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=12081
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>17 May 2011</td>
<td>Fixed directories of IPSO Disk-based for Required Disk Space (on page 13).</td>
</tr>
<tr>
<td></td>
<td>Added Crossbeam support for Security Gateways (&quot;Security Software Containers&quot; on page 8).</td>
</tr>
<tr>
<td>12 May 2011</td>
<td>Added Application Control support on Crossbeam (&quot;Security Gateway Software Blades&quot; on page 10).</td>
</tr>
<tr>
<td>5 May 2011</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 R75.10 Release Notes).
Contents

Important Information ................................................................. 3
Introduction to R75.10 ................................................................. 5
What’s New in R75.10 ................................................................. 6
Platform Provisions and Requirements ........................................... 7
  Supported Upgrade Paths .......................................................... 7
  Supported Security Products by Platform .................................... 8
    Security Software Containers ................................................. 8
    Security Gateway Software Blades ...................................... 10
    Security Management Software Blades .................................. 11
  Clients and Consoles by Windows Platform ................................. 12
  Minimum System Requirements ................................................ 12
  Required Disk Space .............................................................. 13
  Build Numbers ........................................................................ 14
Installing R75.10 ........................................................................ 15
  New Installation of R75.10 ......................................................... 15
  Upgrading from R75 ................................................................. 16
    Upgrade Packages ................................................................. 16
    Upgrading with the SecurePlatform Web User Interface .......... 17
    Upgrading with the Command Line ....................................... 17
    Upgrading with SmartUpdate .............................................. 19
  Installing the Client Applications ............................................ 20
  Uninstalling ............................................................................. 21
fwm getpcap Command ................................................................ 22
Introduction to R75.10

Thank you for updating to Check Point version R75.10. This version contains new features and resolves various issues for Check Point Software Blades. Please read this document carefully before installing R75.10.

Important - Check Point software versions R75.10 or higher require a valid Software Blades license. Users with NGX licenses will not be able to install the software. To learn how to migrate NGX licenses to Software Blades licenses, see Software Blade Migration (http://www.checkpoint.com/products/promo/software-blades/upgrade/index.html) or contact Account Services.

If you manage IPv6 or GX gateways from your management, you must regenerate your IPv6 and GX licenses in the User Center, to be compliant with Software Blades.

Related Information:
R75.10 Home Page (http://supportcontent.checkpoint.com/solutions?id=sk62400)
R75.10 Known Limitations (http://supportcontent.checkpoint.com/solutions?id=sk62401)
R75.10 Resolved Issues (http://supportcontent.checkpoint.com/solutions?id=sk62402)
What's New in R75.10

Mobile Access Software Blade
- Improved Clientless VPN features
  - Support for Secure Workspace and SSL Network Extender (Application and Network Modes) on Windows 7 32/64-bit
  - Improved SSL Network Extender application control by software vendor so you can easily choose to allow all applications from a specific vendor
  - SSL Network Extender on Mac 10.6 connecting to the Mobile Access Software Blade
- Support for Check Point Mobile for iPhone and iPad, from the R75 Hotfix (http://supportcontent.checkpoint.com/documentation_download?ID=11950).
  - Access to Web applications
  - Access to email, calendar, and contacts
  - Two-factor authentication with client certificate and username/password

SmartConsole
- Multiple selection of applications in Application Control
- Faster loading time and improved application performance

SmartEvent and SmartView Tracker
- Faster query response and improved application performance
- Get packet capture data from the Security Gateway with the fwm getpcap Command (on page 22)

VPN Client
This version includes a deployment package of Endpoint Security VPN R75, which replaces SecureClient and Endpoint Connect. For automatic deployment of the new VPN client, select a client upgrade mode in Global Properties > Remote Access > Endpoint Connect.

New Support
- UTM-1 Edge 8.2 gateways
- SecuRemote E75.10
- Pre-shared secret authentication method for E75 remote access clients
Supported Upgrade Paths

R75.10 can be installed on R75 Security Gateways, Security Management servers, and Multi-Domain Security Management Multi-Domain Servers.

To upgrade from NGX R65, R70, R71, or R71.20, first upgrade to version R75. For upgrade instructions, see R75 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=11647).

To upgrade Check Point Suite Products before version NGX R65, first upgrade to NGX R65.

