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 R77.30
For more about this release, see the R77.30 home page http://supportcontent.checkpoint.com/solutions?id=sk104859.

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=40107.

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 R77.30 Release Notes.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>05 July 2017</td>
<td>Updated instructions in Getting Software Packages Offline (on page 14)</td>
</tr>
<tr>
<td>27 December 2016</td>
<td>New image to unify appliance and open server images (&quot;Important Notes&quot; on page 6)</td>
</tr>
<tr>
<td>16 December 2016</td>
<td>New image for appliances</td>
</tr>
<tr>
<td>14 April 2016</td>
<td>Changed link to sk92449 in Updating the CPUSE Deployment Agent (on page 12)</td>
</tr>
<tr>
<td>09 February 2016</td>
<td>Corrected Supported Upgrade Paths (on page 8)</td>
</tr>
<tr>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>01 February 2016</td>
<td>New instructions for CPUSE CLI are added throughout the document. This CLI is supported with CPUSE Deployment Agent 802 and higher.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Legacy CLI instructions are now in a different document. See the R77.30 Legacy CLI Appendix</td>
</tr>
<tr>
<td></td>
<td>New link to the Connectivity Upgrade Best Practices Guide (“Before You Install or Upgrade! “ on page 10).</td>
</tr>
<tr>
<td></td>
<td>Updated Required Disk Space (on page 11).</td>
</tr>
<tr>
<td></td>
<td>Updated Supported Upgrade Paths (on page 8) for R77.10</td>
</tr>
<tr>
<td>20 October 2015</td>
<td>Clarified references to installation instructions for different paths (“Supported Upgrade Paths” on page 8).</td>
</tr>
<tr>
<td></td>
<td>Added supported platforms (“Newly Supported Platforms” on page 9).</td>
</tr>
<tr>
<td>27 May 2015</td>
<td>Updated What’s New (on page 6).</td>
</tr>
<tr>
<td>19 May 2015</td>
<td>First release of this document.</td>
</tr>
</tbody>
</table>
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>Important Notes</td>
<td>6</td>
</tr>
<tr>
<td>What’s New</td>
<td>6</td>
</tr>
<tr>
<td>Supported Upgrade Paths</td>
<td>8</td>
</tr>
<tr>
<td>Compatibility with Gateways</td>
<td>8</td>
</tr>
<tr>
<td>Compatibility with Security Management Servers</td>
<td>9</td>
</tr>
<tr>
<td>Newly Supported Platforms</td>
<td>9</td>
</tr>
<tr>
<td>Compatibility with Clients</td>
<td>10</td>
</tr>
<tr>
<td>Build Numbers</td>
<td>10</td>
</tr>
<tr>
<td>Installation and Upgrade</td>
<td>10</td>
</tr>
<tr>
<td>Before You Install or Upgrade!</td>
<td>10</td>
</tr>
<tr>
<td>Required Disk Space</td>
<td>11</td>
</tr>
<tr>
<td>Using CPUSE</td>
<td>12</td>
</tr>
<tr>
<td>Updating the CPUSE Deployment Agent</td>
<td>12</td>
</tr>
<tr>
<td>Getting New Software Packages</td>
<td>13</td>
</tr>
<tr>
<td>Getting Software Packages Online</td>
<td>13</td>
</tr>
<tr>
<td>Getting Software Packages Offline</td>
<td>14</td>
</tr>
<tr>
<td>Clean Installing</td>
<td>14</td>
</tr>
<tr>
<td>Upgrading</td>
<td>15</td>
</tr>
<tr>
<td>Installing the SmartConsole</td>
<td>15</td>
</tr>
<tr>
<td>Installing the R77.30 Add-on</td>
<td>16</td>
</tr>
<tr>
<td>Uninstalling R77.30</td>
<td>17</td>
</tr>
<tr>
<td>Uninstalling the R77.30 Add-on</td>
<td>18</td>
</tr>
</tbody>
</table>
Introduction

This version installs important Check Point product and Gaia Operating System updates on computers and appliances running R77.30 Multi-Domain Server, Security Management Server, or Security Gateways.

