the upgraded objects is R80.10.

Migrating Global Policies

The `migrate_global_policies` command upgrades a Global Policy database from a Multi-Domain Server and imports it to a R80.10 Multi-Domain Server.

Note - When executing the `migrate_global_policies` utility, the Multi-Domain Server and the Domain Management Servers are stopped.

Before you run the `migrate_global_policies` utility, make sure that you remove all the data from the Global database of the R80.10 Multi-Domain Server.

To upgrade Global Policies from R77.xx to R80.10:

1. On the R77.xx Multi-Domain Server, extract the Upgrade Tools from the R80.10 CD or ISO ("Upgrade Tools" on page 57), if you did not do this already ("Migrating Domain Management Server Database" on page 78).
2. Run: `# mdsenv`
3. Run: `# <`*full path to migrate command*`> migrate export <`*output file*`>`
4. Copy the TGZ file from the R77.xx server to the R80.10 Multi-Domain Server.
5. Run: `# migrate_global_policies` *<full_path_exported_tgz>*
6. Run: `# mdsstart`

Migrating Domain Management Server Database

This procedure exports, updates, and imports the database of an R77.xx Domain Management Server to an R80.10 Domain Management Server.

Before you begin:

- Make sure that there is one Active Domain Management Server in each Domain to be migrated.
- If you want to import logs with the database, run a log switch before you export.
- Make sure that you are migrating the database only on one Domain Management Server. If you migrate a database to more than one Domain Management Server, the import fails and shows an error message.

To import from R77.xx Domain Management Server to R80.10:

1. On the R77.xx Domain Management Server, get the Upgrade Tools from the R80.10 CD or ISO ("Upgrade Tools" on page 57).
2. Extract the tools.

   Extraction makes the `upgrade_tools` subdirectory. In this path, extract the Multi-Domain Security Management tools: `p1_upgrade_tools.tgz`

   For example:

   Install from CD:
   ```
   # gtar xvfz /mnt/cdrom/linux/upgrade_tools/linux/p1_upgrade_tools.tgz -C /var/opt/export_tools
   ```

   Install from DVD:
   ```
   # gtar xvfz /mnt/cdrom/Linux/linux/upgrade_tools/linux/p1_upgrade_tools.tgz -C /var/opt/export_tools
   ```
3. Run: `# mdsenv` *<domainServer_name>*
4. Before you export the database, make sure that you remove the Global Policy from the source Domain Management Server.
5. Run: `#` *<full path to migrate command>* `migrate export [-l]` *<output file>*
   - The `migrate export` command exports one Domain Management Server database to a TGZ file.
   - The output file must be specified with the fully qualified path. Make sure there is sufficient disk space for the output file.
   - The optional `-l` flag includes closed log files and SmartLog data from the source Domain Management Server in the output archive.
6. On the R80.10 Multi-Domain Server, run these API commands https://sc1.checkpoint.com/documents/R80/APIs/#introduction to create a new Domain and a new Domain Management Server (without starting it):

   `# mgmt_cli login` *<user_name>* *<password>*

   `# mgmt_cli add domain name` *<my_domain_name>* `servers.ip-address` *<my_IP_address>* `servers.name` *<my_domain_server_name>* `servers.multi-domain-server` *<R80.10_multi-domain-server_Name>* `servers.skip-start-domain-server true`

7. Copy the TGZ file from the R77.xx Domain Management Server to the R80.10 Multi-Domain Server.
8. Import the exported database:

   `# cma_migrate` *<source management tgz file> <target Domain Management Server fwdir directory>*

   For example:

   ```
   # cma_migrate tmp/orig_mgmt.tgz
   /opt/CPmds-R80.10/customer/cma1/CPsuite-R80.10/fw1
   ```

   You must run `cma_migrate` to import the database. This command updates the database schema before it imports.

   First, the command runs pre-upgrade verification. If no errors are found, migration continues. If there are errors, you must change the source Domain Management Server according to instructions in the error messages. Then do this procedure again.
9. If the R80.10 server has a different IP address than the R77.xx server, establish trust with the Security Gateways ("Certificate Authority Data" on page 71).
10. If the R77.xx server had VPN gateways, configure the keys ("Resolving Issues with IKE Certificates" on page 72).
11. Restart the R80.10 Domain Management Server: `# mdsstop` and then `mdsstart`

Certificate Authority Data

The `cma_migrate` process does not change the Certificate Authority or key data. The R80.10 Domain Management Server has SIC with Security Gateways. If the IP address of the R80.10 server is not the same as the IP address of the R77.xx server, you must establish trust between the new server and the gateways.

Before you begin, see sk17197 http://supportcontent.checkpoint.com/solutions?id=sk17197 to make sure the environment is prepared.

To initialize a Domain Management Server Internal Certificate Authority:

1. Remove the current Internal Certificate Authority for the specified environment, run:

   ```
   # mdsstop_customer <DomainServer NAME>
   # mdsenv <DomainServer NAME>
   # fwm sic_reset
   ```
2. Create a new Internal Certificate Authority, run:

   ```
   # mdsconfig -ca <DomainServer NAME> <DomainServer IP>
   # mdsstart_customer <DomainServer NAME>
   ```

Resolving Issues with IKE Certificates

With a VPN tunnel that has an externally managed, third-party gateway and a Check Point Security Gateway, sometimes there is an issue with the IKE certificates after you migrate the management database.

The Security Gateway presents its IKE certificate to its peer. The third-party gateway uses the FQDN of the certificate to retrieve the host name and IP address of the Certificate Authority. If the IKE certificate was issued by a Check Point Internal CA, the FQDN contains the host name of the original management server. The peer gateway will fail to contact the original server and will not accept the certificate.

To fix:

- Update the external DNS server to resolve the host name to the IP address of the relevant Domain Management Server.
- Revoke the IKE certificate for the gateway and create a new one.

Migrating an R80.10 Database to another R80.10 Server

You can migrate the R80.10 Security Management Server database to a different R80.10 server. The procedure is similar to upgrading from an earlier version to R80.10.

1. Create a backup file of the current system settings from the Gaia WebUI.

   For Multi-Domain Server run `mds_backup`
2. Do the steps to migrate to another R80.10 Security Management Server or Multi-Domain Server.

Upgrading Multi-Domain Security Management on Smart-1 and Open Servers

You can upgrade Smart-1 appliances and open servers.

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 R80.10:

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 in SmartConsole
   d) View status using the SmartConsole or SmartView Monitor
4. Run `mds_backup` to back up your system.

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 Upgrades (CPUSE)

See *Upgrading Using Gaia Upgrades (CPUSE)* ("Upgrading with CPUSE" on page 60).

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=sk111841.
   `Check_Point_Install_and_Upgrade_R80.10.Gaia.iso`
2. Burn the ISO file on a DVD.
3. Connect an external DVD drive to a USB socket on the appliance or open server.
4. From clish, 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.

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

To upgrade using the upgrade package, with CLI:

1. Download the Gaia upgrade package from the Check Point Support Center http://supportcontent.checkpoint.com/solutions?id=sk111841.
   `Check_Point_upg_WebUI_and_SmartUpdate_R80.10.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 R80.10`
7. 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. You are asked if you want to start the upgrade. Select `Yes`.
10. After the upgrade, type `OK` to reboot.

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 `mds_setup` 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.

Run `mds_setup` from the DVD, from the `linux/p1_install/` directory

Use the `mds_import.sh` 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.

Run `mds_setup` from the DVD, from the `linux/p1_install/` directory

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 `linux/p1_install/` directory.
4. Run: `mds_setup`
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.sh` 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 SmartConsole and Global Domain.
   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 SmartConsole and Global Domain.
   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: `mdsenv; fwm mds rebuild_global_communities_status all`

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 (see "Migrating Domain Management Server Database" on page 78) 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. 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 SmartConsole, specifying as an argument the database location you specified in step 2.

   Note - To run the `cma_migrate` utility from SmartConsole, 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

Multi-Domain Security Management High Availability gives you management redundancy for all Domains. Multi-Domain Security Management High Availability operates at these levels:

- **Multi-Domain Server High Availability** - By default, Multi-Domain Servers are automatically synchronized with each other. One Multi-Domain Server is always defined as the **Active** Multi-Domain Server and all other Multi-Domain Servers are **Standby** Multi-Domain Servers. You can connect to an Active or Standby Multi-Domain Server to work on Domain management tasks.

  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.
5. Install the database in SmartDashboard for the applicable Domain Management Server.

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, log in to expert mode and run the `mds_remove` utility.
2. Go to the folder that contains the backup file.
3. Run: `./mds_restore`
   The original environment is restored.
4. Exit expert mode.

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 R80.10, 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 it to change the restored Multi-Domain Server to the new IP address.

To change the IP address:

1. Stop the Multi-Domain Server by running `mdsstop`.
2. Change the IP address in `$MDSDIR/conf/LeadingIP` file to the new IP address.
3. Edit the `$MDSDIR/conf/mdsdb/mdss.C` file. Find the Multi-Domain Server object that has the source Multi-Domain Server IP address and change its IP address to the new IP address. Do not change the Multi-Domain Server name.
4. Install a new license on the target Multi-Domain Server with the new Multi-Domain Server IP address.
5. For multiple Multi-Domain Server environments, repeat steps 1 to 4 for each Multi-Domain Server that has a changed IP address.

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`.

Saving the Multi-Domain Security Management IPS Configuration

When upgrading to R80.10, the previous Domain IPS configuration is overridden when you first assign a Global Policy.

Best Practice - 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.

For more on IPS, see the *R80.10 Multi-Domain Security Management Administration Guide* http://supportcontent.checkpoint.com/documentation_download?ID=46532

Enabling IPv6 on Gaia

IPv6 is automatically enabled if you configure IPv6 addresses in the First Time Configuration Wizard.

If you did not do this, enable IPv6 in one of the following ways:

To enable IPv6 using clish:

```
# set ipv6-state on
# save config
# reboot
```

To enable IPv6 using the WebUI:

1. In the WebUI navigation tree, select **System Management > system Configuration**.
2. For **IPv6 Support**, select **On**.
3. When prompted, select **Yes** to reboot.

Enabling IPv6 on Multi-Domain Security Management

If your environment uses IPv6 addresses, you first must enable IPv6 support for the Multi-Domain Servers and for existing Domain Management Servers. It is not necessary to enable IPv6 support for Domain Management Servers that you create after IPv6 is enabled on the Multi-Domain Server, because this is handled automatically.

Important - You must assign an IPv4 address for each Multi-Domain Server, Multi-Domain Log Servers, Domain Management Server and Domain Log Server. The IPv6 address is optional.

Preliminary steps:

1. Enable IPv6 for the leading interface (typically eth0) with Gaia Web UI.
2. Assign an IPv6 address and default gateway to the management interfaces.
3. Write down the Multi-Domain Server IPv6 address and the host names and IPv6 addresses for all Domain Management Servers. This is necessary because the system restarts after you enable IPv6 support.

To enable IPv6 support for the Multi-Domain Server:

1. Log into the Primary Multi-Domain Server with a terminal emulation application.
2. From the command line, run: `mdsconfig`
3. Select **IPv6 Support for the Multi-Domain Server**.
4. Press **y** when prompted to change the IPv6 preferences.

   Press **y** again to confirm.
5. When prompted for the Leading Interface name, enter the **management interface name** (typically eth0).
6. When prompted, enter the management interface IPv6 address.
7. Press **y** to restart Check Point services.