Note - This release is automatically activated on all Multi-Domain Security Management Domains.
# Supported Security Products by Platform

These tables show the security products related to this release and on which platforms they are supported.

## Security Software Containers

Software containers are supported on these operating systems and platforms.

<table>
<thead>
<tr>
<th>Software Blade Containers</th>
<th>Check Point Platforms and Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Secure Platform</td>
</tr>
<tr>
<td>Security Management</td>
<td>✓</td>
</tr>
<tr>
<td>Security Gateway</td>
<td>✓</td>
</tr>
<tr>
<td>Multi-Domain Security Management</td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software Blade Containers</th>
<th>Other Platforms and Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Microsoft</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003, 2008</td>
</tr>
<tr>
<td>Security Management</td>
<td>✓</td>
</tr>
<tr>
<td>Security Gateway</td>
<td>✓</td>
</tr>
<tr>
<td>Multi-Domain Security Management</td>
<td></td>
</tr>
</tbody>
</table>

### Notes about Security Software Containers

1. The supported IP Appliances models are 150, 290, 390, 560, 690, 1280, and 2450.
2. We recommend that you install Multi-Domain Security Management on Sun M-Series servers. We do not recommend that you install Multi-Domain Security Management on Sun T-Series servers.
Operating System Versions
The versions of the Microsoft and RedHat operating systems that are listed in the Security Software Containers table are:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Editions</th>
<th>Service Pack</th>
<th>32 or 64-bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows XP</td>
<td>Professional</td>
<td>SP3</td>
<td>32-bit</td>
</tr>
<tr>
<td>Windows 2003 Server</td>
<td>N/A</td>
<td>SP1¹, SP2</td>
<td>32-bit</td>
</tr>
<tr>
<td>Windows 2008 Server</td>
<td>N/A</td>
<td>SP1, SP2</td>
<td>32-bit, 64-bit²</td>
</tr>
<tr>
<td>Windows 7</td>
<td>Professional, Enterprise, Ultimate</td>
<td>N/A</td>
<td>32-bit, 64-bit</td>
</tr>
<tr>
<td>RedHat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RHEL 5.0</td>
<td></td>
<td>N/A</td>
<td>32-bit</td>
</tr>
<tr>
<td>RHEL 5.4</td>
<td>kernel 2.6.18</td>
<td>N/A</td>
<td>32-bit</td>
</tr>
</tbody>
</table>

Notes -
1. For Windows 2003 SP1, you must install the hotfix specified in Microsoft KB 906469 ([http://support.microsoft.com/kb/906469](http://support.microsoft.com/kb/906469)).
2. Windows 2008 Server 64-bit is supported for Security Management only.

Dedicated Gateways
These dedicated gateways cannot be upgraded to R75.10:
- Open Server - IPS-1 Sensor, VSX
- Appliances - DLP-1, UTM-1 Edge, IPS-1 Sensor, VSX-1
# Security Gateway Software Blades

<table>
<thead>
<tr>
<th>Software Blade</th>
<th>Operating System</th>
<th>Check Point</th>
<th>Microsoft</th>
<th>Crossbeam</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Firewall with Identity Awareness²</td>
<td>✓</td>
<td>✓³</td>
<td>✓³</td>
<td>✓</td>
</tr>
<tr>
<td>IPSec VPN</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IPS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mobile Access</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DLP⁴</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Control</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Anti-Virus &amp; Anti-Malware</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL Filtering</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-Spam &amp; Email Security</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Security</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Advanced Networking - QOS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Advanced Networking - Dynamic Routing and Multicast Support</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acceleration &amp; Clustering</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓⁴</td>
</tr>
</tbody>
</table>

### Notes about Security Gateway Software Blades

1. Identity Awareness supports connections to Microsoft Active Directory (AD) on Windows Server 2003 and 2008. Connections to AD on Windows Server 2000 are not supported.
2. IPSO supports identity enforcement and logging. For Identity Acquisition (AD Query, Identity Agents and Captive Portal) use a SecurePlatform gateway and share the identities with your IPSO gateways.
3. DLP is supported in High-Availability clusters, including Full HA.
   On UTM-1 130/270, you can either use DLP with Firewall and other Security Gateway software blades, or with Firewall and Security Management software blades.
   The DLP portal supports these web browsers: Internet Explorer 6, 7, 8; Firefox 3; Chrome 8; and Safari 5.
4. Only Clustering is supported on Windows. Acceleration is not supported.
5. Only third-party clustering is supported on Crossbeam.
# Security Management Software Blades