Please read this document before installing. This document has general data and requirements, installation, and upgrade instructions for Gaia only. To install or upgrade on other platforms, see the Appendix to R77.30 Release Notes http://supportcontent.checkpoint.com/documentation_download?ID=40108.


Important Notes

Effective 27 December 2016, the R77.30 image for Open Server / Smart-1 / UTM-1 / Power-1 / IP appliances / Clean Install was unified with the 2200 / 4000 /12000 / 21000 / Threat Emulation image to extend SHA-256 based certificates for all blades and features.

For more about Check Point appliances and earlier images, see sk114513 http://supportcontent.checkpoint.com/solutions?id=sk114513.

What's New

New Software Blade: Threat Extraction

Threat Extraction is a new Software Blade in the Threat Prevention family that pro-actively cleans potential threats from incoming documents. [Requires the R77.30 Add-on]

To learn more about the R77.30 Add-on, see sk105412 http://supportcontent.checkpoint.com/solutions?id=sk105412.

Software Blade Enhancements:

• IPS Software Blade: New protection to detect DNS Tunneling.
• Application Control Software Blade: Detailed monitoring and enforcement of Modbus traffic. [Requires the R77.30 Add-on]

General enhancements and stability improvements:

• VSX enhancement: Multi Bridge - support for multiple bridge interfaces on a Virtual System in Bridge Mode.

• CoreXL Dynamic Dispatcher - improved administrative access on overloaded gateways through prioritization of traffic on highly utilized CPUs and improved utilization through load distribution of traffic among CPUs. See sk105261 http://supportcontent.checkpoint.com/solutions?id=sk105261.

• Priority Queues - improved handling of different types of traffic by the Firewall to mitigate connectivity issues during high CPU utilization by applying traffic prioritization on Security Gateways. See sk105762 http://supportcontent.checkpoint.com/solutions?id=sk105762.

• Support to manage 1100/1200R Appliances running R77.20. **(Requires the R77.30 Add-on)**

• Updated support for e1000e and bnx2 network device drivers.

• Clustering and routing stability fixes (see Resolved Issues), including more flexible configuration for multiple clusters on the same network http://supportcontent.checkpoint.com/solutions?id=sk25977.

• Routing enhancements: OSPF Graceful Restart, Static Multicast Routes, PBR based on protocol and destination port, and routing support in cadmin.


• Support for Carrier solutions (LTE suite): NAT64, GTP, SCTP, CGNAT and more. **(Requires the R77.30 Add-on)**

• Support Single Sign On to SaaS Application through the use of the SAML protocol. See sk98811 http://supportcontent.checkpoint.com/solutions?id=sk98811. **(If the R77.20 Add-on is not installed, install the R77.30 Add-on)**


• Support for **Hyper-V** (Virtualization technology on Windows Server).

• Quick Setup for Check Point appliances, configured as Standalone (Security Management Server and Security Gateway) with pre-defined security policy, in monitor or bridge mode. See sk102231 http://supportcontent.checkpoint.com/solutions?id=sk102231.
Supported Upgrade Paths

You can install this release on supported appliances and open servers as a new installation. See the R77 Release Notes for platform details. You can upgrade to R77.30 from:

<table>
<thead>
<tr>
<th>Version</th>
<th>Upgrade Path</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>R77, R77.10, R77.20</td>
<td>Install the appropriate upgrade package. <strong>Note</strong> - Upgrade from non-Gaia to Gaia R77.30 is not supported.</td>
<td>Use the instructions in this document (“Installation and Upgrade” on page 10)</td>
</tr>
<tr>
<td>R75.40, R75.45, R75.46, R75.47, R75.40VS, R76</td>
<td>Install the appropriate upgrade package. <strong>Note</strong> - You can use the upgrade package to migrate from SecurePlatform or IPSO to Gaia.</td>
<td>R77 Installation and Upgrade Guide <a href="http://supportcontent.checkpoint.com/documentation_download?ID=24831">http://supportcontent.checkpoint.com/documentation_download?ID=24831</a></td>
</tr>
<tr>
<td>R75, R75.10, R75.20, R75.30</td>
<td>Upgrade first to R77.</td>
<td>R77 Installation and Upgrade Guide <a href="http://supportcontent.checkpoint.com/documentation_download?ID=24831">http://supportcontent.checkpoint.com/documentation_download?ID=24831</a></td>
</tr>
<tr>
<td>R70.40, R70.50, R71.50</td>
<td>Advanced Upgrade.</td>
<td>“Advanced Upgrade and Database Migration” chapter in R77 Installation and Upgrade Guide <a href="http://supportcontent.checkpoint.com/documentation_download?ID=24831">http://supportcontent.checkpoint.com/documentation_download?ID=24831</a></td>
</tr>
<tr>
<td>R71 - R71.45</td>
<td>Upgrade first to R71.50.</td>
<td></td>
</tr>
<tr>
<td>R70 - R70.30</td>
<td>Upgrade first to R70.50.</td>
<td></td>
</tr>
</tbody>
</table>

Compatibility with Gateways

If you choose to install an R77.30 Security Management Server, you can manage gateways of these versions:

<table>
<thead>
<tr>
<th>Release</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Gateway</td>
<td>NGX R65, R70, R70.1, R70.20, R70.30, R70.40, R70.50, R71, R71.10, R71.20, R71.30, R71.40, R71.50, R75, R75.10, R75.20, R75.30, R75.40, R75.45, R75.46, R75.40VS, R75.46, R75.47, R76, R77, R77.10, R77.20, R77.30</td>
</tr>
<tr>
<td>Security Gateway 80</td>
<td>R71.45, R75.20.x</td>
</tr>
<tr>
<td>1100 Appliance</td>
<td>R75.20.x, R77.20.x [Requires the R77.30 Add-on]</td>
</tr>
</tbody>
</table>
### Supported Upgrade Paths

<table>
<thead>
<tr>
<th>Release</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1200R Appliance</td>
<td>R77.20.x (Requires the R77.30 Add-on)</td>
</tr>
<tr>
<td>13800 &amp; 21800 Appliances</td>
<td>R77.20, R77.30</td>
</tr>
<tr>
<td>UTM-1 Edge</td>
<td>7.5.x and higher</td>
</tr>
<tr>
<td>61000/41000 Security System</td>
<td>61000 R75.035, 61000 R75.05x R75.40VS for 61000, R76SP, R76SP.10</td>
</tr>
<tr>
<td>VSX</td>
<td>VSX R67 and higher</td>
</tr>
<tr>
<td>Other gateways</td>
<td>DLP-1: R71 and higher, IPS-1: R71, Connectra Centrally Managed: NGX R66, GX 4.0, 5.0</td>
</tr>
</tbody>
</table>

### Compatibility with Security Management Servers

If you choose to install an R77.30 Security Gateway only, you can manage the new gateways with these versions of the Security Management Server or Multi-Domain Server:

<table>
<thead>
<tr>
<th>Version</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>R77, R77.10, R77.20</td>
<td>Some Resolved Issues on the Server may not be applied to the new R77.30 Security Gateways.</td>
</tr>
<tr>
<td>R76</td>
<td>Install the Hotfix and SmartConsole as instructed in sk97626 <a href="http://supportcontent.checkpoint.com/solutions?id=sk97626">http://supportcontent.checkpoint.com/solutions?id=sk97626</a>.</td>
</tr>
</tbody>
</table>

### Newly Supported Platforms

These platforms and components were added in R77.20 or R77.10. ESX 6.0 was added in this release.

