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=18381
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 March 2013</td>
<td>Appliances table updated for IPSO management support (&quot;Check Point Appliances&quot; on page 6).</td>
</tr>
<tr>
<td>18 February 2013</td>
<td>Updated link location for R75.40 Installation and Upgrade Guide in New Installation (on page 9). Moved link to top of page.</td>
</tr>
<tr>
<td>16 December 2012</td>
<td>Updated Security Management Server in Build Numbers (on page 8)</td>
</tr>
<tr>
<td>07 November 2012</td>
<td>Updated Security Gateway in Build Numbers (on page 8)</td>
</tr>
<tr>
<td>11 October 2012</td>
<td>General updates</td>
</tr>
<tr>
<td>4 October 2012</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 R75.45 Release Notes).
# Contents

Important Information........................................................................................................3  
Introduction ......................................................................................................................5  
   What’s New .................................................................................................................5  
      More About the New Acceleration Card .................................................................5  
      More About DDoS Protector .....................................................................................6  
   URL Filtering Protocol ...............................................................................................6  
System Requirements .....................................................................................................6  
   Supported Operating Systems ....................................................................................6  
   Check Point Appliances ..............................................................................................7  
   Supported Upgrade Paths .............................................................................................7  
   Maintaining Server Version .......................................................................................8  
   Required Disk Space .................................................................................................8  
   Build Numbers ..........................................................................................................8  
New Installation .............................................................................................................9  
   Cleaning IPSO Flash-Based Gateways ......................................................................9  
   Downloading the Clean Install Package ..................................................................10  
   Clean Install on IPSO Flash-Based with CLI ............................................................10  
   Clean Install on IPSO Flash-Based with Manual Download ....................................10  
   Installing the Client Applications .............................................................................10  
Upgrading .......................................................................................................................11  
   Before You Upgrade! .................................................................................................11  
   Automatic Software Updates on Gaia .......................................................................11  
   Downloading the Upgrade Package .........................................................................12  
   Upgrading with CLI ...................................................................................................12  
   Upgrading with Web User Interface .........................................................................13  
Post-Installation Configuration ......................................................................................13  
   Using DDoS Protector with R75.45 ........................................................................14  
Uninstalling ....................................................................................................................15  
   Uninstalling with Gaia Automatic Software Updates ..............................................15  
   Uninstalling with CLI ...............................................................................................15  
   Uninstalling with SmartUpdate ...............................................................................16
Introduction

This version installs important Check Point product and Gaia Operating System updates on computers that were upgraded to R75.45 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 installation (on supported upgrade platforms). For more about R75.40 and to download the software, see the Check Point R75.40 page (http://supportcontent.checkpoint.com/solutions?id=sk67581).

- Known Limitations of R75.45 - sk82741 (http://supportcontent.checkpoint.com/solutions?id=sk82741)
- Resolved Issues in R75.45 - sk82742 (http://supportcontent.checkpoint.com/solutions?id=sk82742)
- Known Limitations of R75.40 - sk67582 (http://supportcontent.checkpoint.com/solutions?id=sk67582)
  All R75.40 limitations that are not resolved with this release, are still open.
- Resolved Issues in R75.40 - sk67583 (http://supportcontent.checkpoint.com/solutions?id=sk67583)

Notes -

- This is a hotfix for R75.40. R75.45 does not support installation over R75.40VS. For the differences between R75.40 and R75.40VS, see sk82460 (http://supportcontent.checkpoint.com/solutions?id=sk82460).
- R75.40VS Security Management server can manage R75.45 Security Gateways.
- R75.45 Security Management server can not manage R75.40VS Security Gateways.
- E80.40 management server cannot manage R75.45 Security Gateways.

