Important Information

**Check Point R80**
For more about this release, see the R80 home page

**Latest Version of this Document**
Download the latest version of this document
To learn more, visit the Check Point Support Center

**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 R80 Installation and Upgrade Guide.

**Searching in Multiple PDFs**
To search for text in all the R80 PDF documents, download and extract the complete R80 documentation package
To search for all text in the R77 PDF documents, download and extract the R77 documentation package
Use **Shift-Control-F** in Adobe Reader or Foxit reader.

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 September 2016</td>
<td>Added Upgrading each Domain Server Separately with Migration (on page 28), general updates</td>
</tr>
<tr>
<td>18 July 2016</td>
<td>Improved layout.</td>
</tr>
<tr>
<td>01 June 2016</td>
<td>Improved layout and formatting.</td>
</tr>
<tr>
<td>09 May 2016</td>
<td>• Added <em>Migrating an R80 Database to Another R80 Server</em> (on page 30)</td>
</tr>
<tr>
<td></td>
<td>• Clarified that Standalone to Server migration is not supported (&quot;Preparing to Migrate the Database&quot; on page 20)</td>
</tr>
<tr>
<td></td>
<td>• General updates</td>
</tr>
<tr>
<td>31 March 2016</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Contents

Important Information ................................................................. 3
Terms .............................................................................................................. 7
Getting Started ............................................................................................ 9
  Minimum Disk Space .................................................................................. 9
  Disk Partitions in a Gaia Clean Installation ................................................ 9
  Upgrading to R80 ...................................................................................... 10
  USB Installation ....................................................................................... 10
Configuring R80 Appliances ........................................................................ 11
  Configuring the Management IP Address .................................................. 12
  Running the Gaia First Time Configuration Wizard ..................................... 12
Installing the Gaia Operating System .......................................................... 14
Installing R80 on Gaia Open Servers .......................................................... 15
  Installing Security Management Server on Gaia Open Servers ..................... 15
  Installing Multi-Domain Server on Gaia Open Servers ................................ 16
Installing a Secondary Server for High Availability .................................... 18
Installing Other Servers .............................................................................. 19
  Installing a Log Server for Security Management Server ............................ 19
  Installing a Multi-Domain Log Server ....................................................... 19
  Installing a SmartEvent Server ................................................................ 19
Advanced Upgrade with Database Migration ................................................ 20
  Preparing to Migrate the Database ............................................................ 20
  Overview of Database Migration to R80 .................................................... 21
  Requirements for Database Migration ........................................................ 22
    Upgrade Tools ......................................................................................... 22
    Migrate Command Reference .................................................................. 23
Upgrading Security Management Server with Migration ............................... 23
  Exporting the Current Security Management Server Database .................. 23
  Importing the Security Management Server Database ................................ 24
  Migrating the Database of a Secondary Security Management Server .......... 24
  Migrating Log and Event Databases .......................................................... 25
Upgrading Multi-Domain Security Management with Migration .................... 25
  Exporting the Multi-Domain Server Databases .......................................... 25
  Importing the Database to the Primary Multi-Domain Server ...................... 26
  Importing the Database to Secondary Multi-Domain Servers ...................... 27
Upgrading each Domain Server Separately with Migration ............................ 28
  Migrating Global Policies ......................................................................... 28
  Migrating Domain Server Database .......................................................... 28
Migrating an R80 Database to Another R80 Server ...................................... 30
Migrating a License to a New IP Address (Security Management Server) ........ 31
Restoring on Failure ..................................................................................... 31
Installing SmartConsole Clients ................................................................... 32
  Post-Installation Configuration ................................................................. 32
Loggin in to SmartConsole .......................................................................... 32
Troubleshooting SmartConsole .................................................................... 33
Terms

**Active Domain Server**
The only Domain 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.

**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.

**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.

**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 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.

**Standby Domain Server**

All Domain Servers for a Domain that are not designated as the Active Domain 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.
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 Servers. Configure the disk space on the Multi-Domain Server object.

Disk Partitions in a Gaia Clean Installation

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, enter expert mode and run the `df -h` command.

Most of the remaining space on the disk is reserved for backup images and upgrade. To see the disk space assigned for backup images, connect to the Gaia WebUI and go to the Maintenance > Image Management page. On an Open Server, the available space shown in the Image Management page is less than the space you defined when installing Gaia. The difference between the two amounts is the space reserved for 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.

### Upgrading to R80

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

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.

