Important Information

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

Latest Documentation
The latest version of this document is at: (http://supportcontent.checkpoint.com/documentation_download?ID=25460)
To learn more, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the R75.47 home page (http://supportcontent.checkpoint.com/solutions?id=sk93448).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>05 January 2014</td>
<td>13500 OS support clarification - Gaia only (&quot;Check Point Appliances&quot; on page 6).</td>
</tr>
<tr>
<td>20 November 2013</td>
<td>Updated Endpoint VPN Clients reference in Compatibility with Gateways and Clients (on page 7).</td>
</tr>
<tr>
<td>24 September 2013</td>
<td>R75.47 is not a visible option when you define a gateway (&quot;Maintaining Server Version&quot; on page 7)</td>
</tr>
<tr>
<td></td>
<td>New Windows image file for safe uninstall (&quot;Uninstalling from Windows&quot; on page 16)</td>
</tr>
<tr>
<td>12 September 2013</td>
<td>Upgrading (on page 12) mentions Full Connectivity Upgrade and a new default backup location for appliances</td>
</tr>
<tr>
<td></td>
<td>Added Compatibility with Gateways and Clients (on page 7)</td>
</tr>
<tr>
<td></td>
<td>Uninstalling (on page 16) updated for limitation on Windows</td>
</tr>
<tr>
<td>18 August 2013</td>
<td>Added to What's New (&quot;What's New &quot; on page 5)</td>
</tr>
<tr>
<td>13 August 2013</td>
<td>New R75.47 images (&quot;Build Numbers&quot; on page 9)</td>
</tr>
<tr>
<td>31 July 2013</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on R75.47  Release Notes).
Introduction

This version installs important Check Point product and Gaia Operating System updates on computers that were upgraded to R75.47 Multi-Domain Server, Security Management Server, or Security Gateways.

Please read this document before installing.

This release can be clean-installed on supported platforms, or it can be used to upgrade a R75.40, R75.45, or R75.46 installation (on supported upgrade platforms).

Review the Known Limitations (http://supportcontent.checkpoint.com/solutions?id=93449) before you begin installation.

Notes:
- Security Gateways installed with this release can be managed by Security Management Servers of version R75.40 and higher.
- This is a hotfix for R75.40, R75.45, R75.46. R75.47 does not support installation over R75.40VS or R76.
  For the differences between R75.40 and R75.40VS, see sk82460 (http://supportcontent.checkpoint.com/solutions?id=sk82460).
- E80.40 management server cannot manage R75.47 Security Gateways.

What's New

R75.47 release contains:
- Support for the new 13500 appliance.
- Management of 1100 Appliances (version R75.20 HFA20 and higher), with new SmartDashboard and Smart Provisioning features.
- Upload troubleshooting data (cpinfo) directly to Check Point with CLI or SmartUpdate. See sk92739 (http://supportcontent.checkpoint.com/solutions?id=sk92739).
System Requirements

Supported Operating Systems

This release can be installed on platforms that are supported by R75.40, with these operating systems:

- Gaia
- SecurePlatform
- Linux (upgrade only)
- IPSO 6.2 (MR4a)
- Windows (upgrade only, see R75.40 Release Notes for details on supported versions and editions)
- Solaris (upgrade only)

Check Point Appliances

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2200 Appliance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4000 Appliances</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12000 Appliances</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13500 Appliance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21000 Appliances</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Appliances *</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart-1 5</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart-1 25</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart-1 50</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart-1 150</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Power-1</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UTM-1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

* IP Appliances (IP150, IP280, IP290, IP390, IP560, IP690, IP1280, IP2450) can run R75.47 with IPSO 6.2 (MR4 and earlier MRs) or Gaia OS. IPSO systems are available in diskless flash-based and hybrid (flash-based systems with a supplemental hard disk for local logging). Gaia only supports disk-based IP-Systems. Standalone deployment is only supported on disk-based (IPSO or Gaia) systems.

On Flash-based IPSO Appliances, 1G of RAM is sufficient to run Firewall, IPS, and VPN blades only. To activate more blades, 2G of RAM is required on IP290, IP390, and IP560 Flash-based Appliances.