To enable IPv6 support for existing Domain Management Servers:

1. From the `mdsconfig` menu, select **IPv6 Support for Existing Domain Management Servers**.

2. Press **y** when asked to change the IPv6 preferences for Domain Management Servers.
3. Press **a** to add support to an existing Domain Management Server.
4. Press **y** to add Support to all Domain Management Servers at once.
   Press **y** again to confirm.
5. Press **m** to manually add IPv6 addresses
   Or
   Press **r** to automatically assign IPv6 address from a specified range.
6. Follow the instructions on the screen to enter the IPv6 addresses or a range of IPv6 addresses.

To manually enable IPv6 support for specified Domain Management Servers.

1. From the `mdsconfig` menu, select **IPv6 Support for Existing Domain Management Servers**.
2. At the prompt, press **y** to change the IPv6 preferences for Domain Management Servers.
3. Press **a** to add support to an existing Domain Management Server.
4. Press **n** when asked to enable IPv6 support for all Domain Management Servers at once.
   Press **y** to confirm.
5. At the prompt, enter the Domain Management Server name.
   The available Domain Management Servers show above prompt. You can copy and paste the name.
6. Enter the IPv6 address.
7. At the prompt, press **y** to enable another Domain Management Server or **n** to complete the procedure.

Advanced Upgrade with Database Migration

In This Section:

Supported Upgrade Paths, Platforms and Products

Make sure that the upgrade version and products is a supported on the target operating system and hardware platform. For a list of supported upgrade paths, platforms and products, see the R80.10 Release Notes.

Solaris: You can migrate a Solaris database to Gaia.

Requirements for Advanced Upgrade and Migration

Required Disk Space:

- The hard disk on the target machine must be at least 5 times the size of the exported database.
- The size of the `/var/log` folder on the target must be at least 25% of the size of the `/var/log` directory on the source machine.

Required Network Access:

- The source and target servers must be connected to a network.
- The connected network interface must have an IP address.

IPv4 or IPv6:

If the source environment uses only IPv4 or only IPv6, the target must use the same IP address configuration. You cannot migrate to an environment that uses only the other type of addresses.

Target Version and Products:

You can only upgrade or migrate the version of the server or set of products. The target must have the same or higher version and the same set of installed products.