### USB Installation

You can install a Gaia appliance or open server 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.
Configuring R80 Appliances

In This Section:

- Configuring the Management IP Address ............................................................... 12
- Running the Gaia First Time Configuration Wizard .................................................. 12

You can clean install R80 on Gaia Check Point appliances. If the appliance does not have the R80 image, you can install the R80 ISO file from a USB drive or DVD.

To install R80 on appliances with the R80 image:

1. Open the terminal emulation program.
2. Restart the appliance.
3. When prompted, press any key to enter the boot menu.
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 12].
7. Run the First Time Configuration Wizard ["Running the Gaia First Time Configuration Wizard" on page 12].

To install R80 on appliances from the R80 ISO file:

1. Create the removable installation media:
   - DVD - Burn the R80 ISO on it
   - USB drive - To prepare a USB drive, see: sk65205 http://supportcontent.checkpoint.com/solutions?id=sk65205
2. Connect the USB drive or DVD with the R80 ISO to the appliance.
3. Open the terminal emulation program.
4. Restart the appliance.
5. Redirect the boot sequence to the installation media:
   - DVD - Press Enter within 90 seconds to boot from the DVD
   - USB drive - In the boot screen, at the boot prompt, enter serial and press Enter.
   The R80 file is installed on the appliance.
6. Reboot the appliance, press CTRL + C.
7. Configure the Management IP Address ["Configuring the Management IP Address" on page 12].
8. Run the First Time Configuration Wizard ["Running the Gaia First Time Configuration Wizard" on page 12].
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 19).

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.

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**. 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.
Installing the Gaia Operating System

Install the Gaia operating system on an open server before you install R80. 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 R80 on Gaia Open Servers

In This Section:

Installing Security Management Server on Gaia Open Servers ........................................ 15
Installing Multi-Domain Server on Gaia Open Servers ...................................................... 16

You can install Check Point management products on open servers that run Gaia.

Note - You must install the Gaia operating system ("Installing the Gaia Operating System" on page 14) before you use the First Time Configuration Wizard on an open server.

Installing Security Management 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 12) 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 configuration of Gaia R80. 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. 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.

8. Set the date and time manually, or enter the hostname and IPv4 address of the NTP server. Click Next.


10. Enter the username and password for the Security Management Server administrator account. Click Next.

11. Define IPv4 addresses from which SmartConsole clients can log in to the Security Management Server. Click Next.

12. Get a license automatically from the UserCenter and activate it, or use the trial license.
   If there is a proxy server between the server and the Internet, enter its IP address and port. Click Next.
13. Review the summary and then click Finish.
14. Click Yes when prompted to start the configuration process.
   A progress bar tracks the configuration of each task.
15. Click OK.
16. 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 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 12) 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 configuration of Gaia R80. 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.
   Click Next.
7. 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.
8. Set the date and time manually, or enter the hostname and IPv4 address of the NTP server.
   Click Next.
9. Enter the username and password for the Security Management Server administrator account.
   Click Next.
10. For Installation Type, select Multi-Domain Server. Click Next.
11. For the type of server, select Primary.
12. Select the leading interfaces.
   Leading interfaces are physical interfaces that connect to the external network. These interfaces are for Domain Server virtual IP addresses. Each leading VIP interface can have up to 250 virtual IP addresses (250 Domain Servers).
13. Set the Name and Password for the Multi-Domain Server administrator account. Click Next.
14. Define IPv4 addresses from which SmartConsole clients can log in to the Multi-Domain Server. Click Next.
15. Get a license automatically from the UserCenter and activate it, or use the trial license.
   If there is a proxy server between the server and the Internet, enter its IP address and port.
   Click Next.
16. Review the summary and then click Finish.
17. Click Yes when prompted to start the configuration process.
   A progress bar tracks the configuration of each task.
18. Click OK.
19. 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 Secondary Server for 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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Primary Security Management Server</td>
</tr>
<tr>
<td>2</td>
<td>Direct or indirect connection</td>
</tr>
<tr>
<td>3</td>
<td>Secondary server</td>
</tr>
</tbody>
</table>

Prerequisites for Management High Availability

- The Primary and Secondary servers must be R80 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 SmartConsole.
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 Security Management Guide.
For information about how to configure High Availability for a Multi-Domain Server deployment, see the R80 Multi-Domain Server Administration Guide.
Installing Other Servers

In This Section:

- Installing a Log Server for Security Management Server .......................................... 19
- Installing a Multi-Domain Log Server ......................................................................... 19
- Installing a SmartEvent Server .................................................................................... 19

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

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.