Note: 13500 does not support SecurePlatform. 13500 runs only on Gaia.
## Supported Upgrade Paths

If you are upgrading from a lower version, make sure you can do the necessary intermediate upgrades.

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
<th>Upgrade Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Gateway</td>
<td>R75.40</td>
<td>Direct - Install the appropriate package on the existing installation.</td>
</tr>
<tr>
<td>Security Management Server</td>
<td>R75.45</td>
<td><strong>NOTE:</strong> You can use the &quot;Advanced Upgrade&quot; procedures to upgrade from SecurePlatform to Gaia.</td>
</tr>
<tr>
<td>Multi-Domain Server</td>
<td>R75.46</td>
<td>1. Upgrade to R75.40. We highly recommend that you migrate from SecurePlatform to Gaia operating system. See &quot;Advanced Upgrade&quot; in the R75.40 Installation and Upgrade Guide.</td>
</tr>
<tr>
<td></td>
<td>earlier</td>
<td>2. Install the appropriate package.</td>
</tr>
</tbody>
</table>

**Note** - You cannot upgrade from R75.40VS to R75.47.

## Compatibility with Gateways and Clients

This release is compatible with these gateways and Endpoint clients.

<table>
<thead>
<tr>
<th>Release</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateways</td>
<td></td>
</tr>
<tr>
<td>Security Gateway</td>
<td>NGX R65, R70.x, R71.x, R75, R75.10, R75.20, R75.30, R75.40, R75.45, R75.46</td>
</tr>
<tr>
<td>DLP-1</td>
<td>R71 and higher</td>
</tr>
<tr>
<td>IPS-1</td>
<td>R71</td>
</tr>
<tr>
<td>Series 80</td>
<td>R71 and higher</td>
</tr>
<tr>
<td>VSX</td>
<td>VSX NGX R65, VSX NGX R67</td>
</tr>
<tr>
<td>Connectra</td>
<td>Centrally Managed NGX R66</td>
</tr>
<tr>
<td>UTM-1 Edge</td>
<td>7.5.x and higher*</td>
</tr>
<tr>
<td>GX</td>
<td>4.0</td>
</tr>
</tbody>
</table>

**Endpoint VPN Clients** see sk67820 (http://supportcontent.checkpoint.com/solutions?id=sk67820)

* UTM-1 Edge and Safe@ devices that use locally configured VPN connections with download configuration settings, may experience VPN connectivity failure with R75.47 Security Gateways. To enable this configuration with R75.47, see sk65369 (http://supportcontent.checkpoint.com/solutions?id=sk65369).

## Maintaining Server Version

You can maintain a R75.40, R75.40VS, R75.45, R75.46, or R76 Security Management Server or Multi-Domain Server without upgrading, and manage R75.47 Security Gateways.

If you choose to not upgrade the R75.40 management server:
- Anti-Bot and Anti-Virus will not work with R75.40 Security Management Server
- Some Resolved Issues will not be applied
To enable these Software Blades and features for an R75.40 environment, you must upgrade the R75.40 management server to R75.47.

You cannot enable these features in an R75.40VS environment. The R75.40VS or R76 management server cannot be upgraded to R75.47, and an R75.47 management server cannot manage R75.40VS or R76 gateways.

**To define a R75.47 Security Gateway object with a maintained server version:**
- Use the wizard to define the object.
- Or: In the properties window > gateway Properties > Version, select R75.40. When you run SIC, the installed version of the gateway shows correctly.

---

**Required Disk Space**

**Important** - Make sure there is enough available disk space before you install R75.47! You can delete the downloaded .tgz file after it is extracted, for more disk space for installation.

### Required Disk Space for Installation on Security Management Server

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Packed and Extracted.tgz File</th>
<th>During Installation</th>
<th>Final Used Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaia</td>
<td>root - 2.04 GB</td>
<td>root - 1.5 GB</td>
<td>root - 930 MB</td>
</tr>
<tr>
<td>SecurePlatform / Linux</td>
<td>/var - 2 GB</td>
<td>root - 210 MB /opt - 1.15 GB /var - 512MB</td>
<td>root - 2 MB /opt - 615 MB /var - 310 MB</td>
</tr>
<tr>
<td>IPSO Disk-based</td>
<td>/var - 910 MB</td>
<td>/opt - 600 MB /var - 300 MB</td>
<td>/opt - 300 MB /var - 200 MB</td>
</tr>
<tr>
<td>Windows</td>
<td>1.3 GB</td>
<td>1.5 GB</td>
<td>820 MB</td>
</tr>
</tbody>
</table>