<table>
<thead>
<tr>
<th>Software Blade</th>
<th>Operating System</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Check Point</td>
<td>Microsoft</td>
<td>RedHat Linux</td>
<td>Solaris</td>
<td>Secure Platform</td>
<td>IPSO 6.2 Disk-based</td>
<td>Windows Server 2003</td>
<td>Windows Server 2008</td>
</tr>
<tr>
<td>Network Policy Management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Network Policy Management with Identity Awareness</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Endpoint Policy Management</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logging &amp; Status</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Monitoring</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Smart Provisioning</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management Portal*</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Directory</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart Workflow</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart Event</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart Reporter</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Management Portal is supported on the following Web browsers: Internet Explorer 7, and Mozilla Firefox 1.5 - 3.0
Clients and Consoles by Windows Platform

<table>
<thead>
<tr>
<th>Check Point Product</th>
<th>XP Home (SP3) 32-bit</th>
<th>XP Pro (SP3) 32-bit</th>
<th>Server 2003 (SP1-2) 32-bit</th>
<th>Vista (SP1) 32-bit</th>
<th>Vista (SP1) 64-bit</th>
<th>Server 2008 (SP1-2) 32-bit</th>
<th>Windows 7 Ultimate &amp; Enterprise 32-bit</th>
<th>Windows 7 Ultimate &amp; Enterprise 64-bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartConsole</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SmartDomain Manager</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SecureClient</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Endpoint Security VPN</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SSL Network Extender</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DLP UserCheck</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Identity Agent</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Note about Clients and Consoles

* Endpoint Security VPN and Identity Agent clients support all editions of Windows 7.

Minimum System Requirements

The system requirements for R75.10 are the same as those listed in the R75 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=11647).
### Required Disk Space

**Note** - It is safe to delete the downloaded .tgz file after it is extracted, to have 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>SecurePlatform/Linux</td>
<td>/var - 1.1 GB</td>
<td>/opt - 600 MB</td>
<td>root 460 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 200 MB</td>
<td>/opt - 280 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 200 MB</td>
<td>/var - 200 MB</td>
</tr>
<tr>
<td>IPSO Disk-based</td>
<td>/var - 540 MB</td>
<td>/opt - 400 MB</td>
<td>/opt - 150 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 100 MB</td>
<td>/var - 100 MB</td>
</tr>
<tr>
<td>Windows</td>
<td>450 MB</td>
<td>680 MB</td>
<td>520 MB</td>
</tr>
<tr>
<td>Solaris</td>
<td>/var - 450 MB</td>
<td>/opt - 380 MB</td>
<td>/opt - 210 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 300 MB</td>
<td>/var - 300 MB</td>
</tr>
</tbody>
</table>

* During installation, the process may use additional disk space that will be released when installation ends.

#### 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>SecurePlatform</td>
<td>/var - 1.1 GB</td>
<td>/opt - 700 MB</td>
<td>root - 340 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 200 MB</td>
<td>/opt - 220 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 50 MB</td>
<td>/var - 50 MB</td>
</tr>
<tr>
<td>IPSO Disk-based</td>
<td>/var 295 MB</td>
<td>/opt - 10 MB</td>
<td>/opt - 10 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var 285 MB</td>
<td>/var - 10 MB</td>
</tr>
<tr>
<td>IPSO Flash-based</td>
<td>/preserve - 270 MB</td>
<td>/preserve - 610 MB</td>
<td>/preserve - 320 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 270 MB</td>
<td>/var - 10 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/opt - 10 MB</td>
<td>/opt - 10 MB</td>
</tr>
<tr>
<td>Windows</td>
<td>450 MB</td>
<td>310 MB</td>
<td>220 MB</td>
</tr>
</tbody>
</table>

* During installation, the process may use additional disk space that will be released when installation ends.
### Build Numbers

This table contains the R75.10 software products updated in this release and their build numbers. To confirm that the hotfix is installed, run the version command for each product. If the command returns the build number listed, the hotfix is installed.