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> [--exclude-uepm-postgres-db]
[--include-uepm-msi-files]
```

Parameters	Description
`export` `import`	One of these actions must be used. Make sure services are stopped.
`-l`	Optional. Export or import SmartLog data. Only closed logs are exported. Use the `fw logswitch` command to close the logs before you do the export.
`-n`	Optional. Run silently (non-interactive) using the default options for each setting. **Important**: If you export a management database in this mode, to a directory with a file with the same name, it is overwritten without prompting. If you import using this option, the command runs `cpstop` automatically.
`--exclude-uepm-postgres-db`	Skip over backup/restore of PostgreSQL database of the Endpoint product.
`--include-uepm-msi-files`	Export/import the uepm msi files.
`filename`	Required. Enter the name of the archive file with the server database. The path to the archive must exist.

Important - If the source environment uses only IPv4 or only IPv6, you cannot migrate to an environment that uses only the other type of addresses.

Using the Pre-Upgrade Verification Tool

We recommend that you run the pre-upgrade verifier (see "Using the Pre-Upgrade Verifier Tool" on page 57) on the source server before exporting the management database. The pre-upgrade verifier analyzes compatibility of the management database and its current configuration. A detailed report shows the steps to do before and after the upgrade.

The pre-upgrade verifier can only verify a database that is intended for import into a different major version (for example, R77.xx to R80.10). It cannot be used on a database that is intended for import into the same major version.

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.

Preparing to Migrate the Database

Database Migration lets you move the database from an earlier Security Management Server or Multi-Domain Server, to an R80.10 server.

Important Notes:

- R80 was a management-only release and did not support migration from a Standalone deployment (server and gateway on the same machine). Standalone to Standalone migration is supported for R80.10 and higher.
- Upgrade from IPSO is not supported.
- This procedure has steps to close GUI clients (SmartConsole applications) and to stop Check Point services (`cpstop`). If you do not do one of these before you upgrade, the exported management database can be corrupted.

Before you begin:

1. Make sure the environment meets the requirements ("Requirements for Advanced Upgrade and Migration" on page 94)
2. Make sure that you have SmartDashboard and SmartConsole for the correct source and target versions to connect to the management server.
3. Save a backup from the Gaia WebUI.

   Gaia operating system settings are not backed up. If you restore the database later, you must configure these settings manually. Before you upgrade, open the Gaia WebUI and take note of these settings: interfaces, servers (such as DHCP, DNS, and proxy), routes, NetFlow, system settings (such as time and date, SNMP, jobs), advanced routing protocols and functionality, user management, and High Availability.

Understanding IPv6 and IPv6 Address Issues During Migration

If you migrate from a Security Management Server or Domain Management Server to a target with a different IP address configuration, you must configure the source before you export the database:

- Configure IP address assignments
- Enable IPv6 from the *WebUI* or *mdsconfig*

After you import the database, add or remove IPv4 and IPv6 addresses as required.

When migrating from a Security Management Server with only IPv4 addresses to:

Target	You need to:
Security Management Server with only IPv4 addresses	Follow the normal migration process.
Security Management Server with only IPv6 addresses	• Enable IPv6 on the Source Operating System before exporting the database • After importing the database, change the IP address of the management
Security Management Server with a mixture of IPv4 and IPv6 addresses.	• Enable IPv6 on the Source Operating System before exporting the database • After importing the database, add the IPv6 addresses
Domain Management Server with IPv4 addresses	Follow the normal migration process.
Domain Management Server with a mixture of IPv4 and IPv6 addresses	• Enable IPv6 on the Source Operating System before exporting the database • After importing the database, add the IPv6 addresses

When migrating from a Security Management Server with only IPv6 addresses to:

Target	You need to:
Security Management Server with only IPv4 addresses	After importing the database, change the IPv6 address of the management to IPv4
Security Management Server with only IPv6 addresses	Follow the normal migration procedure
Security Management Server with a mixture of IPv4 and IPv6 addresses.	After importing the database, add the IPv4 addresses
Domain Management Server with IPv4 addresses	After importing the database, remove IPv6 addresses from the management object in SmartDashboard and add IPv4

Target	You need to:
Domain Management Server with a mixture of IPv4 and IPv6 addresses	After importing the database: • Enable IPv6 on the Operating System • Change the IP address of the management to IPv4

When migrating from a Security Management Server with a mixture of IPv4 and IPv6 addresses to:

Target	You need to:
Security Management Server with only IPv4 addresses	After importing the database: • Disable IPv6 on the Operating System • Change the IP address of the management to IPv4
Security Management Server with only IPv6 addresses	After importing the database, remove the IPv4 address from the management
Security Management Server with a mixture of IPv4 and IPv6 addresses.	Follow the normal migration procedure
Domain Management Server with IPv4 addresses	After importing the database, remove the IPv6 address from the management object in SmartDashboard
Domain Management Server with a mixture of IPv4 and IPv6 addresses	Follow the normal migration procedure

When migrating from a Domain Management Server with only IPv4 addresses to:

Target	You need to:
Security Management Server with only IPv4 addresses	Follow the normal migration procedure
Security Management Server with only IPv6 addresses	After importing the database: • Enable IPv6 on the Operating System • Change the IP address of the management to IPv6
Security Management Server with a mixture of IPv4 and IPv6 addresses.	• Enable IPv6 on the Operating System • Add IPv6 addresses
Domain Management Server with IPv4 addresses	Follow the normal migration procedure
Domain Management Server with a mixture of IPv4 and IPv6 addresses	After importing the database: • Enable IPv6 on the Operating System • Add IPv6 Addresses

When migrating from a Domain Management Server with a mixture of IPv4 and IPv6 addresses to:

Target	You need to:
Security Management Server with only IPv4 addresses	• Disable IPv6 on the source Operating System before exporting the database • After importing the database, change the IP address of the management to IPv4
Security Management Server with only IPv6 addresses	After importing the database, remove the IPv4 address from the management.
Security Management Server with a mixture of IPv4 and IPv6 addresses.	Follow the normal migration procedure
Domain Management Server with IPv4 addresses	• Disable IPv6 on the source Operating System before exporting the database • Remove the IPv6 address from the target Domain Management Server object in SmartDashboard
Domain Management Server with a mixture of IPv4 and IPv6 addresses	Follow the normal migration procedure

Migrating the Database

Before you upgrade the Security Management Server, make sure that the correct ports are open for SmartConsole to communicate with the Security Management Server.

Preparing the Source Server

Licenses are related to the management IP address. If you migrate the database to a server with a new IP address, there will be licensing issues. We recommend that you keep the same IP address for the target. If this is not possible, you must prepare the source database before the export and edit the target database after the import ("Migrating a License to a New IP Address (Security Management Server)" on page 102).

On the source before migration:

1. Create a new host object in SmartDashboard with the IP address of the target.
2. Define a Firewall rule that lets the new R80.10 server connect to Security Gateways:

   Source: *new server*

   Destination: **any**

   Service:

   FW1 (TCP 256)

   CPD (TCP 18191)

   FW1_CPRID (TCP 18208)

   CPM (TCP 19009)
3. Install the new security policy on all gateways.

4. If the source has IPv6 addresses, on the source operating system, disable IPv6.
5. In SmartDashboard, delete all secondary management objects from the primary Security Management Server.
6. Close all Check Point GUI clients that are connected to the Security Management Server.
7. If this server is not in production, run: `cpstop`

Exporting the Current Security Management Server Database

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

1. Log in to **expert** mode.
2. Run the Pre-Upgrade Verifier tool (see "Using the Pre-Upgrade Verification Tool" on page 95): `pre_upgrade_verifier`

   If there are errors, correct them before you continue.
3. Run: *<upgrade_tools_path>*`/migrate export` *<filename>*`.tgz`

   The `migrate export` command exports the content of one Security Management Server database to a TGZ file.
4. Follow the instructions.

   The management database is exported to the file that you named in the command. Make sure you define it as a TGZ.
5. If SmartEvent is installed on the source server, export the Events database.

Exporting from Gaia - CLI

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

1. Log in to the **expert** mode.
2. Get the R80.10 migration tools.
3. Run:
   <path to migration tools directory>`/migrate export` *<exported database name>*`.tgz`.
4. Do the instructions shown on the screen. This creates the *<exported database name>*`.tgz` file.

Exporting from Gaia - GUI on DVD

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

1. Insert the R80.10 DVD into source computer drive.
2. At the command prompt, run: `patch add cd`
3. Select the **Gaia R80.10 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.

Importing the Security Management Server Database

Import the Security Management Server configuration that you exported. Make sure that you use the migration tools for the target version.

Before you begin: Install the R80.10 Security Management Server ("Installing a Security Management Server" on page 32).

Important: When you transfer the exported database from the source to the target, use **binary mode** during the transfer.

To import the management server configuration:

1. Log in to **Expert** mode.
2. Transfer (with FTP, SCP, or similar) the exported configuration file collected from the source () to the new server.
3. Calculate the MD5 for the transferred file and compare to the MD5 that was calculated on original server:

   `# md5sum /<directory>/<name>.DDMMYYY-HHMMSS.tgz`
4. Import the configuration: `<migration_tools_path>/migrate import <path_exported_database>/<filename>.tgz`
5. Test the target installation.
6. Disconnect the source server from the network.
7. Connect the target server to the network.

Migrating the Database of a Secondary Security Management Server

1. Export the 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 R80.10 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.

Migrating a License to a New IP Address (Security Management Server)

Licenses are related to the management IP addresses. You must update the license and configure the environment to recognize the new server.

1. Update the licenses with the new IP address. If you use central licenses, they must also be updated with the new IP Address.
2. Run `cpstop` and `cpstart` on Security Management Server.
3. Connect to the new IP address with SmartConsole.
4. Remove the host object and the rule that you created before migration.
5. Update the primary Security Management Server object to make the IP Address and topology match the new configuration.
6. Run `evstop` and `evstart` on SmartEvent servers.
7. On the DNS, map the target Security Management Server host name to the new IP address.

Configuring the new IP address for Log Servers and SmartEvent:

1. When you log in to SmartConsole for the first time, open the Domain Log Server or SmartEvent object.
2. Change the IP address to the new IP address.
3. Publish and install the database.
4. Open the distributed Domain Log Server or SmartEvent object again.
5. In the **Platform** section, click **Get**.

   This updates the server to the correct version.
6. Click **OK**.
7. Publish and install the database.

Migrating Log and Event Databases

When you migrate the Security Management Server to R80.10, the SmartEvent databases are not included.

For more about how to migrate the events database to R80.10, see sk110173 http://supportcontent.checkpoint.com/solutions?id=sk110173.

Restoring on Failure

If there are issues with the upgrade, you can restore the original database. Make sure you have the OS settings that you noted when you backed up ("Advanced Upgrade with Database Migration" on page 94).

1. Clean install the original version.

   Use the *Installation and Upgrade Guide* for major versions, or the *Release Notes* for minor versions or hotfixes.
2. Configure Gaia OS settings in the Gaia WebUI or CLI.

3. Import the exported database.
   - Importing the Security Management Server Database (on page 101)
   - Importing the Database to the Primary Multi-Domain Server (on page 75)

Upgrading ClusterXL Deployments

In This Section:

Planning a Cluster Upgrade

Before you upgrade a ClusterXL, consider the available upgrade options.

Effort and time efficient upgrades with some loss of connectivity

- **Simple Upgrade (with downtime)** ("Upgrading Security Gateways" on page 61) - Select this option if you have a period of time during which network downtime is allowed. This method is the simplest, because each cluster member is upgraded as an independent Gateway.
- **Zero Downtime** ("Zero Downtime Upgrade on a Cluster" on page 106) - Select this option if you cannot have any network downtime and need to complete the upgrade quickly, with a minimal number of dropped connections. During this type of upgrade, there is always at least one active member that handles traffic. Connections are not synchronized between cluster members running different Check Point software versions.
  Note - Connections that were initiated on a cluster member running the old version get dropped when the cluster member is upgraded to a new version. Network connectivity, however, remains available during the upgrade, and connections initiated on an upgraded cluster member are not dropped.

Upgrades that guarantee minimal connectivity loss

- **Optimal Service Upgrade (OSU)** ("ClusterXL Optimal Service Upgrade" on page 107) - Select this option if security is of utmost concern. During this type of upgrade two cluster members process network traffic. Connections that are initiated during the upgrade stay up through the upgrade. A minimal number of connections that were initiated before the upgrade get dropped after the upgrade.
- **Connectivity Upgrade (CU)** ("Connectivity Upgrade" on page 115) - Select this option, if you need to upgrade a Security Gateway or a VSX cluster to any version, and guarantee connection failover. Connections that were initiated before the upgrade are synchronized with the upgraded Security Gateways and cluster members so that no connections are dropped.
  Note - Before you select the **Connectivity Upgrade (CU)** option, see *sk107042 ClusterXL upgrade methods and paths* http://supportcontent.checkpoint.com/solutions?id=sk107042 for limitations.

An administrator can customize the Firewall, VPN, CoreXL, and SecureXL configuration on cluster members by configuring the relevant kernel parameters in special configuration files - `$FWDIR/boot/modules/fwkern.conf`, `$FWDIR/boot/modules/vpnkern.conf`,

`$PPKDIR/boot/modules/simkern.conf`, `$FWDIR/conf/fwaffinity.conf`. For examples, see sk25977 http://supportcontent.checkpoint.com/solutions?id=sk25977. During the upgrade, all customized configuration files are overwritten with the default configuration files.

If you upgrade the cluster through CLI, you can preserve the customized configuration. To do that, you must back up the configuration files before the upgrade and restore them manually immediately after upgrade, before the cluster members are rebooted. See sk42498 http://supportcontent.checkpoint.com/solutions?id=sk42498 for details.

If you upgrade the cluster gateways through WebUI, they are rebooted automatically immediately after the upgrade, and the customized configuration is lost.

Note - If configuration customizations are lost during the upgrade, different issues can occur in the upgraded cluster. Cluster members can stop detecting each other, cluster members can move to undesired state, and traffic can be dropped.

Ready State During Cluster Upgrade/Rollback Operations

When cluster members of different versions are on the same network, cluster members of the new (upgraded) version remain in state **Ready**, and cluster members of the previous version remain in state **Active Attention**. Cluster members in the state **Ready** do not process traffic for the cluster Virtual IP address and do not synchronize with other cluster members.

To prevent cluster members from being in Ready state:

- Physically disconnect the cluster member
- Shut down all interfaces:
  - On Gaia/IPSO, run this clish command: `set interface <Interface_Name> state off`
  - On SecurePlatform, run this command in Expert mode: `ifconfig <Interface_Name> down`
  - On Windows, disable the interface through **Control Panel** > **Network and Sharing Center**

Upgrading 32/64-bit Cluster Members

High Availability cluster deployments are supported on 32-bit and 64-bit kernel operating systems. Make sure that all cluster members are running the same 32-bit or the same 64-bit operating system. If the kernel versions are different among the cluster members, those that are running the 64-bit version will stay in the state **Ready** and will not synchronize with the other cluster members or process any traffic for the cluster Virtual IP address.

Upgrading Third-Party and OPSEC Certified Cluster Products

- When upgrading clusters of IP appliances running IPSO operating system (VRRP and IP Clusters), use the Zero Downtime or the Minimal Effort procedure.
- When upgrading other third-party clustering products, use the Minimal Effort procedure. If the third party vendor has an alternative for the Zero Downtime Upgrade, refer to their documentation for upgrading.

Minimal Effort Upgrade on a ClusterXL Cluster

If you can afford to have a period of time during which network downtime is allowed, and choose to perform a Minimal Effort Upgrade, each cluster member is upgraded as an individual gateway. For additional instructions, refer to Upgrading Security Gateways (on page 61).

Zero Downtime Upgrade on a Cluster

Zero Downtime Upgrade is supported on all Check Point clusters and third-party clustering products.

During a Zero Downtime Upgrade one member of the cluster remains active, while the other cluster members get upgraded. The active cluster member is upgraded last.

The procedure below describes a three member cluster. However, it can be used for clusters with two or more members.

- In **High Availability** mode, cluster member M1 is the active member and is upgraded last. M2 and M3 are standby members.