### Required Disk Space for Installation on Security Gateway

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Packed and Extracted.tgz File</th>
<th>During Installation</th>
<th>Final Used Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaia</td>
<td>root - 2.02 GB</td>
<td>root - 1.44 GB</td>
<td>root - 515 MB</td>
</tr>
<tr>
<td>Gaia upgraded from SecurePlatform R71.x</td>
<td>/var - 2 GB</td>
<td>root - 35 MB /opt - 475 MB /var - 1070 MB</td>
<td>root - 20 MB /opt - 475 MB /var - 65 MB</td>
</tr>
<tr>
<td>SecurePlatform / Linux</td>
<td>/var - 2.01 GB</td>
<td>root - 225 MB /opt - 1.16 GB /var - 565 MB</td>
<td>root - 15 MB /opt - 415 MB /var - 65 MB</td>
</tr>
<tr>
<td>IPSO Disk-based</td>
<td>/var - 910 MB</td>
<td>/opt - 600 MB /var - 200 MB</td>
<td>/opt - 210 MB /var - 100 MB</td>
</tr>
<tr>
<td>Windows</td>
<td>1.3 GB</td>
<td>850 MB</td>
<td>500 MB</td>
</tr>
</tbody>
</table>
# Build Numbers

This table contains the R75.47 software products updated in this release and their build numbers. To confirm that this release is installed, run the version command for each product.

<table>
<thead>
<tr>
<th>Software Blade / Product</th>
<th>Build No.</th>
<th>Version Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Gateway</td>
<td>Build 171</td>
<td>fw ver -k</td>
</tr>
<tr>
<td>Security Management</td>
<td>Build 016</td>
<td>fwm ver</td>
</tr>
<tr>
<td>Multi-Domain Server</td>
<td>Build 146</td>
<td>fwm mds ver</td>
</tr>
</tbody>
</table>

You must install an upgraded SmartConsole after you install the management server and gateways.

<table>
<thead>
<tr>
<th>Console</th>
<th>Build No.</th>
<th>Version Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartConsole Applications</td>
<td>986690144</td>
<td>Help &gt; About Check Point &lt;Application Name&gt;</td>
</tr>
<tr>
<td>SmartDomain Manager</td>
<td>986690112</td>
<td>Help &gt; About Check Point Multi-Domain Security Management</td>
</tr>
</tbody>
</table>

**Important Note:** Effective August 12-13, 2013, the R75.47 images in the Check Point Support Center (http://supportcontent.checkpoint.com/solutions?id=sk93448) have been replaced. When installing the new R75.47 images, the Hotfix described in [sk94029](http://supportcontent.checkpoint.com/solutions?id=sk94029) is automatically installed on top of R75.47.

To find out if the Hotfix is installed, run this command (in Gaia and SecurePlatform run from Expert mode):

cpprod_util CPPROD_GetValue FW1//6.0//HotFixes HOTFIX_FOXX_HF_HA47_017 1

- If the return value is 1, the Hotfix is installed.
- If the return value is Failed to find the value, we recommend installing the Hotfix described in [sk94029](http://supportcontent.checkpoint.com/solutions?id=sk94029).
New Installation

R75.47 is released as:

- an upgrade to R75.40, R75.45, or R75.46 ("Upgrading" on page 12).
- a clean installation for Gaia open servers and appliances supported by R75.40.
- a clean installation for SecurePlatform appliances supported by R75.40.
- a clean installation for IPSO Flash-based appliances.

To install this release on Gaia or SecurePlatform, see the R75.40 Installation and Upgrade Guide (http://supportcontent.checkpoint.com/documentation_download?ID=13948).

To install on IPSO, clean the gateway and then install R75.47 (see next sections).