<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>979001061</td>
<td><code>fw ver -k</code>&lt;br&gt;This is Check Point VPN-1(TM) &amp; FireWall-1(R) R75.10 - Build 061&lt;br&gt;kernel: R75.10 - Build 061</td>
</tr>
<tr>
<td>Security Management</td>
<td>979001015</td>
<td><code>fwm ver</code>&lt;br&gt;This is Check Point Security Management Server R75.10 - Build 015</td>
</tr>
<tr>
<td>SmartConsole Applications</td>
<td>979001045</td>
<td><code>Help &gt; About Check Point &lt;Application Name&gt;</code>&lt;br&gt;R75.10 (Build 979001045)</td>
</tr>
<tr>
<td>Multi-Domain Server</td>
<td>979001015</td>
<td><code>fwm mds ver</code>&lt;br&gt;This is Check Point Multi-Domain Server R75.10 - Build 015</td>
</tr>
<tr>
<td>SmartDomain Manager</td>
<td>979001008</td>
<td><code>Help &gt; About Check Point SmartDomain Manager</code>&lt;br&gt;R75.10 (Build 979001008)</td>
</tr>
<tr>
<td>SecurePlatform</td>
<td>979001017</td>
<td><code>splat_ver</code></td>
</tr>
</tbody>
</table>
New Installation of R75.10

In This Section

New Installation of R75.10 15
Upgrading from R75 16
Installing the Client Applications 20
Uninstalling 21

Important - Check Point software versions R75.10 or higher require a valid Software Blades license. Users with NGX licenses will not be able to install the software. To learn how to migrate NGX licenses to Software Blades licenses, see Software Blade Migration (http://www.checkpoint.com/products/promo/software-blades/upgrade/index.html) or contact Account Services.

If you manage IPv6 or GX gateways from your management, you must regenerate your IPv6 and GX licenses in the User Center, to be compliant with Software Blades.

New Installation of R75.10

R75.10 is released as:

- an upgrade to version R75
- a clean installation for IPSO Flash-based appliances, including 1GB and 2GB Flash appliances (IP29x, IP39x and IP56x)

To install R75.10 on IPSO Flash-based Security Gateway with CLI:

1. Run: `newpkg`
2. Type the number (1 - 3) for the FTP server or local path where the TGZ is.
3. Enter the IP address, credentials, and pathnames when prompted.
4. Type `y` to download the TGZ. The file is downloaded and installation starts.
5. When prompted for installation type, type `1` to select Install this as a new package. R75.10 is installed under `/opt`.

To install R75.10 on IPSO Flash-based Security Gateway with manual download:

1. Download this installation file from the Check Point Support Center: Check_Point_R75_10_for_1G_Flash_IPSO6_2.tgz
2. Install the package:
   - **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_10_for_1G_Flash_IPSO6_2.tgz
   ```

To install R75.10 Security Gateway on all other platforms:

2. After you successfully install R75, install the upgrade package for your platform ("Upgrading from R75" on page 16).
Upgrading from R75

This section includes the procedures for installing R75.10 on management servers, gateways and log servers that already have R75 or higher installed.

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

Included Topics

- Upgrade Packages
- Upgrading with the SecurePlatform Web User Interface
- Upgrading with the Command Line
- Upgrading with SmartUpdate

Upgrade Packages

Before upgrading to R75.10, download the upgrade package for your platform from the Check Point Support Center:

<table>
<thead>
<tr>
<th>Platform and Upgrade Package</th>
<th>Upgrade Procedure</th>
</tr>
</thead>
</table>
| SecurePlatform and Linux (Open Servers and Appliances) | • SecurePlatform Web User Interface  
• Command Line  
• SmartUpdate |
| Check_Point_R75.10.linux.tgz | |
| IPSO 6.2 Disk-based | • Command Line  
• SmartUpdate |
| Check_Point_R75.10.ipso6_2.tgz | |
| IPSO 6.2 Flash-based (*) | • Command Line for IPSO Flash-Based  
• SmartUpdate |
| Check_Point_R75.10.ipso6_2_Flash.tgz | |
| Windows | • Command Line  
• SmartUpdate |
| Check_Point_R75.10.Windows.tgz | |
| Solaris | Command Line |
| Check_Point_R75.10.Solaris.tgz | |

* This upgrade package is only for appliances with 4GB Flash (IP69x, IP128x and IP245x). For appliances with 1GB and 2GB Flash (IP29x, IP39x and IP56x), you must do a clean install ("New Installation of R75.10" on page 15).
Upgrading with the SecurePlatform Web User Interface

You can install R75.10 on SecurePlatform Security Gateways and Security Management open servers and appliances using the Web User Interface.

⚠️ Important - Safe Upgrade is not supported from R75 to R75.10. Make a manual snapshot of the machine before you upgrade.

To install R75.10 using the Web User Interface:
1. Make sure all GUI applications are closed.
2. Download the upgrade package for your platform ("Upgrade Packages" on page 16).
3. Connect to the SecurePlatform 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 device automatically reboots.
8. Re-login to the machine.

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

To uninstall afterwards, revert to the snapshot manually.

Upgrading with the Command Line

You can use these instructions to install R75.10 using the CLI on open servers and IP series appliances, except for IPSO Flash-based appliances. To install on IPSO flash-based appliances, you must use the CLI instructions for IPSO flash-based appliances.

To install on Check Point appliances with SecurePlatform, use the Web User Interface or SmartUpdate.

- To install on IPSO platforms, use the command line. Network Voyager is not supported.
- You can safely delete the .tgz file after you extract the package (step 6).

To install R75.10 using the CLI:
1. Log onto the target machine.
2. If you are installing on SecurePlatform:
   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.
3. Verify that the target computer contains sufficient free disk space ("Required Disk Space" on page 13).
4. Create a temporary directory in the /var partition on non-Windows platforms, or in the c:\ partition on Windows platforms.
5. Copy the upgrade package for your platform ("Upgrade Packages" on page 16) to the temporary directory using SFTP, SCP, or other secure method.
6. Navigate 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.
7. Start the installation routine:

   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 also recommend that you backup the system by executing mds_backup command before
   installation.

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

8. Follow the instructions on the screen to install the appropriate components. Only those 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 the
word 'Succeeded'.

9. When prompted, reboot the computer.

10. Repeat the above steps for all management servers, log servers and gateways as required by your
deployment.

11. After completing the installation on all computers, install the security policy on gateways and servers as
appropriate.

**Upgrading with the Command Line for IPSO Flash-Based**

**Notes**
- IPSO Flash-based platforms are supported for use as Security Gateways only.
- Installation using Network Voyager is not supported and may result in system
instability. You must install this version using the CLI only.
- Only use this upgrade procedure for appliances with 4GB Flash (IP69x, IP128x
and IP245x). For appliances with 1GB and 2GB Flash (IP29x, IP39x and IP56x),
you must do a clean install ("New Installation of R75.10" on page 15).

**Before installing on an IPSO Flash-based Appliance:**

1. Delete any Check Point packages that are earlier than R75, and then delete any previous tgz files. You
can do this using Network Voyager or using the command shell:
   Using Network Voyager:
   a) Choose Configuration > System Configuration > Packages > Delete Packages.
   b) Select a previous installation package to delete, and click Apply.
   c) Delete the any tgz files.
   d) Click Apply.
   Using the command shell, run the following commands:
   ```
   newpkg -q
   newpkg -u <previous package name>
   rm opt/packages/<previous tgz name>
   newpkg -q prints a list of the installed packages.
   ```
2. If there is an IPSO image on the machine that is not in use, delete it using Network Voyager:
   a) Choose Configuration > System Configuration > images > Manage Images.
   b) Click Delete IPSO Images.
   c) Select the IPSO image to delete, and click Apply.
3. Verify that there is enough free disk space for the installation of the packages. ("Required Disk Space"
on page 13)
To install and activate this version on an IPSO Flash-based Appliance:

1. Using the command shell, copy the upgrade package for IPSO Flash-based appliances ("Upgrade Packages" on page 16) to /var/tmp on the IP Appliance through ftp.

   Note - The installation package must be located in the /var/tmp directory.

2. Navigate to the /var/tmp directory.

3. Extract the tgz package by running:
   
   ```bash
   tar -zxvf <file name>
   ``

4. Delete the tgz package by running:
   
   ```bash
   rm -rf <file name>
   ```

5. Run
   
   ```bash
   ./UnixInstallScript
   ```

6. Follow the instructions on the screen to install the appropriate components. When prompted, stop all Check Point processes.
   