- In **Load Sharing** mode, all members are active. Randomly choose one of the cluster members to upgrade last. Call it M1.

To upgrade a cluster with the Zero Downtime method:

1. Upgrade the licenses of *all* cluster members. A convenient time to do this is during the upgrade of the Security Management Server.

   To avoid possible problems with switches around the cluster, we recommend changing 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. Attach the upgraded licenses to all cluster members:
   a) Connect to the Security Management Server through SmartUpdate. The updated licenses are displayed as **Assigned**.
   b) Use the **Attach assigned licenses** option to attach the assigned licenses to the cluster members.
3. Upgrade M2.

   After the upgrade, reboot M2.
4. Upgrade M3.

   After the upgrade, reboot M3
5. In SmartDashboard:
   a) In the **Gateway Cluster General Properties** window, change the **Cluster version** to R80.10.
   b) In the **Install Policy** window, clear these options: **For Gateway Clusters, install on all the members**, **Install on each selected Module independently > if it fails do not install at all**.
   c) Install the security policy on the cluster.

The policy successfully installs on M2 and M3. Policy installation fails on M1 and generates a warning. You can safely ignore the warning.

6. On M1, run: `cphaprob stat`

   Verify that the status of cluster M1 is `Active` or `Active Attention`.

   `Active Attention` means that the outbound status of the synchronization interface on M1 s down. This is because M1 stopped communicating with other cluster members.

7. On M1, run: `cpstop`.

   This forces a failover to M2 or M3 (in High Availability mode) or to M2 and M3 (in Load Sharing mode).

   Make sure that one member is Active (in High Availability) or that all members are Active (in Load Sharing).

8. On M2 and M3, run: `cphaprob stat`
9. Upgrade M1.
10. Reboot M1.
11. **Optional**: To return the cluster control protocol to multicast (instead of broadcast), run `cphaconf set_ccp multicast` on all cluster members.

Upgrading Clusters With Minimal Connectivity Loss

For minimal loss of connectivity, Check Point provides these cluster upgrade methods:

- ClusterXL Optimal Service Upgrade
- Connectivity Upgrade

To select the correct facility, refer to the table below:

Upgrade Name	From version(s)	To version(s)
ClusterXL Optimal Service Upgrade	R67.10 (VSX only) R75.40VS R76 R77	R77 and later R80.10 minor versions
Connectivity Upgrade	R75.40VS R76	R77.20 and later R80.10 minor versions

ClusterXL Optimal Service Upgrade

Use the Optimal Service Upgrade feature to upgrade a Security Gateway or VSX cluster from R75.40VS to R80.10 and future major releases. This feature upgrades the cluster with a minimum loss of connectivity.

When you upgrade the cluster, two cluster members are used to process the network traffic. 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 can also use the Optimal Service Upgrade feature to upgrade a VSX cluster from R67.10 to R80.10. When you use this feature to upgrade from VSX R67.10, download the R67.10 upgrade

Hotfix and install it on one VSX cluster member. For more about upgrading to R67.10, see the *R67.10 Release Notes* http://supportcontent.checkpoint.com/documentation_download?ID=11753.

For more about the Optimal Service Upgrade and to download the R67.10 upgrade Hotfix, go to sk74300 http://supportcontent.checkpoint.com/solutions?id=sk74300.

Upgrade Workflow from R75.40VS

Use the Optimal Service Upgrade to upgrade a cluster from R75.40VS to a later version, without loss of connectivity.

- **OLD** cluster member - Cluster member before the upgrade.
- **NEW** cluster member - Cluster member that has been upgraded.

Note - Do not use this workflow to upgrade a VSX cluster from R67.10 ("Upgrade Workflow from R67.10 VSX" on page 111).

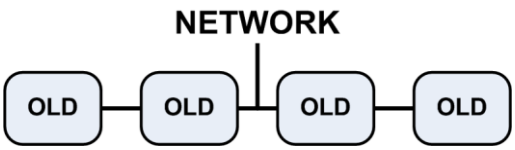
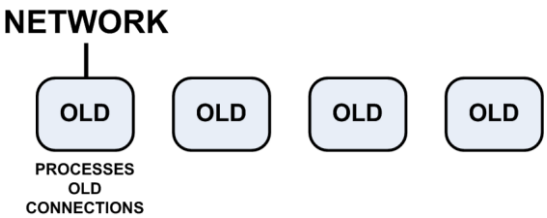
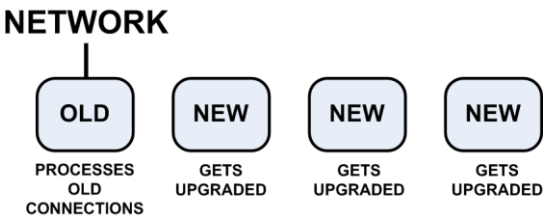
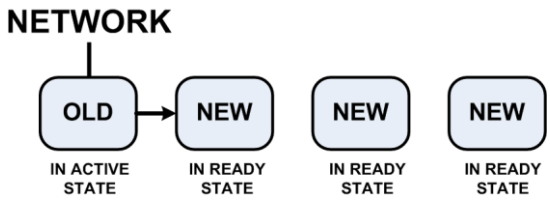
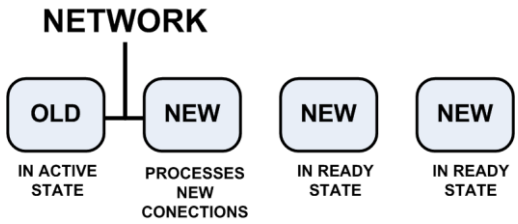
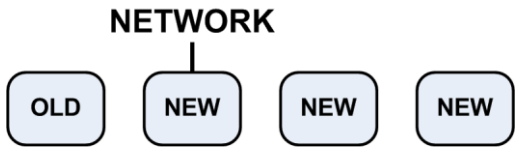
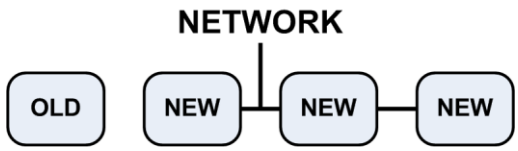
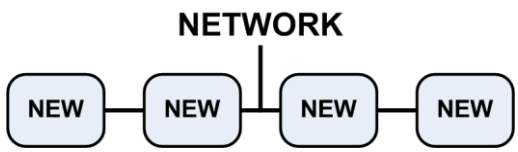
Diagram of Cluster Members	Summary	Step
	• Cluster with four members (**OLD**).	
	• Leave one cluster member connected to the network (**OLD**) and disconnect all other cluster members. The connected cluster member continues to process old connections. • For upgrades to R77.30, make sure that the cluster ID (the value of the `cluster_id` parameter) is the same on all cluster members. • For upgrades to R77.20 or an earlier version, make sure that the value of the `fwha_mac_magic` parameter is the same on all cluster members.	1 2
	• Upgrade the cluster members that are disconnected from the network (**NEW**). • For upgrades to R77.30 or a later version, make sure that the cluster ID (the value of the `cluster_id` parameter) is the same on all the upgraded cluster members. Change it, if necessary. • For upgrades to R77.20 or an earlier version, make sure that the value of the `fwha_mac_magic` parameter on all the upgraded cluster members is the same. Change it, if necessary.	3 4

Diagram of Cluster Members	Summary	Step
	• Connect one upgraded (**NEW**) cluster member to the network. • On the active (**OLD**) cluster member, turn off *fwaccel* on all Virtual Systems. This allows the active (**OLD**) cluster member synchronize all delayed connections with the upgraded (**NEW**) cluster member. **Note**: If there are a lot of connections on the Virtual Systems, turning off `fwaccel` will cause all the connections to be forwarded to the firewall. In this case, run the `cpstop` command to turn off the firewall. • On the active (**OLD**) cluster member, start the Optimal Service Upgrade procedure.	5 6 7
	• On the upgraded cluster member (**NEW**) that you connected to the network, start the Optimal Service Upgrade procedure. The upgraded cluster member begins to process new connections.	8
	• Check the number of active connection on the old cluster member. When this cluster member almost stops processing connections, stop the Optimal Service Upgrade procedure on it. • Disconnect the old cluster member from the network.	9 10
	• Reconnect the other upgraded cluster members to the network.	11
	• Upgrade the old cluster member. • Connect all the cluster members to the network. • Install the policy.	12 13 14

Upgrading the Cluster from R75.40VS

Two cluster members are used to maintain connectivity, while you upgrade all the other cluster members.

To use the Optimal Service Upgrade to upgrade the cluster members:

1. Disconnect all cluster members from the network, except for one cluster member.
   Make sure that the management interfaces are not connected to the network.
2. On the old cluster member (connected to the network), configure kernel parameters:
   - **Upgrade to R77.30**:
     Run: `cphaconf cluster_id get`
     Make sure all cluster members have the same cluster ID. If the cluster ID value is different on a cluster member, run this command to configure the correct value: `cphaconf cluster_id set` *<value>*
   - **Upgrade to R77.20 and lower**:
     Make sure all cluster members use the same value for the `fwha_mac_magic` parameter.
     Run: `fw ctl get int fwha_mac_magic`
     The default value for the `fwha_mac_magic` parameter is `254`. If your configuration uses a different value, on each member, run: `fw ctl set int fwha_mac_magic` *<value>*

   For more about the `cluster_id` and `fwha_mac_magic` parameters, see the *R77 ClusterXL Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=TBD and sk25977 http://supportcontent.checkpoint.com/solutions?id=sk25977.
3. Install R80.10 on all the cluster members that are not connected to the network.
4. Make sure that all the cluster members use the same kernel parameter values:
   - **Upgrade to R77.30 and higher**: Make sure all cluster members have the same cluster ID.
     On each member, run: `cphaconf cluster_id get`
     If a member has a different ID, run: `cphaconf cluster_id set` *<value>*
   - **Upgrade to R77.20 and lower**: Make sure all cluster members have the same value for this parameter: `fw ctl get int fwha_mac_magic`
     If a member has a different value, run: `fw ctl set int fwha_mac_magic` *<value>*
5. Prepare the old cluster member for synchronization of old connections with the upgraded cluster member:
   a) On the old cluster member, turn off fwaccel - run: `fwaccel off -a`
   b) On the old cluster member, start the Optimal Serve Upgrade - 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`
    d) In SmartDashboard, change the version of the cluster object to R80.10 and install the Policy.
11. Upgrade the old cluster member and reconnect it to the network.
12. If the cluster has two members: In SmartDashboard, change the version to R80.10.
13. Install the Policy.

Upgrade Workflow from R67.10 VSX

Use the Optimal Service Upgrade to upgrade a VSX cluster from R67.10 to a later version, without loss of connectivity. When you upgrade the cluster, use two cluster members to process the network traffic.

- **OLD** cluster member - The R67.10 VSX Gateway on which you install the Optimal Service Upgrade Hotfix http://supportcontent.checkpoint.com/solutions?id=sk74300.
- **NEW** cluster member - VSX Gateway that is upgraded to R80.10 and processes new connections.

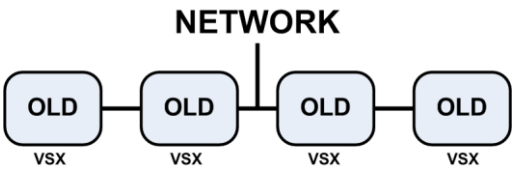
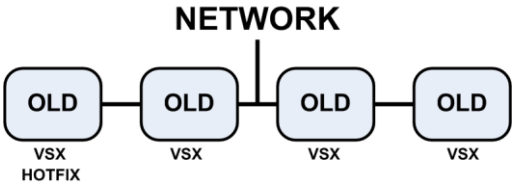
Diagram of Cluster Members	Summary	
	• VSX cluster with four R67.10 VSX Gateways (**OLD**).	
	• Install the Optimal Service Upgrade Hotfix on the cluster member that will stay connected to the network during the upgrade.	1

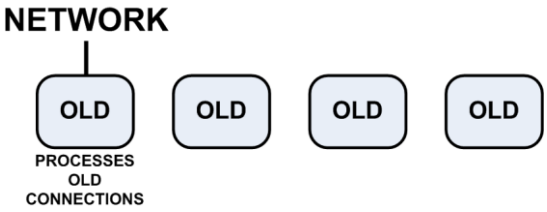
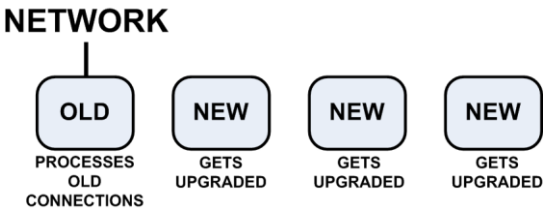
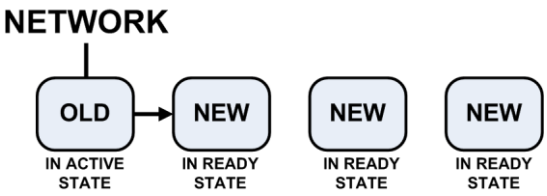
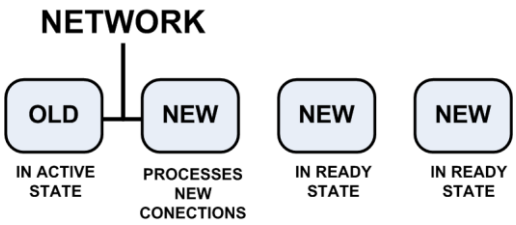
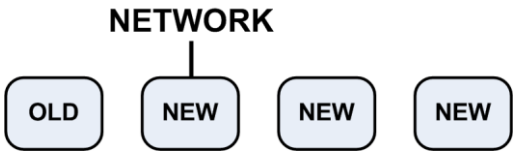
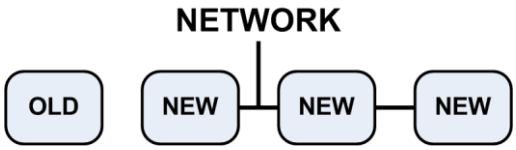
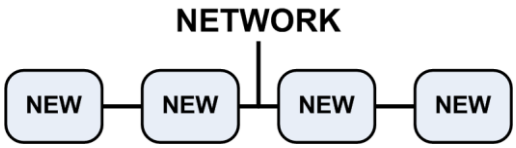
Diagram of Cluster Members	Summary	
	• Leave the cluster with the Hotfix connected to the network, and disconnect all other cluster members from the network. • For upgrades to R77.30, make sure that the cluster ID (the value of the `cluster_id` parameter) is the same on all cluster members. • For upgrades to R77.20 or an earlier version, make sure that the value of the `fwha_mac_magic` parameter is the same on all cluster members.	2 3
	• Upgrade the cluster members that are disconnected from the network (**NEW**). • For upgrades to R77.30 or a later version, make sure the cluster ID (the value of the `cluster_id` parameter) is the same on all the upgraded cluster members. Change it, if necessary. • For upgrades to R77.20 or an earlier version, make sure that the value of the `fwha_mac_magic` parameter on all the upgraded cluster members is the same. Change it, if necessary.	4 5
	• Connect one upgraded (**NEW**) cluster member to the network. • On the active (**OLD**) cluster member, turn off *fwaccel* on all Virtual Systems. This allows the active (**OLD**) cluster member synchronize all delayed connections with the upgraded (**NEW**) cluster member. **Note**: If there are a lot of connections on the Virtual Systems, turning off `fwaccel` will cause all the connections to be forwarded to the firewall. In this case, run the `cpstop` command to turn off the firewall. • On the active (**OLD**) cluster member, start the Optimal Service Upgrade procedure.	6 7 8

Diagram of Cluster Members	Summary	
	• On the upgraded cluster member (**NEW**) that you connected to the network, start the Optimal Service Upgrade procedure. The upgraded cluster member begins to process new connections.	9
	• Check the number of active connection on the old cluster member. When this cluster member almost stops processing connections, stop the Optimal Service Upgrade procedure on it. • Disconnect the old cluster member from the network.	10 11
	• Reconnect the other upgraded cluster members to the network.	12
	• Upgrade the old cluster member. • Connect all the cluster members to the network. • Install the policy.	13 14 15

Upgrading the VSX Cluster from R67.10

Two cluster members are used to maintain connectivity, while you upgrade all the other cluster members.

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. This is the old cluster member with Hotfix. For instructions and download links, refer to sk74300 http://supportcontent.checkpoint.com/solutions?id=sk74300.
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. On the old cluster member, configure kernel parameters:
   - **Upgrade to R77.30**:

     Run: `cphaconf cluster_id get`

     If the cluster ID value is not as expected, run: `cphaconf cluster_id set` *<value>*

     Make sure all cluster members have the same cluster ID. If a member has a different ID, run this `set` command to configure the correct value.

- **Upgrade to R77.20 and lower**:

  Make sure all cluster members use the same value for the `fwha_mac_magic` parameter.
  Run: `fw ctl get int fwha_mac_magic`

  The default value for the `fwha_mac_magic` parameter is `254`. If your configuration uses a different value, on each member, run: `fw ctl set int fwha_mac_magic` *<value>*

For more about the `cluster_id` and `fwha_mac_magic` parameters, see the *R77 ClusterXL Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=TBD and sk25977 http://supportcontent.checkpoint.com/solutions?id=sk25977.

4. Install R80.10 on all the cluster members that are not connected to the network.
5. Prepare the old cluster member for synchronization of old connections with the upgraded cluster member:
   a) On the old cluster member, turn off fwaccel - run: `fwaccel off -a`
   b) On the old cluster member, start the Optimal Serve Upgrade - 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

Connectivity Upgrade

Before you run Connectivity Upgrade:

- Make sure that the cluster has two members, one **Active** and one **Standby**
- Read sk107042 ClusterXL upgrade methods and paths
  http://supportcontent.checkpoint.com/solutions?id=sk107042
- Read sk101209 R77.20 Known Limitations
  http://supportcontent.checkpoint.com/solutions?id=sk101209
- Read sk104860 R77.30 Known Limitations
  http://supportcontent.checkpoint.com/solutions?id=sk104860

Check Point Connectivity Upgrade (CU) synchronizes existing connections to maintain connectivity during cluster upgrades.

Connectivity Upgrade is supported during these upgrades:

Upgrade from Version	R77.20	R77.30	R80.10
R75.40VS	CU	CU	CU
R75.46	CU	CU	CU
R75.47	CU	CU	CU
R76	CU	CU	CU
R77	-	CU	CU

Upgrade from Version	R77.20	R77.30	R80.10
R77.10	-	CU	CU
R77.20	-	CU	CU
R77.30	-	-	CU

Notes -

- Software Blade information does not get synchronized. If a connection needs to be inspected by a Software Blade, and this Software Blade is configured in SmartDashboard to *Prefer Connectivity Over Security*, then the connection is accepted without the inspection. Otherwise, the connection is dropped.
- All member gateways must have the same number of CoreXL Firewall instances.
- All member gateways must run the same 32-bit or 64-bit kernel edition.

Upgrading VSX High Availability Cluster

Before you upgrade:

Make sure that the cluster has 2 members, one of which is **Active** and the other is in **Standby**.

To check the cluster member status:

On each gateway, run: `cphaprob stat`

To upgrade the cluster:

1. Upgrade the **Standby** cluster member with a clean install.
2. On the upgraded cluster member, run: `cphaprob stat`
   Make sure the status is **Ready**.
3. Configure dynamic routing.
   For BGP, you must configure graceful restart, for BGP routes to remain after failover.
4. Run: `cphacu start [no_dr]`
   If dynamic routing synchronization is not required, use the `no_dr` option.
   The Connectivity Upgrade runs, and shows this message when it finishes: `Connectivity upgrade status: Ready for Failover`
5. On the old **Active** cluster member, run these commands:
   a) `cphaprob stat`
      Make sure the local member is in **Active** or **Active Attention** state, and the upgraded member is in **Down** state.
   b) `fwaccel off -a`
      Turns off `fwaccel` on all Virtual Systems so that the delayed connections are synchronized to the upgraded member that is now in **Ready** state.
   c) `cpstop`

The connections fail over to the upgraded member.

6. On the upgraded cluster member, run: `cphaprob stat`
   Make sure that it is now in **Active** state.
7. On the new **Active** cluster member, run: `cphacu stat`
   Make sure that it handles the traffic. See cphacu stat (on page 121).
8. Upgrade the former **Active** cluster member with a clean install.
   Reboot the gateway after the upgrade.

To make sure all cluster members are up and in VSX High Availability mode:

On each cluster member, run: `cphaprob stat`

If the state of a cluster member is **HA not started**, run: `cphastart`

Upgrading ClusterXL High Availability With Connectivity Upgrade

Before you upgrade:

Make sure that the cluster has 2 members, one of which is **Active** and the other is in **Standby**.

To check the cluster member status:

On each gateway, run: `cphaprob stat`

To upgrade the cluster:

1. Upgrade the standby cluster member.
   Reboot the gateway after the upgrade.
2. In SmartDashboard:
   a) In the **Gateway Cluster General Properties** window, change the **Cluster version** to the upgraded version.
   b) In the **Install Policy** window, go to **Installation Mode > Install on each selected gateway independently** section and make sure **For Gateway Clusters install on all the members, if it fails do not install at all** is not selected.
   c) Install the security policy on the cluster.

   Note - The policy successfully installs on the standby cluster member and fails to install on the Active cluster member. This is expected. Ignore the warning.
3. On the **Active** cluster member, run: `cphaprob stat`
   Make sure the status is **Active** or **Active Attention**, and record the **Sync IP** and the **Member ID** of the cluster member.
4. On the upgraded cluster member, run: `cphaprob stat`
   Make sure the status is **Ready**.
5. Configure dynamic routing.
   For BGP, you must configure graceful restart, for BGP routes to remain after failover.
6. Run: `cphacu start [no_dr]`
   If dynamic routing synchronization is not required, use the `no_dr` option.
   The Connectivity Upgrade runs, and shows this message when it finishes: `Connectivity upgrade status: Ready for Failover`

7. Run: `cphacu stat`
   Make sure that the **Active** cluster member handles the traffic.
8. On the **Active** cluster member, run these commands:
   a) `cphaprob stat`
      Make sure the local member is in **Active** or **Active Attention** state, and the upgraded member is in **Down** state.
   b) `fwaccel off -a`
      Turns off `fwaccel` on all Virtual Systems so that the delayed connections are synchronized to the upgraded member that is now in **Ready** state.
   c) `cpstop`
      The connections fail over to the upgraded cluster member.
9. On the upgraded cluster member, run: `cphaprob stat`
   Make sure that it is now in the **Active** state.
10. On the new upgraded cluster member, run: `cphacu stat`
    Make sure it handles the traffic.
11. Upgrade the former **Active** cluster member.
    Make sure to reboot it after the upgrade.
12. Install Policy.

After the cluster upgrade is complete, the Cluster Control Protocol is in the broadcast mode. To return it to the multicast mode, on all cluster members, run: `cphaconf set_ccp multicast`

Connectivity Upgrade Commands

cphacu start

Description Runs Connectivity Upgrade on a cluster member.

Syntax