What's New

- Anti-Bot and Anti-Virus fixes
- New features for Gaia
- Aggregation of logs of the IPS Non Compliant HTTP and Non Compliant DNS protections
- Log Server – performance improvements enables writing logs in a more efficient way. This solved capacity issues in specific scenarios.
- Anti-Malware report – Expose the severity and category of the malwares found in the overview and additional pages to allow better high level understanding of Anti-Bot and Anti-Virus Blade findings.
- Support for the 21000 Appliance Security Acceleration Module (SAM) and 10G SFP+ Acceleration-Ready I/O Card ("More About the New Acceleration Card" on page 5)
- DDoS Protector appliance support ("More About DDoS Protector" on page 6)

More About the New Acceleration Card

The release supports the 21000 Appliance Security Acceleration Module (SAM) and 10G SFP+ Acceleration-Ready I/O Card. Install the Check Point Security Acceleration Module for the 21000 Appliance for network traffic acceleration and low latency. It is an accessory which can be installed in the rear slot of the appliance. The 10G SFP+ Acceleration Ready I/O card is a new 21000 Interface card which is used with the SAM.

For more about the 21000 Appliance Security Acceleration Module, see sk68701 (http://supportcontent.checkpoint.com/solutions?id=sk68701).
More About DDoS Protector

This release integrates SmartView Tracker and SmartEvent with the Check Point DDoS Protector appliance.

**SmartEvent** includes SmartEvent Intro, SmartReporter and Event Correlation for centralized reporting, real-time security event correlation, and management of security data. Security teams do not look through massive amounts of data: they focus on the threats and trends with the greatest risk potential.

**SmartView Tracker** is a Logging and Status Software Blade for real-time tracking of logged connections and administrator activity. SmartView Tracker reduces time required to troubleshoot configuration errors.

**Check Point DDoS Protector** is an appliance with advanced Denial of Service (DoS) detection and prevention. DDoS Protector technology inspects signatures and behavior before new server sessions are started.

Configurations for DDoS Protector Support

**Important** - Before you begin installation, back up the Domain Log Server, the SmartEvent server, and (if in a Multi-Domain Security Management environment) the Multi-Domain Log Server.

- Install R75.45 on all relevant logging servers in your environment.
- After you install R75.45 on the logging servers, install the new SmartConsole ("Installing the Client Applications" on page 10) and then configure DDoS Protector for R75.45 ("Using DDoS Protector with R75.45" on page 14).

URL Filtering Protocol

The Security Management Server provides a URL filtering service for centrally managed UTM-1 Edge devices. In R75.45, the new URL Filtering Protocol is Check Point’s standard engine that is cloud based and does not require updates. No effect on UTM-1 Edge devices or service quality is expected. This change is transparent for UTM-1 Edge devices.

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
- 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>21400 Appliance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Appliances (IP150, IP280, IP290, IP390, IP560, IP690, IP1280, IP2450)</td>
<td>✓ (Disk-based only)</td>
<td>✓ * (Disk-based only)</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 Appliance platforms are available in disk-based, diskless flash-based and hybrid (flash-based systems with a supplemental hard disk for local logging, swap space and core file storage) configurations.

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></td>
<td><strong>NOTE:</strong> You can use the &quot;Advanced Upgrade&quot; procedures to upgrade from SecurePlatform or IPSO to Gaia.</td>
</tr>
<tr>
<td>Multi-Domain Server</td>
<td></td>
<td>We highly recommend that you migrate from SecurePlatform or IPSO to the Gaia operating system. See &quot;Advanced Upgrade&quot; in the R75.40 Installation and Upgrade Guide.</td>
</tr>
</tbody>
</table>

1. Upgrade to R75.40.  
   We highly recommend that you migrate from SecurePlatform or IPSO to the Gaia operating system.  
   See "Advanced Upgrade" in the R75.40 Installation and Upgrade Guide.

2. Install the appropriate package.

**Note** - You cannot upgrade from R75.40VS to R75.45.  
This release is automatically activated on all Multi-Domain Security Management Domains.
Maintaining Server Version

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

You cannot enable these features in an R75.40VS environment. The R75.40VS or R76 management server cannot be upgraded to R75.45, and an R75.45 management server cannot manage R75.40VS or R76 gateways.

Required Disk Space

⚠️ **Important** - Make sure there is enough available disk space before you install R75.45!