Downloading the Clean Install Package

Download the R75.47 Full ISO package for your platform from the Check Point Support Center.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaia appliances*, Open Server, and Data Center</td>
<td>Check_Point_R75.47_GAIA.iso</td>
</tr>
<tr>
<td>SecurePlatform appliances* and Data Center</td>
<td>Check_Point_R75.47_SPLAT_Appliance.iso</td>
</tr>
<tr>
<td>Smart-1 Appliances</td>
<td>Check_Point_R75.47_SPLAT_Smart-1.iso</td>
</tr>
<tr>
<td>IPSO 6.2 Flash-based</td>
<td>Check_Point_R75.47_Security_Gateway_for_IPSO6_2.tgz</td>
</tr>
</tbody>
</table>

* Supported Check Point Appliances (on page 6)

Clean Install on IPSO Flash-Based Gateways

To install on IPSO, clean the Security Gateway of Check Point installations, TGZ files, and unused IPSO images. You use Network Voyager or the command shell. (Use Voyager to delete unused IPSO images.)

To delete Check Point packages using Network Voyager:
1. Click Configuration > System Configuration > Packages > Delete Packages.
2. Select an installation package to delete, and click Apply.
3. Delete tgz files.
4. Click Apply.

To delete Check Point packages using command shell:
1. Run: newpkg -q
   - The output is the list of installed packages. Use this output in the next commands.
2. Run: newpkg -u <package name>
3. Run: rm opt/packages/<tgz name>

After you clean the gateway, you can install R75.47.

To install on IPSO Flash-based Security Gateway with CLI:
1. Make sure there is enough free disk space for installation ("Required Disk Space" on page 8).
2. Download the R75.47 clean install package for IPSO 6.2 Flash-based to /preserve/opt/packages.
3. Run: `newpkg`
4. Type the number (1 - 3) for the FTP server or local path where the `tgz` is.
5. Enter the IP address, credentials, and pathnames when prompted.
6. Type `y` to download the `tgz`. The file is downloaded and installation starts.
7. When prompted for installation type, type `1` to select **Install this as a new package**.
   R75.47 is installed under `/opt`.

**To install on IPSO Flash-based Security Gateway with manual download:**
1. Download the R75.47 clean install package for IPSO 6.2 Flash-based.
2. Install the package:
   - **Network Voyager** - See "Installation on IPSO" in the *R75.40 Installation and Upgrade Guide*.
   - **Command Line add package** - Copy the file to an ftp server and run:
     ```
     add package media ftp addr <ip_address> user <username> password <password>
     name Check_Point_R75.47_Security_Gateway_for_IPSO6_2.tgz
     ```

**Installing the Client Applications**

The client applications for this release are part of the Check Point SmartConsole.

**To manually install the SmartConsole:**
1. Download R75.47 SmartConsole for Windows: `Check_Point_SmartConsole_R75.47_Windows.exe`
2. Double-click the file to install the SmartConsole.

**To install the Multi-Domain Security Management SmartDomain Manager:**
1. Download R75.47 SmartDomain Manager for Windows: `Check_Point_SmartDomain_Manager_R75.47_Windows.exe`
2. Double-click the file to install the SmartDomain Manager.
Upgrading

We recommend that you back up your system before installing this release package. Save a manually created image before you install.

**Full Connectivity Upgrade**

R75.47 supports Full Connectivity Upgrade from R75.40, up to R75.47.

To learn more, see the [R75.40 Installation and Upgrade Guide](http://downloads.checkpoint.com/dc/download.htm?ID=13948).

**New Backup Path**

After you upgrade to R75.47, backup files on Gaia appliances are saved to `/var/log/CPbackup/backups/R75.40`.

**Before You Upgrade!**

**Mobile Access Manual Changes:**

If you use the Mobile Access Software Blade and you made manual changes to configuration files on the Security Gateway, you must manually change the upgraded files after installation.

Do not overwrite the R75.47 files with your customized files!

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

1. Open the files and make note of the changes.
2. Upgrade to R75.47.
3. Manually edit the new versions of the files, to include your changes.

**Downloading the Upgrade Package**

Download the R75.47 upgrade package for your platform from the Check Point Support Center.