<table>
<thead>
<tr>
<th>Platform/Version</th>
<th>Related Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 8.1, 32-bit and 64-bit</td>
<td>SmartConsole, Mobile Access client features, Identity Awareness agent, UserCheck agent</td>
</tr>
<tr>
<td>Windows Server 2012 and 2012 R2</td>
<td>Security Management Server, SmartConsole, Active Directory for AD Query, Identity Agent for Terminal Servers</td>
</tr>
<tr>
<td>Windows 7 SP1</td>
<td>All installations and upgrades supported for Windows 7 SP1</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5.9</td>
<td>All installations supported for Linux</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 6.5</td>
<td>All installations supported for Linux</td>
</tr>
<tr>
<td>Internet Explorer 11</td>
<td>Mobile Access client features</td>
</tr>
<tr>
<td>ESX 6.0, ESX 5.5, ESX 5.1</td>
<td>Security Gateway Virtual Edition Network Mode</td>
</tr>
</tbody>
</table>
Compatibility with Clients

R77.30 Servers with the Endpoint Policy Management blade enabled can manage these Endpoint Security clients: E80.51, E80.50, E80.4x.

R77.30 Servers and Gateways support these Remote Access Clients: E80.6x, E80.5x, E80.4x, E75.x. See sk67820 http://supportcontent.checkpoint.com/solutions?id=sk67820, VPN Client Version and Supported Gateway Version section.

Build Numbers

This table contains the R77.30 software products updated in this release and their build numbers. To confirm installation, run the version command for each product.

<table>
<thead>
<tr>
<th>Product</th>
<th>Build No.</th>
<th>Version Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Gateway</td>
<td>Build 990180503</td>
<td>fw ver -k</td>
</tr>
<tr>
<td>Security Management Server</td>
<td>Build 990180035</td>
<td>fwm ver</td>
</tr>
<tr>
<td>Multi-Domain Security Management</td>
<td>Build 990180317</td>
<td>fwm mds ver</td>
</tr>
<tr>
<td>SmartConsole Applications</td>
<td>Build 990180413</td>
<td>Help &gt; About Check Point &lt;Application Name&gt;</td>
</tr>
</tbody>
</table>

Installation and Upgrade

To install or upgrade Check Point products running the Gaia OS, we recommend using CPUSE (on page 12) through its WebUI or CLI modes.

The legacy CLI install and upgrade procedures are also supported. See the R77.30 Legacy CLI Appendix http://supportcontent.checkpoint.com/documentation_download?ID=46611.

For platforms other than Gaia, see the Appendix http://supportcontent.checkpoint.com/documentation_download?ID=40108.

To install or upgrade VSX, follow the instructions in sk97552 http://supportcontent.checkpoint.com/solutions?id=sk97552.

Before You Install or Upgrade!

- Save a snapshot to back up your system before you install this release.
Full Connectivity Upgrade is not supported.

- If you upgrade from R77 or later with a Mobile Access-enabled gateway in the environment, use the important pre-upgrade instructions in sk98213 http://supportcontent.checkpoint.com/solutions?id=sk98213.
- To install or to upgrade from R77.10 and earlier versions to R77.30 on a 21700, 21600, or 13500 appliance, you must update the LOM firmware. See sk98788 http://supportcontent.checkpoint.com/solutions?id=sk98788.

Required Disk Space

In R77.30, free disk space is verified before installation. Make sure you have the minimum free space required per partition.

**Note:** CPUSE upgrade has the lowest requirements and is recommended when possible.

**To see the disk space required for a package with CPUSE WebUI:**

1. In the Gaia WebUI, click **CPUSE > Status and Actions.**
2. Click on a package.
   - The details of the package show, including the **Package Size.** This is the amount of free disk space required to install the package.

**To see the disk space required for a package with CPUSE CLI:**

1. Show all available packages with their package numbers [Num]:
   
   ```
   show installer package <TAB>
   ```
2. Show the size of a package:
   
   ```
   show installer package <package_number> size
   ```

This table shows the disk space required for some packages.

<table>
<thead>
<tr>
<th>Current Version / Upgrade Tool</th>
<th>Management Server or Standalone</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>R77.30 Clean install - CPUSE</td>
<td>Disk space that is at least the size of the existing root partition</td>
<td>Disk space that is at least the size of the existing root partition</td>
</tr>
</tbody>
</table>

If you do not have enough disk space, you can use the LVM Manager to configure partition disk space on Gaia. See sk95566 http://supportcontent.checkpoint.com/solutions?id=sk95566.
Required Disk Space for Multi-Domain Security Management:
Before you run a clean install of R77.30 on Multi-Domain Servers, make sure that at least 10GB of free disk space in the root partition is available. For an environment with many Domain Management Servers, more than 10GB of free disk space is often required.