Installation can use more disk space that is released when installation ends. 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 / SecurePlatform / Linux</td>
<td>/var - 1.8 GB</td>
<td>root - 200 MB /opt - 700 MB /var - 400 MB</td>
<td>root - 0 MB /opt - 400 MB /var - 200 MB</td>
</tr>
<tr>
<td>IPSO Disk-based</td>
<td>/var - 1 GB</td>
<td>/opt - 400 MB /var - 600 MB</td>
<td>/opt - 200 MB /var - 100 MB</td>
</tr>
<tr>
<td>Windows</td>
<td>700 MB</td>
<td>1 GB</td>
<td>600 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 / SecurePlatform / Linux</td>
<td>/var - 1.8 GB</td>
<td>root - 200 MB /opt - 700 MB /var - 400 MB</td>
<td>root - 20 MB /opt - 400 MB /var - 100 MB</td>
</tr>
<tr>
<td>IPSO Disk-based</td>
<td>/var - 800 MB</td>
<td>/opt - 330 MB /var - 600 MB</td>
<td>/opt - 230 MB /var - 100 MB</td>
</tr>
<tr>
<td>Windows</td>
<td>700 MB</td>
<td>750 MB</td>
<td>300 MB</td>
</tr>
</tbody>
</table>

Build Numbers

This table contains the R75.45 software products updated in this release and their build numbers. To confirm that the hotfix is installed, run the version command for each product.
New Installation


R75.45 is released as:
- an upgrade to version R75.40 ("Upgrading" on page 11)
- 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

## Cleaning IPSO Flash-Based Gateways

To clean 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>`

### To delete unused IPSO images using Network Voyager:
1. Click **Configuration > System Configuration > Images > Manage Images**.
2. Click **Delete IPSO Images**.
3. Select the IPSO image to delete, and click **Apply**.

---

### Software Blade / Product Build No. Version Command

<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 193</td>
<td><code>fw ver -k</code></td>
</tr>
<tr>
<td>Security Management</td>
<td>Build 015</td>
<td><code>fwm ver</code></td>
</tr>
<tr>
<td>Multi-Domain Server</td>
<td>Build 165</td>
<td><code>fwm mds ver</code></td>
</tr>
</tbody>
</table>
| SecurePlatform           | Build 018 | Upgrade: `splat_ver`  
                          |            | Clean install: `ver` |

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>986650154</td>
<td>Help &gt; About Check Point <strong>&lt;Application Name&gt;</strong></td>
</tr>
<tr>
<td>SmartDomain Manager</td>
<td>986650147</td>
<td>Help &gt; About Check Point Multi-Domain Security Management</td>
</tr>
</tbody>
</table>
Downloading the Clean Install Package

Download the R75.45 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_R75.45_GAIA_SPLAT_linux.iso</td>
</tr>
<tr>
<td>SecurePlatform appliances* and Data Center</td>
<td>Check_Point_R75.45_SPLAT_Appliance.iso</td>
</tr>
<tr>
<td>Smart-1 Appliances</td>
<td>Check_Point_R75.45_SPLAT_Smart-1.iso</td>
</tr>
<tr>
<td>IPSO 6.2 Flash-based</td>
<td>Check_Point_R75.45_Security_Gateway_for_IPSO6_2.tgz</td>
</tr>
</tbody>
</table>

* Supported Check Point Appliances (on page 6)

Clean Install on IPSO Flash-Based with CLI

To install on IPSO Flash-based Security Gateway with CLI:

1. If there are installed Check Point installations, tgz files, or unused IPSO images, clean the gateway ("Cleaning IPSO Flash-Based Gateways" on page 9).
2. Make sure there is enough free disk space for installation.
3. Download the R75.45 clean install package for IPSO 6.2 Flash-based to /preserve/opt/packages.
4. Run: newpkg
5. Type the number (1 - 3) for the FTP server or local path where the tgz is.
6. Enter the IP address, credentials, and pathnames when prompted.
7. Type y to download the tgz. The file is downloaded and installation starts.
8. When prompted for installation type, type 1 to select Install this as a new package. R75.45 is installed under /opt.