```
cphacu start [no_dr]
```

Notes

If dynamic routing synchronization is not required, use the `no_dr` option.

Output

`cphacu start` command outputs this information:

- *Dynamic Routing synchronization status*
- *Performing Full Sync on VSID <VSID number>*
- *Connectivity Upgrade Status* -
  - *Disabled* - Connectivity Upgrade is not running on this cluster member
  - *Enabled, ready for failover* - Connectivity Upgrade completed successfully, and the **Active** member can now do the failover
  - *Not enabled since member is Active* - Connectivity Upgrade cannot run, because this member is **Active**
  - *Full sync for connectivity upgrade is still in progress. Wait until full sync finishes*

- *The peer member is handling the traffic* - Shows which cluster member currently handles the traffic and the version of the Cluster Control Protocol for each member
- *Connection table* - Shows the summary of the connections table for each Virtual System

Example 1 - VSX High Availability

```
[Expert@gw2:0]# cphacu start

Starting Connectivity Upgrade...


Dynamic routes synchronization started...
=========================================

Finished Dynamic routes synchronization.


Performing Full Sync
====================
Performing Full Sync on VSID 0. This may take several minutes (depending on the
number of connections); please wait...
Performing Full Sync on VSID 2. This may take several minutes (depending on the
number of connections); please wait...
Performing Full Sync on VSID 3. This may take several minutes (depending on the
number of connections); please wait...

================================================================================
Full Sync ended (Delta Sync is enabled)
For delayed connections (Templates) to be synchronized it is recommended to turn
off SecureXL
on the old member before doing a failover. Run: 'fwaccel off' on the old member
Please note: turning SecureXL off might slow down existing connections.
================================================================================

Connectivity upgrade status: Enabled, ready for failover
========================================================

The peer member is handling the traffic
=======================================
Version of the local member: 3122
Version of the peer member : 2502

Connections table
=================
VS      HOST            NAME               ID   #VALS  #PEAK  #SLINKS
0       localhost       connections        8158 30     103    34
2       localhost       connections        8158 0      1      0
3       localhost       connections        8158 1      2      2
```

Example 2 - ClusterXL High Availability

```
[Expert@HostName]# cphacu start
Starting Connectivity Upgrade...

Dynamic routes synchronization started...
=========================================

Finished Dynamic routes synchronization.


Performing Full Sync
====================
Performing Full Sync. This may take several minutes (depending on the number of
```

```
connections); please wait...

================================================================================
==
Full Sync ended (Delta Sync is enabled)
For delayed connections (Templates) to be synchronized it is recommended to turn
off SecureXL
on the old member before doing a failover. Run: 'fwaccel off' on the old member
Please note: turning SecureXL off might slow down existing connections.
================================================================================
==

Connectivity upgrade status: Enabled, ready for failover
============================================================

The peer member is handling the traffic
=======================================
Version of the local member: 3121
Version of the peer member : 2910

Connections table
=================
HOST                  NAME                                ID #VALS #PEAK #SLINKS
localhost             connections                       8158    34    38
37
```

Example 3 - No Dynamic Routing VSX

```
[Expert@gw2:0]# cphacu start no_dr

Starting Connectivity Upgrade...


Dynamic routing synchronization is disabled!

Performing Full Sync
====================
Performing Full Sync on VSID 0. This may take several minutes (depending on the
number of connections); please wait...
Performing Full Sync on VSID 2. This may take several minutes (depending on the
number of connections); please wait...
Performing Full Sync on VSID 3. This may take several minutes (depending on the
number of connections); please wait...

================================================================================
==
Full Sync ended (Delta Sync is enabled)
For delayed connections (Templates) to be synchronized it is recommended to turn
off SecureXL
on the old member before doing a failover. Run: 'fwaccel off' on the old member
Please note: turning SecureXL off might slow down existing connections.
================================================================================
==

Connectivity upgrade status: Enabled, ready for failover
============================================================

The peer member is handling the traffic
=======================================
Version of the local member: 3122
Version of the peer member : 2502

Connections table
```

```
=================
VS       HOST       NAME               ID   #VALS #PEAK #SLINKS
0        localhost  connections        8158    28   103       30
2        localhost  connections        8158     0     1        0
3        localhost  connections        8158     1     2        2
```

cphacu stat

Description Shows the status of Connectivity Upgrade.

Syntax

```
cphacu stat
```

Example 1 - VSX High Availability

```
 [Expert@HostName]# cphacu stat

Connectivity upgrade status: Disabled
====================================

The peer member is handling the traffic
========================================
Version of the local member: 2907
Version of the peer member : 2502

Connection table
================
VS       HOST          NAME                ID    #VALS    #PEAK     #SLINKS
0        localhost     connections         8158    16      56        16
1        localhost     connections         8158     0      3         0
2        localhost     connections         8158     0      0         0
3        localhost     connections         8158     0      0         0
4        localhost     connections         8158     0      0         0
5        localhost     connections         8158     0      0         0
6        localhost     connections         8158     0      1
```

Example 2 - ClusterXL High Availability

```
 [Expert@HostName]# cphacu stat

Connectivity upgrade status: Disabled
====================================

The peer member is handling the traffic
========================================
Version of the local member: 2907
Version of the peer member : 2502