<table>
<thead>
<tr>
<th>Platform</th>
<th>R75.47 Upgrade Package</th>
<th>Upgrade Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaia open server or appliance*</td>
<td>Check_Point_R75.47.tgz for R75.40</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check_Point_R75.45_R75.47.tgz for R75.45</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check_Point_R75.46_R75.47.tgz for R75.46</td>
<td></td>
</tr>
<tr>
<td>Gaia open server or appliance*</td>
<td>Check_Point_R75.47.GAIA.tgz</td>
<td>CLI</td>
</tr>
</tbody>
</table>
Upgrading

<table>
<thead>
<tr>
<th>Platform</th>
<th>R75.47 Upgrade Package</th>
<th>Upgrade Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurePlatform open server or appliance*</td>
<td>Check_Point_R75.47.SPLAT.tgz</td>
<td>WebUI or CLI</td>
</tr>
<tr>
<td>Linux open server</td>
<td>Check_Point_R75.47.Linux.tgz</td>
<td>CLI</td>
</tr>
<tr>
<td>IPSO 6.2 Disk-based</td>
<td>Check_Point_R75.47.IPSO6.tgz</td>
<td>CLI</td>
</tr>
<tr>
<td>Windows</td>
<td>Check_Point_R75.47.windows.tgz</td>
<td>CLI</td>
</tr>
<tr>
<td>Solaris</td>
<td>Check_Point_R75.47.solaris2.tgz</td>
<td>CLI</td>
</tr>
</tbody>
</table>

* Supported Check Point Appliances (on page 6)

Upgrading on Gaia with Automatic Software Updates from WebUI

To install on Gaia with Automatic Software Updates from WebUI:
1. In Gaia WebUI, go to Software Updates > Status and Actions.
   Note – If you upgrade from R75.40 and the archive GaiaSoftwareUpdatesAgent_358.tgz is not created, see sk81680 (http://supportcontent.checkpoint.com/solutions?id=sk81680).
2. Select GaiaSoftwareUpdatesAgent_358.tgz update archive in the table.
3. Click Download.
   The package downloads.
4. Click Install.
5. Select appropriate archive in the table, and make sure the status is Available for Download:
   • Check_Point_R75.47.tgz - for upgrade from R75.40.
   • Check_Point_R75.45_R75.47.tgz - for upgrade from R75.45.
   • Check_Point_R75.46_R75.47.tgz - for upgrade from R75.46.
6. Click Download.
   The package downloads.
7. Click Check Install to verify installation.
8. Click OK.
   Installation verified - Installation is allowed confirmation window shows. Verification is complete.
9. Click Install.
10. Reboot the device.

To download and install the new SmartConsole:
1. Open Gaia WebUI and go to Software Updates > Status and Actions.
2. Select Check_Point_SmartConsole_R75.47.tgz in the table and make sure the status is Available for Download.
3. Click Download.
   The package downloads.
4. Click Install.
5. Go to overview page and click Download Now.
   The SmartConsole downloads to your desktop.
6. Double-click the downloaded file to install the SmartConsole.
Note - During a manual installation procedure, we recommend to clear the Self-test - Auto-rollback in the failure box on the Policy page, and click Apply.

Upgrading with CLI

Use these instructions to upgrade to R75.47 on Gaia, SecurePlatform, IPSO, or Windows.

You can safely delete the .tgz file after you extract the package (step 5).

To install R75.47 using the CLI:

1. Log onto the target machine.
   - On SecurePlatform only:
     a) Run `idle 120` to make sure that the installation is not interrupted by the automatic logon timeout.
     b) Run `expert` to enter expert mode.

2. Make sure the target computer or appliance has sufficient free disk space.

3. Create a temporary directory
   • in the /var partition on non-Windows platforms.
   • in the c:\ partition on Windows platforms.

4. Copy the upgrade package for your platform to the temporary directory using SFTP, SCP, or similar secure utility.

5. Go to the temporary directory and extract the .tgz package.
   • on non-Windows platforms run `gtar -zxvf <file name>`.
   • on Windows platforms use an archive utility such as WinZip.

   Important - Before installing on Multi-Domain Security Management, run `mdsenv` and then `mdsstop`.
   If this is not done, the system will experience functionality issues.
   We recommend that you back up the system before installation: `mds_backup`

6. Start installation:
   • On non-Windows platforms, from the /var partition, run `.//UnixInstallScript`.
     Note: You must run this command from the /var partition.
   • On Windows platforms, run `Setup.exe`.