Using CPUSE
To upgrade or clean install a supported Gaia server or gateway, we recommend CPUSE (Check Point Upgrade Service Engine, previously known as Gaia Software Updates).
CPUSE supports pre-downloaded packages, so no online connection is needed.
If you have an internet connection, CPUSE connects your appliance or open server to the Check Point Cloud. From the Gaia portal, make sure the appliance or open server can reach Check Point Cloud:
• Allow outgoing traffic over web ports 80 and 443.
• If your environment uses a proxy, configure it and allow this traffic to go through.
CPUSE has two modes:
• WebUI
• CLI - Supported with CPUSE Deployment Agent 802 and higher
To learn more about CPUSE (including limitations), see sk92449 http://supportcontent.checkpoint.com/solutions?id=sk92449.

Updating the CPUSE Deployment Agent
CPUSE uses the Deployment Agent on your Gaia servers and gateways to find, download, and install available updates. Make sure you have the latest build of the Deployment Agent. See sk92449 http://supportcontent.checkpoint.com/solutions?id=sk92449.

To update the Deployment Agent from build 710 or higher with WebUI:
If the WebUI shows New Deployment Agent Available, click Update Now.

To update the Deployment Agent from build 627 or lower with WebUI:
1. In the WebUI, open CPUSE > Status and Actions and select:
   GaiaSoftwareUpdatesAgent_<latest build>.tgz
   Note – If you are upgrading from R75.40 and this package does not show, see sk92449 http://supportcontent.checkpoint.com/solutions?id=sk92449.
2. Click Download.
   The package is downloaded from the Check Point Support Center.
3. Click Install.
To update the Deployment Agent with CLI:

1. To check the current version of the Deployment Agent, run:
   
   `[Expert@HostName]# cpvinfo $DADIR/bin/DAService | grep -E "Build|Minor"`

2. Transfer the updated Deployment Agent package `DeploymentAgent_<build>.tgz` to the Gaia machine into `/<path_to_updated_DA>/` directory.

3. Unpack the Deployment Agent package:
   
   `[Expert@HostName]# cd /<path_to_updated_DA>/
   [Expert@HostName]# tar -zxvf DeploymentAgent_<build>.tgz`

4. Install the Deployment Agent RPM. The older installed agent will be automatically stopped during the RPM installation. Run:
   
   `[Expert@HostName]# rpm -Uhv --force CPda-00-00.i386.rpm`

5. Start the Deployment Agent:
   
   `[Expert@HostName]# $DADIR/bin/dastart`

Getting New Software Packages

**Online packages** - If your server or gateway is connected to the internet, CPUSE connects your appliance or open server to the Check Point Cloud to download packages.

**Offline packages** - If you are not connected to the internet, import packages from your local computer, the Check Point Cloud, FTP server, or a local path on the gateway or server.

Getting Software Packages Online

**To download new packages with WebUI while connected to the internet:**

1. Log in to the Gaia WebUI, and from the navigation tree click `CPUSE > Status and Actions`.
2. Select a R77.30 package.
3. Click **Download**.
   
   The Deployment Agent downloads the package from the Check Point Cloud.

**To download new packages with CLI while connected to the internet:**

1. Log into the CPUSE CLI.
2. See all packages available for download. Run:
   
   `installer download` and press the TAB key.
   
   The installer returns the names of available packages.
3. Download a package. Run:
   
   `installer download {<Package_Number> | <Package_Name>} [pause | resume | not-interactive]`
   
   Make sure to include the package filename `<Package_Name>` or package number `<Package_Number>`.

The `installer` command runs in interactive mode by default.