Clean Install on IPSO Flash-Based with Manual Download

To install on IPSO Flash-based Security Gateway with manual download:

1. Download the R75.45 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_R75.45_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 R75.45 SmartConsole for Windows: Check_Point_SmartConsole_R75.45_Windows.exe
2. Double-click the file to install the SmartConsole.

To install the Multi-Domain Security Management SmartDomain Manager:

1. Download R75.45 SmartDomain Manager for Windows:
   Check_Point_SmartDomain_Manager_R75.45_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.

Before You Upgrade!

**Windows 7**: Turn off User Account Control (UAC) before you install on Windows 7. Reboot after install.

**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 R75.45 files with your customized files!

<table>
<thead>
<tr>
<th>Data</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Configurations</td>
<td>$CVPNDIR/conf/cvpnd.C</td>
</tr>
<tr>
<td>Apache Configuration Files</td>
<td>$CVPNDIR/conf/httpd.conf</td>
</tr>
<tr>
<td></td>
<td>$CVPNDIR/conf/includes/*</td>
</tr>
<tr>
<td>Local certificate authorities</td>
<td>$CVPNDIR/var/ssl/ca-bundle/</td>
</tr>
<tr>
<td>DynamicID (SMS OTP) Local Phone List</td>
<td>$CVPNDIR/conf/SmsPhones.lst</td>
</tr>
<tr>
<td>RSA configuration</td>
<td>/var/ace/sdconf.rec</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 R75.45.
3. Manually edit the new versions of the files, to include your changes.

**Automatic Software Updates on Gaia**

For **Gaia only** use Automatic Software Updates tool for automatic, policy-based downloads, installations and user notification for software hotfixes and HFAs.

- **Note** - During installation, you may see error messages that show: Failed to acquire the lock. or Unable to connect to the server. Press OK to reconnect.
  You can click OK and continue.

- **Note** - After installation, the Security Gateway reboots automatically.

**To install on Gaia with Automatic Software Updates from WebUI:**
1. Make sure there is at least 300 MB on $CPDIR, and at least 100 MB on /tmp.
2. Take a snapshot of the machine.
   This is highly recommended!
   If you use a proxy to access the Internet, use the instructions in this SK to set the proxy.
4. Log in to the WebUI of the Gaia computer or appliance to update.
5. In the **Software Updates > Status and Actions** menu, select: **Check_Point_R75.45_GAIA.tgz**
6. Click **Download**.
7. When the package is downloaded, click **Install**.

### Downloading the Upgrade Package

Download the R75.45 upgrade package for your platform from the Check Point Support Center.

<table>
<thead>
<tr>
<th>Platform</th>
<th>R75.45 Upgrade Package</th>
<th>Upgrade Procedure</th>
</tr>
</thead>
</table>
| Gaia open server or appliance*| • Check_Point_R75.45.tgz - for R75.40  
• Check_Point_R75.45_R75.45.tgz - for R75.45 | Gaia Automatic Software Updates  
("Automatic Software Updates on Gaia" on page 11) |
| Linux open server             | Check_Point_R75.45.GAIA_SPLAT_linux.tgz | • CLI                                                  |
| SecurePlatform open server or appliance* | Check_Point_R75.45.GAIA_SPLAT_linux.tgz | • WebUI  
• CLI  
• SmartUpdate |
| IPSO 6.2 Disk-based           | Check_Point_R75.45.IPSO6.tgz  | • CLI  
• SmartUpdate                                          |
| IPSO 6.2 4G Flash-based       | Check_Point_R75.45.IPSO6_Flash.tgz | • CLI  
• SmartUpdate                                          |
| Windows                       | Check_Point_R75.45.windows.tgz  | • CLI  
• SmartUpdate                                          |
| Solaris                       | Check_Point_R75.45.solaris2.tgz  | • CLI                                                  |

* Supported Check Point Appliances (on page 6)

### Upgrading with CLI

Use these instructions to upgrade to R75.45 on Gaia, SecurePlatform, or Windows.