7. Do the instructions on the screen to install the applicable components.
   Only components required for a specific target (management or gateway) are installed automatically.
   When the installation finishes, each successfully installed component appears in a list followed by: `Succeeded`.

8. When prompted, reboot the computer.
   Note: In a cluster environment, make sure to upgrade all the cluster members.

Upgrading with Web User Interface

You can install R75.47 on SecurePlatform Security Gateways and Security Management Servers with the WebUI.

Important - Safe Upgrade is not supported from R75.40, R75.45, or R75.46 to R75.47. Make a manual snapshot of the machine before you upgrade.

To install R75.47 using the Web User Interface:

1. Make sure all GUI applications are closed.
2. Download the upgrade package for your platform.
3. Connect to the Web User Interface:
Post-Installation Configuration

After R75.47 is installed, including the SmartDashboard or SmartDomain Manager client, configure the environment to recognize the new version.

1. Open SmartDashboard and log in to the R75.47 Security Management Server that controls the new gateways.
2. Open the gateway object properties window of an new gateway and change the version to R75.47.
3. If you use the Mobile Access blade with Endpoint Security on Demand Compliance scanning, update it now: SmartDashboard > Mobile Access > Endpoint Security on Demand > Update Databases Now
4. Repeat for all management servers, Log Servers and gateways.
5. Install the security policy on new gateways and servers.

Important - After upgrading, move the snapshot file from the Desktop to a pathname without spaces. This must be done before you attempt to restore the machine.
To uninstall, revert to the snapshot manually.
Uninstalling

Before you uninstall:

Disable the IPS Event Analysis and SmartWorkflow Software Blades in the Security Management Server object. If you already disabled them before upgrading, you do not need to disable them again.

Uninstalling from Windows


Uninstalling from other Operating Systems

Note - If you uninstall from SecurePlatform, the login prompt and the WebUI Welcome screen will still show "Check Point SecurePlatform R75.47" as the installed version. SecurePlatform operating system packages are not uninstalled. Use the `fw ver` command to see the actual installed version.

In a Security Management Server deployment, to uninstall R75.47 from SecurePlatform, Linux, IPSO, and Solaris, run:

```
/opt/CPUninstall/R75.47/UnixUninstallScript
```

You can use this on Gaia, if you did not use the Automatic Software Updates to upgrade or install.

Uninstalling in Multi-Domain Security Management

In a Multi-Domain Security Management deployment, use these steps to uninstall R75.47.

To uninstall R75.47 in Multi-Domain Security Management deployments:

1. Disable R75.47 from each Domain Management Server:
   a) Login to the SmartDomain Manager.
   b) In Versions & Blades Updates, right click and select Deactivate.

2. On each Multi-Domain Server, Domain Log Server and Multi-Domain Log Server, run:
   `/opt/CPUninstall/R75.47/UnixUninstallScript`

3. Run the same script on Domain Management Servers and Security Gateways.
4. Activate Software Blades that were active before the upgrade to R75.47.

Uninstalling with Gaia Automatic Software Updates

If you installed with Automatic Software Updates, you must uninstall in this way.

Note - Some of the Gaia packages are SecurePlatform RPMs. These packages cannot be uninstalled.

Before you uninstall:

If you deployed Multi-Domain Security Management on Gaia, disable R75.47 from each Domain Management Server:

1. Login to the SmartDomain Manager
2. In Versions & Blades Updates, right click and select Deactivate.
To uninstall from Gaia with Automatic Software Updates from WebUI:

1. Log in to the WebUI of the Gaia computer or appliance and go to Software Updates > Status and Actions.

   \[\textbf{Important} - \text{If the warning} \text{Installation service is not running. Package actions disabled.} \text{appears, the Deployment Agent is down. To activate the Deployment Agent, switch to expert mode and run this command:} \text{dbget installer:start.}\]

2. Make sure the update archive file is in the table:
   - Check_Point_R75_47.tgz if you updated from R75.40.
   - Check_Point_R75_45_R75_47.tgz if you updated from R75.45.
   - Check_Point_R75_46_R75_47.tgz if you updated from R75.46.

3. Make sure the status is **Installed**.

4. Select the package.

5. Click **Uninstall**.

6. Reboot.