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.

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 SmartConsole.
Advanced Upgrade with Database Migration

In This Section:
- Preparing to Migrate the Database .................................................................20
- Overview of Database Migration to R80 ..........................................................21
- Requirements for Database Migration .............................................................22
- Upgrading Security Management Server with Migration ...............................23
- Upgrading Multi-Domain Security Management with Migration .................25
- Upgrading each Domain Server Separately with Migration .......................28
- Migrating an R80 Database to Another R80 Server ........................................30
- Migrating a License to a New IP Address (Security Management Server) ....31
- Restoring on Failure ........................................................................................31

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 server.

Important Notes:
- R80 is a management-only release and does not support migration from a Standalone deployment (server and gateway on the same machine). Standalone to Standalone migration will be supported in R80.10.
- 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 Database Migration" on page 22)
2. Make sure that you have SmartConsole 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.
Overview of Database Migration to R80

This procedure is an overview that explains how to migrate the database to a R80 Security Management Server with a new IP address.

1. Get the R80 migration tools package ["Upgrade Tools" on page 22].
   It is important that you use the correct migration tools package. Download the latest version of the migration tools from the Support Center http://supportcontent.checkpoint.com/solutions?id=sk108623.
   a) Extract the downloaded package, to the source and the target servers.
      Important - Extract all the files to the same directory and run the tools from that directory.
   b) Make sure the files have executable permissions: chmod 777 *

2. Create a new temporary host object in SmartConsole or SmartDashboard with the IP address of the target.

3. Define a Firewall rule that lets the new R80 server connect to Security Gateways:
   Source: new server
   Destination: target Security Gateways
   Service:
   - FW1 (TCP 256)
   - CPD (TCP 18191)
   - FW1_CPRID (TCP 18208)
   - CPM (TCP 19009)

4. Install the new security policy on all gateways.

5. If the source has IPv6 addresses, on the source operating system, disable IPv6.

6. In SmartConsole or SmartDashboard, delete the temporary host objects from the primary Security Management Server.

7. Close all Check Point GUI clients that are connected to the Security Management Server.

8. If this server is not in production, run: cpstop

9. Export the database with the R80 export tools.
   - Security Management Server ["Exporting the Current Security Management Server Database" on page 23]
   - Multi-Domain Server ["Exporting the Multi-Domain Server Databases" on page 25]

10. Clean install the new R80 Security Management Server or Multi-Domain Server.
    - Install on an appliance ["Configuring R80 Appliances" on page 11].
    - Install on a Gaia open server ["Installing R80 on Gaia Open Servers" on page 15].

11. Configure Gaia OS settings in the Gaia WebUI or CLI.

12. Import the database.
    - Security Management Server ["Importing the Security Management Server Database" on page 24]
    - Multi-Domain Server ["Importing the Database to the Primary Multi-Domain Server" on page 26]
## Requirements for Database 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:
The target must use the same IP address configuration as the source. If the source uses IPv6, you must change it to IPv4 before you can migrate.

### 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.

## 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 Support site [http://supportcontent.checkpoint.com/solutions?id=sk108623](http://supportcontent.checkpoint.com/solutions?id=sk108623).

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

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>migrate.conf</td>
<td>Holds configuration settings for Advanced Upgrade / Database Migration.</td>
</tr>
<tr>
<td>migrate</td>
<td>Runs Advanced Upgrade or migration.</td>
</tr>
<tr>
<td></td>
<td>On Windows, this is <code>migrate.exe</code>.</td>
</tr>
<tr>
<td>pre_upgrade_verifier</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>On Windows this is <code>pre_upgrade_verifier.exe</code></td>
</tr>
<tr>
<td></td>
<td><code>pre_upgrade_verifier -p $FWDIR -c &lt;Current Version&gt; -t &lt;Target Version&gt;</code></td>
</tr>
<tr>
<td>migrate export</td>
<td>Backs up all Check Point configurations, without operating system information.</td>
</tr>
<tr>
<td></td>
<td>On Windows, this is <code>migrate.exe export</code></td>
</tr>
<tr>
<td>migrate import</td>
<td>Restores backed up configuration.</td>
</tr>
</tbody>
</table>
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]
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>export</td>
<td>One of these actions must be used. Make sure services are stopped.</td>
</tr>
<tr>
<td>import</td>
<td></td>
</tr>
<tr>
<td>-l</td>
<td>Optional. Export or import SmartView Tracker logs and SmartLog data. Only closed logs are exported. Use the <code>fw logswitch</code> command to close the logs before you do the export.</td>
</tr>
<tr>
<td>-n</td>
<td>Optional. Run silently (non-interactive) using the default options for each setting.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> 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 <code>cpstop</code> automatically.</td>
</tr>
<tr>
<td>--exclude-uepm-postgres-db</td>
<td>Skip over backup/restore of PostgreSQL database of the Endpoint product.</td>
</tr>
<tr>
<td>--include-uepm-msi-files</td>
<td>Export/import the uepm msi files.</td>
</tr>
<tr>
<td>filename</td>
<td>Required. Enter the name of the archive file with the server database. The path to the archive must exist.</td>
</tr>
</tbody>
</table>