Connection table
================
HOST                  NAME                 ID    #VALS    #PEAK    #SLINKS
localhost             connections          8158    16      56
```

Upgrading with SmartUpdate

In This Section:

Introduction

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.

These 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.

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
- Upgrade a package to a management version other than the latest
- Apply Hot Fix Accumulators (HFAs)

To update a single package on a remote gateway:

1. In the **Package Management** window, click the Check Point Security Gateway to upgrade.
2. Select **Packages > distribute**.
3. From the **distribute Packages** window, select the package to distribute.

   Use the `Ctrl` and `Shift` keys to select multiple packages, and click **distribute**.

   The installation proceeds only if the upgrade packages selected are available in the **Package Repository**.

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.

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 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 *R80.10 Command Line Interface Reference Guide* http://supportcontent.checkpoint.com/documentation_download?ID=TBD.

- **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 Licenses Using SmartUpdate

To open SmartUpdate, select **Manage Licenses and Packages** from the SmartConsole main menu. The **SmartUpdate** window opens.

To manage licenses using SmartUpdate, select the **SmartUpdate** view in the SmartConsole 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 see the repository contents:

1. Open SmartUpdate.
2. In the menu, click **SmartUpdate** > **Licenses & Contracts** > **View Repository**. The **License & Contract Repository** pane shows in the SmartUpdate view.

To add new licenses to the repository:

1. Right-click in an empty part of the repository view.
2. Click **SmartUpdate** > **Licenses & Contracts** > **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 see the new license in the repository.

To attach a license to a component:

1. Click **SmartUpdate** > **Licenses & Contracts** > **Attach License**.
2. Select a license from the **Attach Licenses** window. The license shows as attached in the repository.

Web Security License Enforcement

A gateway or gateway cluster requires a **Web Securit**y 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

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.

Sending CPinfo to Check Point Automatically

SmartUpdate lets you automatically generate and send CPinfo to Check Point Technical support.

To automatically generate and send CPinfo:

1. Open **SmartUpdate**.
2. Right click a Security Gateway or Security Management Server.
3. Select **Upload CPInfo to Check Point**.

The **Upload CPinfo from...** window opens.

4. Enter your **UserCenter** authentication credentials (email and password) and SR number.
5. Select **Download and install latest CPInfo package**.
6. Enter an SR Number if you have one.
7. Click **Upload More files** if you want to send additional files.

   Click **Add** to enter the full path to the remote file on the remote gateway or Security Management Server.
8. Click **OK**.

   The **Operation Status** window opens.
   - CPinfo generates the data, encrypts and transfers the data to the **UserCenter**.
   - After the secure file upload successfully completes, an email notification is sent to the email address specified in step 3.

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.

Check Point Cloud Services

In This Section:

Automatic Downloads

Check Point products connect to Check Point cloud services to download and upload information.

You can enable or disable **Automatic Downloads** in the Gaia First Time Configuration Wizard, on the **Products** page. We recommend that you enable Automatic Downloads, so that you can use these features:

- *Blade Contracts* are annual licenses for Software Blades and product features. If there is no of a valid Blade contract, the applicable blades and related features will work, but with some limitations.
- *CPUSE* lets you manage upgrades and installations with the Gaia WebUI.

  Note - To learn more about CPUSE, see: sk92449
  http://supportcontent.checkpoint.com/solutions?id=sk92449
- *Data updates* and *Cloud Services* are necessary for the full functionality of these Software Blades and features:
  - Application Control and URL Filtering
  - Application Database
  - URL database
  - AppWiki
  - Threat Prevention (Anti-Bot, Anti-Virus, Anti-Spam, IPS, Threat Emulation)
  - Threat Wiki
  - HTTPS Inspection
  - Compliance
  - SmartEndpoint

The Automatic Downloads feature is applicable to the Security Management Server, Multi-Domain Server, log servers, and Security Gateways (R77 and higher).

If you disable Automatic Downloads in the First Time Configuration Wizard, you can enable it again in **Global Properties**:

1. Open **Global Properties > Security Management Access**.
2. Select **Automatically download Contracts and other important data**.
3. Restart SmartDashboard.
4. Install the Policy

To learn more, see sk94508 http://supportcontent.checkpoint.com/solutions?id=sk94508.

Sending Data to Check Point

In the Gaia First Time Configuration Wizard, on the **Summary** page, you can enable or disable data uploads to Check Point. This feature is enabled by default. The **Upgrades (CPUSE)** action statistics require this feature.

In R77 and higher, this setting activates the Check Point User Center Synchronization tool. It updates your User Center account with information from your Security Gateways, mapping your SKUs to your actual deployment.

This setting of a Security Management Server applies to all its Security Gateways (R77 and above).

You can always change this setting in SmartConsole.

1. Open **Menu** > **Global Properties** > **Security Management Access**.
2. Select **Improve product experience by sending data to Check Point**.
3. Restart SmartDashboard.
4. Install the Policy

To learn more, see sk94509 http://supportcontent.checkpoint.com/solutions?id=sk94509.

Note: In some cases, the download process sends a minimal amount of required data about your Check Point installation to the Support Center.

Advanced Deployments and Conversions

In This Section:

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 configuring the bridge, install the Security Gateway.

To manage the gateway in bridge mode:

- The gateway must have a separate, routed IP address
- You must configure the bridged interfaces

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:

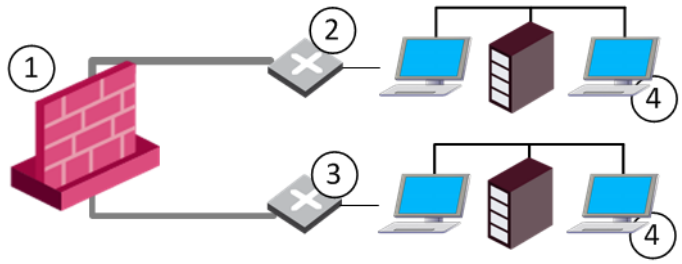
1. Run: `add bridging group <Group Name> interface <physical interface name>`
2. Run again for each interface in the bridge.
3. Run: `save config`
4. Add a bridge interface IP address:
   - IPv4: `set interface <Group Name> ipv4-address <IP> subnet-mask <Mask>`
   - IPV6: `set interface <Group Name> ipv6-address <IP> mask-length <Prefix>`
5. Run: `save config`

Supported Software Blades: Gateway and Virtual Systems

These Software Blades support bridge mode (unless stated they do not) for single Security Gateway deployment, cluster with one switch in Active/Active and Active/Standby deployment, and cluster with four switches.

Supported Blade	Supports Gateways in Bridge Mode	Supports Virtual Systems in Bridge Mode
Firewall	Yes	Yes
IPS	Yes	Yes
URL Filtering	Yes	Yes
DLP	Yes	No
Anti-Bot and Anti-Virus	Yes	Yes
Application Control	Yes	Yes
HTTPS Inspection	Yes	No
Identity Awareness	Yes	No
Threat Emulation	Yes	Yes
QoS	Yes	No
Client Authentication	Yes	No
User Authentication	Yes	No

Configuring One Gateway in Bridge Mode



Item	Description
1	Security Gateway bridges Layer-2 traffic over one IP address, with a subnet on each side, using the same address
2	Switch from a bridged interface to a subnet
3	Switch from a second bridged interface to a second subnet
4	Internal network

To define the bridge topology:

1. Configure a dedicated management interface.
2. Configure the bridge interface. It must be in the bridged subnet. Only the bridge interface has an IP address. The bridge ports must not have IP addresses.
3. Configure the bridge topology in the properties of the network object:
   - If a bridge port connects to the Internet, set the interface to **External**.
   - If the Security Gateway is in rules with Internet objects, set the interface to **External**.
   - If the topology uses Anti-Spoofing for the internal port (interface), set the interface to **Internal** and select the network that connects to the port.
   - If the topology does not use Anti-Spoofing, disable Anti-Spoofing on the bridge port.

   For example:

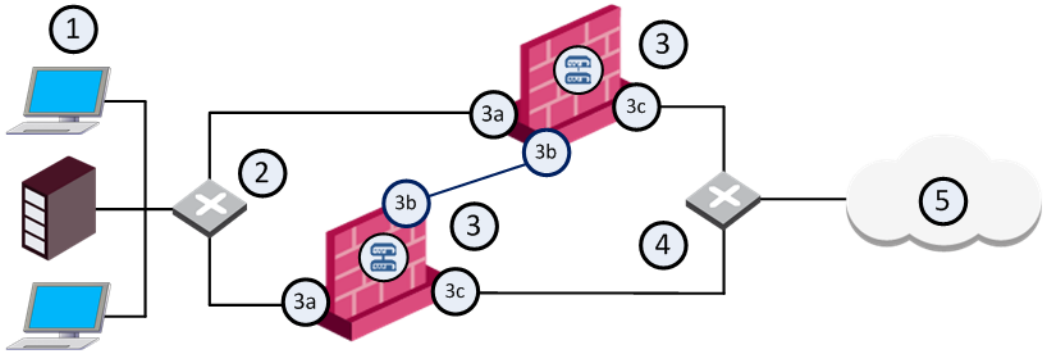
   Bridge Interface - **eth0** - **External** - **192.0.2.0.208/24**

   Bridge Port to Internet - **eth1** - **External** - **0.0.0.0/0**

   Bridge Port with Anti-Spoofing - **eth2** - **Internal to** *CP_default_Office* **network** - **0.0.0.0/0**

Configuring Gateway Cluster in Bridge Mode

You can configure cluster gateways for bridge mode in different deployments Active/Standby mode or Active/Active mode.



Item	Description
1	Internal network
2	Switch for internal network
3	Security Gateway bridging Layer-2 traffic
3a	eth1 - connects to the internal network
3b	eth3 - ClusterXL Sync interface
3c	eth2 - connects to the external network (192.168.10.1)
4	Switch for external network
5	Internet

Configuring Active/Standby Mode

This is the preferred mode in topologies that support it.

In Active-Standby mode, ClusterXL decides the cluster state. The standby member drops all packets. It does not pass any traffic, including STP/RSTP/MSTP. If there is a failover, the switches are updated by the Security Gateway to forward traffic to the new active member.

If you use this mode, it is best to disable STP/RSTP/MSTP on the adjacent switches.

To configure Active/Standby mode:

1. Configure the cluster ("Configuring Active/Active Mode " on page 139).
2. Run: `cpconfig`
3. Enter `8`, to select **Enable Check Point ClusterXL for Bridge Active/Standby**.
4. Confirm: `y`
5. Reboot the cluster member.
6. Install Policy.
7. Test the cluster state: `cphaprob stat`

   The output should be similar to:

```
Cluster Mode: High Availability (Active Up, Bridge Mode) with IGMP Membership
Number     Unique Address     Firewall State (*)
1 (local>  2.2.2.3            Active
2          2.2.2.2            Standby
```

Configuring Active/Active Mode

When you define a bridge interface on a Security Gateway cluster, Active/Active mode is activated by default.

Before you begin, install ClusterXL High Availability on a Gaia appliance or open server.

To configure Active/Active mode, do these steps on each member of the cluster:

1. Configure dedicated management and Sync interfaces.
2. Add a bridge interface, as in a one-gateway deployment ("Configuring One Gateway in Bridge Mode" on page 137).

   Do not configure an IP address on the newly created bridge interface.
3. In SmartDashboard, add the cluster object:

   a) Open the **Network Management** page of the of the cluster object.

   b) Get the cluster Interfaces with Topology.

   c) Make sure the dedicated management and Sync interfaces are configured.

   d) Make sure the bridge interface and bridge ports are not in the topology.

   Bridge port topology cannot be defined. It is **external** by default.
4. Install Policy.
5. See the cluster state: `cphaprob stat`

   Example of expected output:

```
Cluster Mode: High Availability (Active Up, Bridge Mode) with IGMP
Membership
Number     Unique Address     Firewall State (*)
1 (local>  192.0.2.3            Active
2          192.0.2.2            Active
```

6. Make sure that cluster is configured for High Availability ("Confirming the High Availability Configuration" on page 140).

Confirming the High Availability Configuration

After you configure Active/Active mode, the output for `chpaprob stat` shows that the `Firewall State` is `Active/Active`. Make sure that the cluster is configured for High Availability.

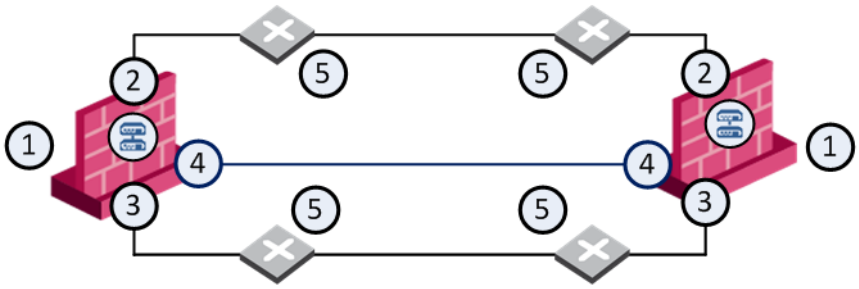
To confirm the High Availability configuration:

1. Open the cluster object.
2. In the cluster **Properties** window, click **ClusterXL**.
3. In the **Cluster Mode** section, make sure that **High Availability** is selected.
4. Click **OK**.

Cluster Between Four Switches

You can configure a bridged cluster between four switches, in Active/Active mode.

Active/Standby mode is not supported.



Item	Description
1	Security Gateway bridging Layer-2 traffic
2	eth1
3	eth2
4	eth3 - ClusterXL Sync interface
5	Switch

See also: Link Aggregation with ClusterXL in Layer-2
http://supportcontent.checkpoint.com/documentation_download?ID=23341

Routing and Bridges

Security Gateways with a bridge interface can support Layer 3 routing over non-bridged interfaces. If you configure a bridge interface with an IP address for one Security Gateway (not a cluster), the bridge functions as a regular Layer 3 interface. It participates in IP routing decisions on the gateway and supports Layer 3 routing.

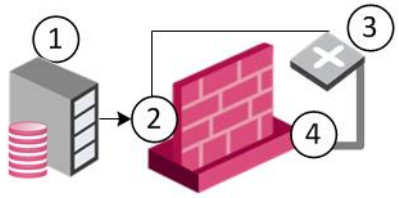
- Cluster deployments do not support this configuration.
- You cannot configure the bridge to be the route gateway.
- One Security Gateway can support multiple bridge interfaces, but only one bridge can have an IP address.

- The Security Gateway cannot filter or transmit packets on a bridge interface that it inspected before (*double-inspection*).

Management over Bridge

When a Layer-3 management interface sends traffic through the firewall, the traffic is dropped. The firewall cannot inspect the same packet again.

- The first packet is inspected and goes from the management interface to the router.
- The router sends the packet to the bridge interface.
- The firewall concludes that this packet is a retransmission and drops it.



Item	Description
1	Security Management Server sends management packet to management interface
2	Management interface on Security Gateway Firewall bridging Layer-2 traffic inspects the packet and sends it to the router
3	Router sends the packet to the bridge interface
4	Bridge interface drops the packet as a retransmission

Configure the Security Gateway to handle management packets properly.

Security Gateways R77.10 and Higher

This feature is supported in R77.10 and higher.

You can configure the Security Gateway to recognize that the first packet is from the management interface. The firewall makes sure that the MD5 hash of the packet that leaves the management interface and enters the bridge interface is the same. Other packets in this connection are handled by the bridge interface without using the router.

To enable management over the bridge:

1. Edit `$FWDIR/boot/modules/fwkern.conf`.
   If necessary, create this file.
2. Add the appropriate line to the file:
   - For IPv4 traffic - `fwx_bridge_reroute_ipv4=<management>`
   - For IPv6 traffic - `fwx_bridge_reroute_ipv6=<management>`

   `<management>` is the IP address of the management interface.
3. Reboot the Security Gateway.

Security Gateways R77 and Earlier

Incoming and outgoing traffic from a Layer-3 management interface is dropped if traversed over a bridge interface. You can make this traffic pass. Disable inspection on the management interface and disable local Anti-Spoofing.

Note: This removes inspection from the management interface and could compromise gateway security. If you are unsure whether your environment is safe to use this method, contact Check Point Solution Center.

To configure management over the bridge:

1. Open `$PPKDIR/boot/modules/simkern.conf` and add:
   `simlinux_excluded_ifs_list=`*interface name*
   (Create this file if not found.)
   Where the value (*interface name*) is the management interface name.
   This excludes the management interface from SecureXL.
2. Edit $`FWDIR/modules/fwkern.conf`.
   (Create this file if not found.)
   Add these lines:
   ```
   fwx_bridge_use_routing=0
   fw_local_interface_anti_spoofing=0
   fwlinux_excluded_ifs_list=interface name
   ```
   Where the value (*interface name*) is the management interface name.
   This disables local Anti-Spoofing and bridge routing, and excludes the management interface from security inspection.
3. Reboot.

IPv6 Neighbor Discovery

Neighbor discovery works over the ICMPv6 Neighbor Discovery protocol, which is the functional equivalent of the IPv4 ARP protocol. ICMPv6 Neighbor Discovery Protocol must be explicitly allowed for all bridged networks in your Firewall rules. This is different from ARP, for which traffic is always allowed regardless of the Rule Base.

This is an example of a rule that allows ICMPv6 Neighbor Discovery protocol:

- **Source** - *Bridged_Network*
- **Destination** - *Bridged_Network*
- **Services & Applications** - **neighbor-advertisement**, **neighbor-solicitation**, **router-advertisement**, **router-solicitation**, **redirect6**
- **Action** - **Accept**

Configuring Link State Propagation

You can bind two ports together, so that when the link state for one port goes down, the other port also goes down. This lets a switch detect and react to a link failure on the other side of a bridge or another part of the network.

This feature is available in one of these modes:

- **Automatic port detection and port pair creation** - All bridge ports are assigned to a port pair (the pair in the bridge).
- **Manual port pair creation** - Up to four port pairs are supported.

Link state propagation is supported on these Check Point appliance line cards:

- CPAC-4-1C/CPAC-8-1C – Copper line cards with IGB driver

- CPAC-4-1F – 1Gbe fiber line card with an IGB driver
- CPAC-4-10F – 10Gbe fiber line card with an IXGBE driver

For example:
```
fw_lsp_pair1="eth1,eth2"
```

Note - You can add up to four lines to this file, one for each pair.

Note: The below procedures are applicable to R77.20 and higher.

To configure Link State Propagation for automatic port detection:

1. Open `FWDIR/modules/fwkern.conf` in a text editor.
   If there is no `fwkern.conf` file, create a new one.
2. Add this line:
   `fw_link_state_propagation_enabled=1`
3. Reboot the computer.

To create port pairs automatically:

1. Open `FWDIR/modules/fwkern.conf` in a text editor.
   If there is no `fwkern.conf` file, create a new one.
2. Add these lines:
   ```
   fw_link_state_propagation_enabled=1
   fw_manual_link_state_propagation_enabled=1
   fw_lsp_pair<1-4>="<interface_name1,interface_name2>"
   ```
3. Reboot the computer.

Note - Link State Propagation is a Firewall Software Blade feature. It is supported for Security Gateways and clusters. You must configure Link State Propagation for each cluster member.

Managing Ethernet Protocols

This feature is supported in R77.10 and higher.

It is possible to configure a Security Gateway with bridge interface to allow or drop protocols that are not based on IP that pass through the bridge interface. For example, protocols that are not IPv4, IPv6, or ARP.

By default, these protocols are allowed by the Security Gateway.

To manage the traffic of Ethernet protocols:

1. Change the value of global parameter `fwaccept_unknown_protocol` in `$FWDIR/modules/fwkern.conf`. The default value is `1`.
2. Create user defined tables in `$FWDIR/conf/user.def`:

```
$ifndef __user_def__
$define __user_def__

\\
\\ User defined INSPECT code
\\
```

```
allowed_ethernet_protocols={ <0x44,0x44> );
dropped_ethernet_protocols={ <0x4,0x4> );