- To run it in non-interactive mode, run with the `not-interactive` option.
- To pause a package download, run with the `pause` option.
- To continue a paused download, run with the `resume` option.
Getting Software Packages Offline

Get the relevant packages from the *R77.30 CPUSE Offline Packages* section of the R77.30 homepage [http://supportcontent.checkpoint.com/solutions?id=sk104859](http://supportcontent.checkpoint.com/solutions?id=sk104859).

To import new packages with WebUI when not connected to the internet:
1. Put the packages in a drive on the Windows computer from which you log in to the Gaia WebUI.
2. Log in to the Gaia WebUI.
3. From the navigation tree click **CPUSE > Status and Actions**.
4. From the toolbar, click **Import Package**.
5. Browse to the location of the package and click **Import**
6. Click **OK**.
   The Deployment Agent imports the package.

To import new packages with CLI when not connected to the internet:
1. Put the packages in the location from which you will import them. CPUSE CLI can import packages from:
   - FTP server.
   - Local path on the gateway or server.
2. Log into the CPUSE CLI.
3. Import a package. Run:
   ```bash
   installer import {ftp <IPv4_Address> path <Path> username <Username> [password <Password>] | local <Full_Path>} [not-interactive]
   ```
   The Deployment Agent imports the package.

Clean Installing

To clean install R77.30 with CPUSE WebUI:
1. Log in to the Gaia WebUI on the appliance or server that is installed with the Gaia operating system.
2. From the navigation tree click **CPUSE > Status and Actions**.
3. Under **Major Versions**, right-click on a downloaded package and select **Clean Install**.

To clean install R77.30 with CPUSE CLI:
1. Log into the CPUSE CLI on the appliance or server that is installed with the Gaia operating system.
2. Install the package. Run:
   ```bash
   installer install {<Package_Number> | <Package_Name>} [not-interactive]
   ```
Upgrading

To upgrade to R77.30 using CPUSE WebUI:
1. Log in to the Gaia WebUI, and from the navigation tree click CPUSE > Status and Actions.
2. **From R76 or lower**: Under Major Versions, right-click on a downloaded R77.30 package and select Upgrade.
3. **From R77 or higher**: Under Minor Versions, right-click on a downloaded R77.30 package and select Install.
   Installation starts immediately. It reboots the device automatically.
   From R77 versions, after the device is rebooted, the installation is complete.
   From lower versions, the installation process continues after the reboot.

To upgrade to R77.30 using CPUSE CLI:
1. Log into the CPUSE CLI.
2. **From R76 or lower**, run:
   installer upgrade {{Package_Number} | {Package_Name}} [not-interactive]
3. **From R77 or higher**, run:
   installer install {{Package_Number} | {Package_Name}} [not-interactive]
   Installation starts immediately. It reboots the device automatically.
   From R77 versions, after the device is rebooted, the installation is complete.
   From lower versions, the installation process continues after the reboot.

Installing the SmartConsole

When a new SmartConsole is available, a message shows in the WebUI Overview. Click Download now to install it. Alternatively, follow one of the procedures below.

To install the R77.30 SmartConsole with CPUSE WebUI:
1. In the WebUI, open CPUSE > Status and Actions.
2. Under Minor Versions (HFAs), select the package.
3. Right-click the package and select Install.
4. A window opens in Windows. Click Yes to run the SmartConsole.

To install the R77.30 SmartConsole with CPUSE CLI:
1. From the CPUSE CLI, run:
   installer install {{Package_Number} | {Package_Name}} [not-interactive]
   Click Yes to run the SmartConsole.
Installing the R77.30 Add-on

⚠️ Important - The R77.30 Add-on can only be installed on R77.30 management servers.

If you install the R77.30 Add-on, you must install it on every Security Management Server, Multi-Domain Server, and Log Server.

Check Point recommends that you install the R77.30 Add-on only if you require the feature it enables, or if Technical Support suggests that you do so.