Upgrading Security Management Server with Migration

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

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: `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.

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 Security Management Server.

**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:
   ```bash
   # 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.
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 Log and Event Databases

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

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

Upgrading Multi-Domain Security Management with Migration

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

**Important** - Unlike in previous versions, in R80, the order that you import servers is very 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 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_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
   (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). 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 the 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
   (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 [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.DDMMYY-HHMMSS.tgz`

14. Calculate the MD5 for this file:
    `# md5sum /var/log/exported_mds.DDMMYY-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 Multi-Domain Security Management and the latest R80 Jumbo Hotfix on the target Multi-Domain Server.

**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.DDMMYY-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.DDMMYY-HHMMSS.tgz`
4. Import the configuration: 
   $MDSDIR/scripts/mds_import.sh
   <path_exported_database>/exported_mds.DDMYY-MM-DD_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 Server and Domain Log Server objects on this Multi-Domain Server:

On each Domain 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 Multi-Domain Security Management on the target Multi-Domain Server.

- 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.DDMYY-MM-DD_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.DDMYY-MM-DD_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.DDMYY-MM-DD_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 Server and Domain Log Server objects on this Multi-Domain Server:

1. On each Domain Server and Domain Log Server that you import, run:
   
   ```bash
   $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.

Upgrading each Domain Server Separately with Migration

You can upgrade the Multi-Domain Security Management in stages with each Domain Server upgraded at a time. To complete the gradual upgrade process, first migrate the Global Policy (“Migrating Global Policies” on page 28) and then migrate each Domain Server separately (see “Migrating Domain Server Database” on page 28).

Migrating Global Policies

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

**Note** - When executing the `migrate_global_policies` utility, the Multi-Domain Server and the Domain 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 Multi-Domain Server.

To upgrade Global Policies from R77.xx to R80:

1. On the R77.xx Multi-Domain Server, extract the Upgrade Tools from the R80 CD or ISO (“Upgrade Tools” on page 22), if you did not do this already (“Migrating Domain Server Database” on page 28).
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 Multi-Domain Server.
5. Run: `# migrate_global_policies full_path_exported_tgz`
6. Run: `# mdsstart`

Migrating Domain Server Database

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

**Before you begin:**

- Make sure that there is one Active Domain 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 Server. If you migrate a database to more than one Domain Server, the import fails and shows an error message.

To import from R77.xx Domain Server to R80:

1. On the R77.xx Domain Server, get the Upgrade Tools from the R80 CD or ISO (“Upgrade Tools” on page 22).

2. Extract the tools.
   Extraction makes the upgrade_tools subdirectory. In this path, extract the Multi-Domain Security Management tools: pl_upgrade_tools.tgz
   For example:
   Install from CD:
   `# gtar xvfz /mnt/cdrom/linux/upgrade_tools/linux/pl_upgrade_tools.tgz -C /var/opt/export_tools`
   Install from DVD:
   `# gtar xvfz /mnt/cdrom/Linux/linux/upgrade_tools/linux/pl_upgrade_tools.tgz -C /var/opt/export_tools`

3. Run: `# mdsenv <domainServer_name>`

4. Before you export the database, make sure that you remove the Global Policy from the source Domain Server.

5. Run: `# <full path to migrate command> migrate export [-l] <output file>`
   • The migrate export command exports one Domain 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 Server in the output archive.

6. On the R80 Multi-Domain Server, run these API commands https://sc1.checkpoint.com/documents/R80/APIs/#introduction to create a new Domain and a new Domain 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_multi-domain-server_Name> servers.skip-start-domain-server true`

7. Copy the TGZ file from the R77.xx Domain Server to the R80 Multi-Domain Server.

8. Import the exported database:
   `# cma_migrate <source management tgz file> <target Domain Server fwdir directory>`
   For example:
   `# cma_migrate tmp/orig_mgmt.tgz /opt/CPmds-R80/customer/cma1/CPsuite-R80/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 Server according to instructions in the error messages. Then do this procedure again.