fendif /*__user_def__*/
```

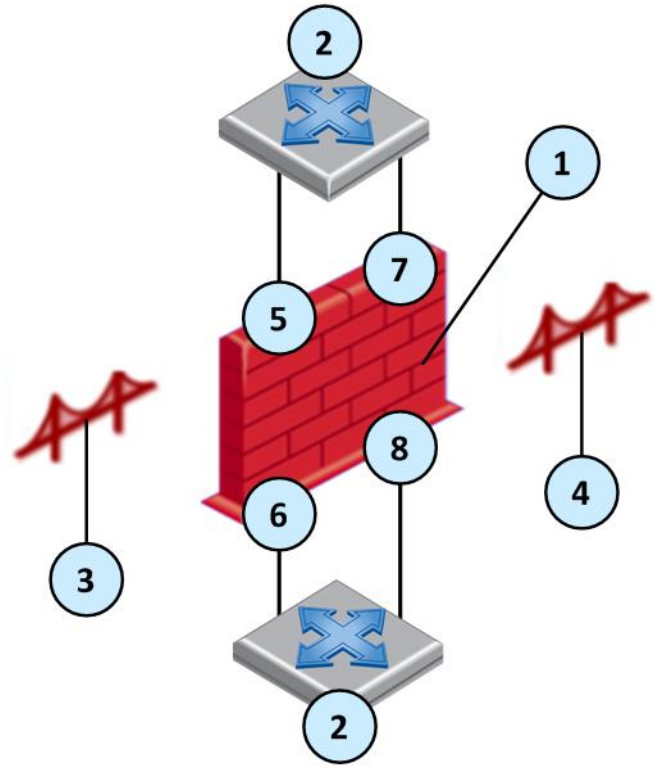
Traffic is allowed if:

- `fwaccept_unknown_protocol` is enabled
- OR protocol is in `allowed_ethernet_protocols` table
- AND NOT in `dropped_ethernet_protocols` table

VLANs

When switches are configured with VLANs, VLAN traffic can pass through our bridge in Access mode or in Trunk mode:

- **Access mode** (VLAN translation) – Bridge is constructed from two VLAN interfaces.
- **Trunk mode** – Bridge is constructed from two non-VLAN interfaces. The VLAN tag is not removed, and the firewall processes the tagged packet. The traffic passes with the original tag to its destination.



Item	Description
1	Security Gateway
2	Switch
3	Access mode bridge 1 with VLAN translation
4	Access mode bridge 2 with VLAN translation
5	VLAN 3 (eth 1.3)

Item	Description
6	VLAN 33 (eth 2.33)
7	VLAN 2 (eth 1.2)
8	VLAN 22 (eth 2.22)

Access Mode VLAN

When the switch is configured in Access Mode, create the bridge from two VLAN interfaces as the slave ports of the bridge. For VLAN translation, use different numbered VLAN interfaces to create the bridge. You can build multiple VLAN translation bridges on the same Security Gateway.

Note - VLAN translation is not supported over bridged FONIC (Fail open NIC) ports. See sk85560 http://supportcontent.checkpoint.com/solutions?id=sk85560.

To configure VLAN translation:

1. Add the VLANs. In the WebUI: **Network Management > Network Interfaces > Add > VLAN**.
2. The **Add VLAN** window opens. Configure the interfaces of the VLAN: **IPv4**, **IPv6**, **VLAN ID**, and add the VLAN interface to a physical interface.

   When you set a VLAN ID to be a member of a physical interface, the VLAN interface name *<physical_interface>.<vlan_id>*. For example, if **VLAN ID 2** is a member of **eth1**, the VLAN interface is **eth1.2.**
3. Open the **Add Bridge** window and select the VLAN interfaces in the **Bridge** tab.

Special Protocols

PVST - Per-VLAN Spanning Tree. PVST is a proprietary Cisco version of STP and maintains a spanning tree instance for each VLAN. It uses ISL Trunking and lets a VLAN trunk be forwarded for some VLANs and blocked for others. Because PVST treats each VLAN as a separate network, it can load balance traffic at layer-2. It forwards some VLANs on one trunk and other VLANs on another trunk without causing a Spanning Tree loop.

BPDU - Bridge Protocol Data Unit. BPDUs are data messages that are exchanged across the switches within an extended LAN that uses STP topology.

When VLAN translation is configured, BPDU frames can arrive with the wrong VLAN number to the ports through the bridge. This mismatch can cause the switch port to enter blocking mode.

In Active-Standby mode only, there are options to avoid blocking mode.

To disable BPDU forwarding:

1. Edit the file `/etc/rc.d/init.d/network`
2. After the line:
   `./etc/init.d/functions`

   Add this line:
   `/sbin/sysctl -w net.bridge.bpdu_forwarding=0`
3. Save the file.
4. Reboot the Security Gateway.

To configure the gateway to allow only IPv4, IPv6, and ARP traffic:

1. Add to **$FWDIR/modules/fwkern.conf** the line: `fwaccept_unknown_protocol=0`
2. Reboot the Security Gateway.

Trunk Mode

If you configure the switch ports as VLAN trunk, the Check Point bridge should not interfere with the VLANs. To configure bridge with VLAN trunk, create the bridge from two interfaces (no VLAN).

Note - VLAN translation is not supported in Trunk mode.

Converting a Security Management Server to Multi-Domain Server on Smart-1 Appliances

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 SmartConsole on a computer and 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 net mask 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 Smart-1 50 or 150 appliances 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 then enter Expert mode.
2. Run `s2mwrapper`.
3. Follow the on-screen instructions.
4. Log out of the appliance.
5. Log in SmartConsole with the `cpconfig` administrator user name and password.

Security Before Firewall Activation

There are different reasons for a computer to not have a security policy installed and to be vulnerable. To protect the computer and network, Check Point has baseline security:

- **Boot Security -** Security during boot process
- **Initial Policy -** Security before a policy is installed for the first time

Boot Security

During the boot process, there are a few seconds after the computer can receive communication (and can be attacked) and before the security policy is loaded and enforced. firewall Boot Security protects the computer, and its networks, during this time. Boot Security works through *control of IP Forwarding* on boot and the *Default Filter*.

The Default Filter also provides protection if firewall processes are stopped for maintenance.

Control of IP Forwarding on Boot

Boot Security disables IP forwarding in the OS kernel. There is never a time when IP Forwarding is active without a security policy. This protects the networks behind the Security Gateway.

The Default Filter

Boot Security loads the Default Filter when it disables IP Forwarding, after bootup and before interfaces are configured. You can configure the Default Filter to work in different modes:

- *General Filter* accepts no inbound communication (this is the default option).
- *Drop Filter* accepts no inbound or outbound communication. This filter drops all communications in and out of the gateway during a period of vulnerability.

  Best Practice: If the boot process requires that the gateway communicate with other hosts, do not use the Drop Filter.

The Default Filter also provides Anti-Spoofing protection for the Security Gateway.

Changing the Default Filter

There are two filter files in **$FWDIR/lib**: **defaultfilter.boot** and **defaultfilter.drop**

To change the Default Filter:

1. Copy the Default Filter file (**defaultfilter.boot** or **defaultfilter.drop**) to: `$FWDIR/conf/defaultfilter.pf`
2. Compile the Default Filter: `fw defaultgen`

   The output is `$FWDIR/state/default.bin`
3. Get the Default Filter file path: `fwboot bootconf get_def`
4. Copy `default.bin` to the Default Filter file path.
5. Generate the Initial Policy: `cpconfig`

Defining a Custom Default Filter

For administrators with Inspect knowledge, you can define your own Default Filter.

Make sure your security policy does not interfere with the boot process.

To define a Default Filter:

1. Create an Inspect script named: `$FWDIR/conf/defaultfilter.pf`

   Important - The script must not do these functions:
   - Logging
   - Authentication
   - Encryption
   - Content security
2. Run: `fw defaultgen`
3. Run: `fwboot bootconf get_def`
4. Copy `$FWDIR/state/default.bin` to the Default Filter file path.
5. Generate the Initial Policy from: `cpconfig`

Using the Default Filter for Maintenance

It is sometimes necessary to stop firewall processes for maintenance. It is not always practical to disconnect the Security Gateway from the network (for example, if the gateway is on a remote site).

Run the `cpstop` command with the `-fwflag` *<value>* to make sure the Security Gateway is protected when Check Point processes are stopped.

```
> cpstop -fwflag {-proc|-default}
```

Parameter	Description
`-fwflag -proc`	Maintains the active Security Policy running in the kernel when Check Point daemons and services are stopped. Rules with generic allow, reject, or drop rules based on services continue to work.
`-fwflag -default`	The active Security Policy running in the kernel is replaced with the Default Filter, which allows open connections to the gateway to remain open.

The Initial Policy

Until the Security Gateway administrator installs the security policy on the gateway for the first time, security is enforced by an Initial Policy. The Initial Policy operates by adding "implied rules" to the Default Filter. These rules forbid most communication yet allows the communication needed for the installation of the security policy. The Initial Policy also protects a gateway during Check Point product upgrades, when a SIC certificate is reset on the gateway, or in the case of a Check Point product license expiration.

Note - During a Check Point upgrade, a SIC certificate reset, or license expiration, the Initial Policy overwrites the user-defined policy.

The sequence of actions during boot of the Security Gateway computer until a security policy is loaded for the first time:

1. The computer boots up.
2. The Default Filter loads and IP Forwarding is disabled.
3. The interfaces are configured.
4. Security Gateway services start.
5. The Initial Policy is fetched from the local gateway.
6. SmartConsole clients connect or Trust is established, and the security policy is installed.

The Initial Policy is enforced until a user-defined policy is installed, and is never loaded again. In subsequent boots, the regular policy is loaded immediately after the Default Filter.

There are different Initial Policies for standalone and distributed setups. In a standalone configuration, where the Security Management Server and the Security Gateway are on the same computer, the Initial Policy allows CPMI communication only. This permits SmartConsole clients to connect to the Security Management Server.

In a distributed configuration, where the Primary Security Management Server is on one computer and the Security Gateway is on a different computer, the Initial Policy allows the following:

- Primary Security Management Server computer — allows CPMI communication for SmartConsole clients.
- Security Gateway — allows **cpd** and **fwd** communication for SIC communication (to establish trust) and for Policy installation.

In a distributed configuration, the Initial Policy on the Security Gateway does not allow CPMI connections. The SmartConsole will not be able to connect to the Security Management Server if the SmartConsole must access the Security Management Server through a gateway running the Initial Policy.

There is also an Initial Policy for a Secondary Security Management Server (Management High Availability). This Initial Policy allows CPMI communication for SmartConsole clients and allows **cpd** and **fwd** communication for SIC communication (to establish trust) and for Policy installation.

Monitoring Security

You can see that the Default Filter or the Initial Policy are loaded on a non-production Security Gateway. Restart the computer before Install Policy and run:
`$FWDIR/bin/fw stat`

If the output shows **defaultfilter** for the Default Filter status and **InitialPolicy** for the installed policy, the computer is running on the default, pre-firewall security.

Unloading Default Filter or Initial Policy

To unload a Default Filter or an Initial Policy from the kernel, use the command to unloading a regular policy. Do this only if you are sure that the security of the Default Filter or Initial Policy is not required.

To unload the Default Filter locally: `fw unloadlocal`

To unload an Initial Policy from a remote Security Management server: `fwm unload` *<gateway>*

Where *gateway* is the SIC_name of the gateway.

Troubleshooting: Cannot Complete Reboot

In some configurations, the Default Filter prevents the Security Gateway from completing the reboot after installation.

First, look at the Default Filter. Does the Default Filter allow traffic required by the boot procedures? If the boot process cannot complete successfully, remove the Default Filter.

1. Reboot in **single user** mode.
2. Set the Default Filter to not load again: `fwbootconf bootconf Set_def`
3. Reboot.

Command Line Reference

control_bootsec

Enables or disables Boot Security. The command affects both the Default Filter and the Initial Policy.

`$FWDIR/bin/control_bootsec [-r] [-g]`

Options	Description
-r	Removes boot security
-g	Enables boot security

fwboot bootconf

Configure boot security options. This command is in `$FWDIR/boot`.

`$FWDIR/bin/fwboot bootconf <command> [value]`

Commands	Values	Description
Get_ipf	none	Reports if firewall controls IP Forwarding. • Returns 1 if IP Forwarding control is enabled on boot. • Returns 0 if IP Forwarding is not controlled on boot.
Set_ipf	0 | 1	Turns off/on control of IP forwarding for the next boot. **0 -** Turns off **1 -** Turns on
Get_def	none	Returns the full path to the Default Filter that will be used on boot.

Set_def	<*filename*>	Loads the file as the Default Filter in the next boot. The only safe and recommended directory is `$FWDIR\boot`**.** (The `default.bin` filename is a default name.) **Note -** Do NOT move these files.

comp_init_policy

Use the *comp_init_policy* command to generate and load, or to remove, the Initial Policy.

This command generates the Initial Policy. It ensures that it will be loaded when the computer is booted, or any other time that a Policy is fetched, for example, at *cpstart*, or with the **f***w fetch localhost* command. After running this command, *cpconfig* adds an Initial Policy if there is no previous Policy installed.

```
$FWDIR/bin/comp_init_policy [-u | -g]
```

Options	Description
-u	Removes the Initial Policy, and makes sure that it will not be generated in the future when **cpconfig** is run.
-g	Generates the Initial Policy and makes sure that it is loaded the next time a policy is fetched (`cpstart`, `reboot`, `fw fetchlocalhost`). After running this command, **cpconfig** adds an Initial Policy when needed.

The *comp_init_policy -g* command will only work if there is no previous policy. If there is a policy, make sure that after removing the policy, you delete the folder *$FWDIR\state\local\FW1***.** The *$FWDIR/state/local/FW1* folder contains the policy that will be fetched when *fw fetch localhost* is run.

The *fw fetch localhost* command is the command that installs the local policy. *cpstart. comp_init_policy* creates the initial policy, but has a safeguard so that the initial policy will not overwrite a regular user policy (since initial policy is only used for fresh installations or upgrade). For this reason, you must delete the *$FWDIR\state\local\FW1* directory if there is a previous policy, otherwise *comp_init_policy* will detect that the existing user policy and will not overwrite it.

If you do not delete the previous policy, the original policy will be loaded.

cpstop -fwflag default and cpstop -fwflag proc

To stop all firewall processes but leave the Default Filter running, run: `cpstop -fwflag -default`

To stop all Security Gateway processes but leave the security policy running, run: `cpstop -fwflag -proc`

To stop and start all Check Point processes, run: `cpstop` and `cpstart`

```
cpstop -fwflag [-default | -proc]
```

Options	Description
-default	Kills firewall processes (such as `fwd`, `fwm`, `vpnd`**,** `snmpd`). Logs, kernel traps, resources, and security server connections stop. The security policy in the kernel is replaced with the Default Filter.

-proc	Kills firewall processes. Logs, kernel traps, resources, and security server connections stop. The security policy remains loaded in the kernel. Allow, reject, and drop rules that do not use resources, only services, continue to work.