<table>
<thead>
<tr>
<th>Upgrade From</th>
<th>To</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>R77.20</td>
<td>R77.30</td>
<td>R77.30 without features that require the Add-ons</td>
</tr>
<tr>
<td>R77.20 + Add-on</td>
<td>R77.30</td>
<td>R77.30 with Add-on features of R77.20</td>
</tr>
<tr>
<td>R77.20</td>
<td>R77.30 + Add-on</td>
<td>R77.30 with Add-on features of R77.20 and R77.30</td>
</tr>
<tr>
<td>R77.20 + Add-on</td>
<td>R77.30 + Add-on</td>
<td>R77.30 with Add-on features of R77.20 and R77.30</td>
</tr>
</tbody>
</table>

To install on Multi-Domain Security Management environments:
1. On the Multi-Domain Server, run `mdsstart` after you upgrade to R77.30 and before you install the Add-on.
2. Optional: Install the R77.30 Add-on on the Multi-Domain Server and Multi-Domain Log Server, with CPUSE.
3. Login to the SmartDomain Manager.
4. In Versions & Blades Updates, right-click a relevant Domain Management Server and select Activate.
5. Select R77.20 Add-on and R77.30 Add-on.
6. Repeat to activate both Add-ons for each relevant Domain Management Server.
   Check Point recommends that you activate both the R77.20 Add-on and the R77.30 Add-on on Domain Management Servers.

To import the database from R77.20 + R77.20 Add-on to R77.30:
Install R77.30 and the R77.30 Add-on on the target server before you import the database.
See the “Advanced Upgrade and Database Migration” chapter in the R77 Installation and Upgrade Guide.
Uninstalling R77.30

You can uninstall only if R77.30 was an upgrade from R77, R77.10, or R77.20.

If you clean installed or upgraded from R76 or lower versions, you can revert to a Gaia snapshot. For more about how to restore a backup and revert to an earlier version, see the R77 Gaia Administration Guide.

Important:

- If you installed with legacy CLI, you must uninstall with legacy CLI. See the R77.30 Legacy CLI Appendix
- If you installed R77.30 with CPUSE, you must uninstall it with CPUSE.
- If you installed the R77.30 Add-on, you must uninstall it first (see the next section).
- In Multi-Domain Security Management environments, you must deactivate the R77.30 Add-on before you uninstall it (see the next section).

To uninstall R77.30 with CPUSE WebUI:

1. Log in to the Gaia WebUI, and from the navigation tree click CPUSE > Status and Actions.
2. Right-click on the R77.30 package and select Uninstall.

To uninstall R77.30 with CPUSE CLI:

In the CPUSE CLI, run:

```bash
installer uninstall {<Package_Number> | <Package_Name>} [not-interactive]
```

To uninstall R77.30 in Multi-Domain Security Management environments:

1. Log in to SmartDomain Manager.
   - If you installed the R77.30 Add-on, uninstall it first (see the next section).
2. Run this command on each Multi-Domain Server and Multi-Domain Log Server:
   ```bash
   /opt/CPUninstall/R77.30/UnixUninstallScript
   ```
3. When prompted, reboot.

Note: After you uninstall, the Login prompt and the WebUI Welcome screen still show "Check Point Gaia R77.30".
Uninstalling the R77.30 Add-on

⚠️ **Important:** If you installed the R77.30 Add-on with CPUSE, you must uninstall it with CPUSE.

During uninstallation, objects and services added by the Add-on are removed. Before you uninstall the Add-on, delete rules and groups that use the Add-on objects and services (or remove these objects and services from the rules and groups).

If you do not remove the Add-on objects and services, and try to uninstall the R77.30 Add-on, uninstallation fails. You can see the list of the remaining Add-on objects to remove in this log: /opt/CPshrd-R77/log/PIscrub-preuninstall.elg

To uninstall the R77.30 Add-on with CPUSE WebUI:
1. Remove all Add-on objects.
2. In CPUSE, select the R77.30 Security Management Server.
3. Right-click on the **Check Point R77.30 Add-on** package and select **Uninstall**.

To uninstall the R77.30 Add-on with CPUSE CLI:
In the CPUSE CLI, run:

```
installer uninstall {<Package_Number> | <Package_Name>} [not-interactive]
```