9. If the R80 server has a different IP address than the R77.xx server, establish trust with the Security Gateways (“Certificate Authority Data” on page 30).
10. If the R77.xx server had VPN gateways, configure the keys ("Resolving Issues with IKE Certificates" on page 30).

11. Restart the R80 Domain Server:  
   # mdsstop and then mdsstart

**Certificate Authority Data**

The `cma_migrate` process does not change the Certificate Authority or key data. The R80 Domain Server has SIC with Security Gateways. If the IP address of the R80 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 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 Server.
- Revoke the IKE certificate for the gateway and create a new one.

**Migrating an R80 Database to Another R80 Server**

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

1. Create a backup file of the current system settings from the Gaia WebUI.
   For Multi-Domain Server run `mds_backup`

2. Perform the steps to migrate to another R80 Security Management Server or Multi-Domain Server ("Overview of Database Migration to R80" on page 21).
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.

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 20).

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.
   - Security Management Server ("Importing the Security Management Server Database" on page 24)
   - Multi-Domain Server ("Importing the Database to the Primary Multi-Domain Server" on page 26)
Installing SmartConsole Clients

In This Section:
- Post-Installation Configuration ................................................................................... 32
- Logging in to SmartConsole ......................................................................................... 32
- Troubleshooting SmartConsole ................................................................................... 33

The SmartConsole and other SmartConsole applications are the GUI clients 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 distribution media or download the SmartConsole application from the Support Center [http://supportcontent.checkpoint.com/solutions?id=sk108623](http://supportcontent.checkpoint.com/solutions?id=sk108623).
2. Run the SmartConsole executable.
3. Continue with the instructions on the screen.

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 making connections between the Security Management Server and Gateways. For Windows, you must define the name of the ICA host. You can use the default name or define your own. The ICA name must be in the host name.domain format, for example, ica.checkpoint.com.
- **Fingerprint**: Save the certificate fingerprint when you log in to SmartConsole clients for the first time.

Logging in 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
Licensing

In This Section:

Software Licensing ............................................................................................................... 34
Licensing Multi-Domain Security Management .................................................................. 35

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

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

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

Software Licensing

If you have not migrated to Software Blade licenses, use the migration options from the Check Point website http://www.checkpoint.com/downloads/product-related/brochure/Software-Blades-Architecture.pdf. Migration to Software Blades is free of charge to purchasers of the Software Subscription service [Enterprise Base Support].


If the license is for an appliance that is connected to the Internet, the license is activated automatically. Use the procedure below for open servers or offline servers.

To get a license from the Check Point User Center:

1. Add the required Check Point products and evaluations to your User Center account: click Accounts & Products > Add Products.
   If you cannot add the product you want, contact your Check Point partner or Account Services accountservices@checkpoint.com - mailto:accountservices@checkpoint.com?subject=Licensing Issues, to make sure the correct certificate keys are assigned to your account.

2. Generate a license key: click Accounts & Products > Products.

3. Select your products.
   The selected product evaluations are assigned license keys.

4. Read and accept the End Users License Agreement.

5. Import the license with cpconfig.
   The certificate keys associate the product license with the Security Management Server:
   - The new license remains valid, even if the IP address of the Security Gateway changes.
   - Only one IP address is needed for all licenses.
   - A license can be detached from one Security Gateway and assigned to another.
Licensing Multi-Domain Security Management

If you cannot activate the license automatically (the Multi-Domain Server is on an open server or is offline), install the license with this procedure.

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

To add licenses from the SmartConsole:

1. Open General > Multi-Domain Server Contents.
2. Double-click a Multi-Domain Server or Multi-Domain Log Server.
   The Multi-Domain Server Configuration window opens.
3. Open the License tab.
4. Install licenses using Fetch or Add:
   Fetch - Click Fetch From File. In the window that opens, browse to and double-click the license file.
   Add:
   a) Click Add.
   b) In the email message that you received from Check Point, copy the entire license string (starting with cplic putlic... and ending with the last SKU/Feature).
   c) In the Add License window, click Paste License.
   d) Click Calculate.
   e) Compare the Validation Code with the code that you received in your email. If validation fails, contact the Check Point licensing center, with the validation codes from the email and from this window.