💡 You can safely delete the `.tgz` file after you extract the package (step 6).

**To install R75.45 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 the 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, or 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 `mdsstopt`. 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`.
     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.
   In a cluster environment, make sure to upgrade all the cluster members.

### Upgrading with Web User Interface

You can install R75.45 on SecurePlatform Security Gateways and Security Management Servers with the WebUI.

⚠️ **Important** - Safe Upgrade is not supported from R75.40 to R75.45. Make a manual snapshot of the machine before you upgrade.

**To install R75.45 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:
   - Open server: `https://<IP>`
   - Appliance: `https://<IP>:4434`
4. Open the **Upgrade** page:
   - Open server: **Device > Upgrade**
   - Appliance: **Appliance > Upgrade**
5. In the **Upgrade Steps** pane, browse to the downloaded file.
6. Click the **Upload package** button.
7. Click **Start Upgrade**.
   At the end of the installation, the computer or appliance automatically reboots.
8. Log in.

⚠️ **Important** - After upgrading, move the snapshot file from the Desktop to a pathname without spaces. This must be done before you try to restore the machine.

To uninstall, revert to the snapshot manually.

### Post-Installation Configuration

After R75.45 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 R75.45 Security Management server that controls the new gateways.
2. Open the gateway object properties window of an new gateway and change the version to **R75.45**.
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.

Using DDoS Protector with R75.45

DDoS Protector requires manual configuration to support R75.45.

To get DDoS Protector logs in R75.45:
1. In SmartDashboard, open the network objects that receive logs from DDoS Protector.
2. Open the Logs tab and select accept syslog.
3. If the log server is deployed on a computer or appliance that is not the management server, click Policy > Install Database.
4. Restart the log server processes. Run: cpstop and then cpstart
Uninstalling

Uninstalling with Gaia Automatic Software Updates

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

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

To uninstall from Gaia with Automatic Software Updates from WebUI:
1. In Gaia WebUI go to Software Updates > Status and Actions.
2. Select the installed R75.45 package.
3. Click Uninstall.
4. Reboot the device.

Uninstalling with CLI

Uninstall instructions are different for Multi-Domain Security Management and for Security Management server deployments.

To uninstall R75.45 in Security Management Server deployments:
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.

On Non-Windows platforms, continue with:
On each management server and dedicated Domain Log Server, run:
/opt/CPUninstall/R75.45/UnixUninstallScript
On Windows platforms, continue with:
1. Go to: C:\Program files\CheckPoint\CPUninstall\R75.45
2. Run: Uninstall.bat

To uninstall R75.45 in Multi-Domain Security Management deployments:
1. Disable R75.45 from each Domain Management Server:
   a) Login to the SmartDomain Manager
   b) In Versions & Blades Updates, right click and select Deactivate.
2. Run this command on each Multi-Domain Server, Domain Log Server and Multi-Domain Log Server: /opt/CPUninstall/R75.45/UnixUninstallScript
3. Activate Software Blades that were active before the upgrade to R75.45.

Note - If you uninstall from SecurePlatform, the login prompt and the WebUI Welcome screen will still show “Check Point SecurePlatform R75.45” as the installed version. SecurePlatform operating system packages are not uninstalled. Use the fw ver command to see the actual installed version.
Uninstalling with SmartUpdate

You can use SmartUpdate to remotely uninstall on gateways of all platforms, except IPSO. You must uninstall all packages, except for the SecurePlatform package that cannot be uninstalled from SecurePlatform gateways.

To uninstall with SmartUpdate:
1. Make sure SmartDashboard is closed.
2. Open SmartUpdate.
3. From the Packages menu choose Get Data From All.
4. Right-click each package with Minor Version value of R75.45 and select Uninstall, in this order:
   - Security Gateway
   - Mobile Access (for SecurePlatform gateways, if installed)
   - all other Minor Version products
5. On Windows platforms, reboot manually.