   Only those 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 the word 'Succeeded'.

7. When prompted, reboot the computer by pressing y.

**Upgrading with SmartUpdate**

You can use SmartUpdate to remotely install this version on Security Gateways installed on all supported platforms.

To install with SmartUpdate:

1. Install the upgrade package for your platform ("Upgrade Packages" on page 16) on the Security Management Server using the Command Line ("Upgrading with the Command Line" on page 17).

2. Open SmartUpdate and close SmartDashboard.

3. Click Packages > Get Data from All.
   
   When the Operation Status of the known gateways is Done, the installed packages and their versions are listed.


5. Add the installation package file (*.tgz) for each required gateway platform to the Package Repository (Packages > Add; or drag-and-drop).
   
   Wait until the Operation Status of adding the package is Done. The packages appear in the Package Repository. This may take a few minutes.

6. Right-click the package and choose Distribute.

7. From the Distribute Package window, select the devices on which you want to install this version.

8. Click Distribute.

   The installation package is distributed to and installed on the selected Security Gateways. The Security Gateways are rebooted automatically, except for those that are installed on Windows. You must manually reboot Security Gateways installed on Windows.

   Note - On a Windows platform, if the gateway does not accept traffic after installing this version, re-install the policy.
Installing the Client Applications

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

To manually install the SmartConsole:
1. Download Check_Point_SmartConsole_R75.10_Windows.exe.
2. Double-click the file to install the SmartConsole.

To install the Multi-Domain Security Management SmartDomain Manager:
1. Download Check_Point_SmartDomain_Manager_R75.10_Windows.exe.
2. Double-click the file to install the SmartDomain Manager.
Uninstalling

Notes -
- Uninstallation from IPSO flash-based appliances is not supported.
- Uninstallation of IPS pattern granularity is not supported. After uninstall of R75.10, the patterns remain converted to protections.

To uninstall R75.10 in Security Management Server deployments:
1. Disable the IPS Event Analysis and/or SmartWorkflow Software Blades. If you already disabled them before upgrading to R75.10, you do not need to disable the Software Blades.
   To do this, disable the Software Blades in the Security Management server's object.
2. On each management server and dedicated log server:
   - All non-Windows platforms:
     Run: /opt/CPUninstall/R75.10/UnixUninstallScript
   - Windows platforms:
     (i) Go to: C:\Program files\CheckPoint\CPUninstall\R75.10
     (ii) Run: Uninstall.bat

To uninstall R75.10 in Multi-Domain Security Management deployments:
1. Disable the R75.10 from each CMA as follows:
   a) Login to the Multi-Domain Security Management MDG.
   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/R75.10/UnixUninstallScript
3. Activate Software Blades that were active before the upgrade to R75.10.

   Note - After uninstalling this release from a SecurePlatform machine, the command line login prompt and the Web interface Welcome screen will still display Check Point SecurePlatform R75.10 as the installed version. This is because packages related to the SecurePlatform operating system are not uninstalled during the uninstallation process. Use the fw ver command to see the current version of your software.

To uninstall with SmartUpdate:
You can use SmartUpdate to remotely uninstall on gateways of all platforms, except IPSO.
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 R75.10 and select Uninstall, in this order:
   - Security Gateway
   - Mobile Access (for SecurePlatform gateways, if installed)
   - all other Minor_Version products

   Note - All packages must be uninstalled except for the SecurePlatform package that cannot be uninstalled from SecurePlatform gateways.
5. On Windows platforms, reboot manually.
**fwm getpcap Command**

If you view Check Point logs with third-party software, you can use `fwm getpcap` to get packet capture data from the Security Gateway. Each log that has packet capture data includes a packet capture ID. You use this ID in `fwm getpcap` to get the packet capture data.

### fwm getpcap

**Description**
gets packet capture data from the Security Gateway

**Syntax**
```
fwm getpcap -g <Gateway> -u '{<CAP_ID>}' [-p <OUT_PATH>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Gateway&gt;</td>
<td>the object name or IP address of the gateway that captured the data</td>
</tr>
<tr>
<td>&lt;CAP_ID&gt;</td>
<td>the capture ID that is included in the log</td>
</tr>
<tr>
<td>&lt;OUT_PATH&gt;</td>
<td>(optional) the location to save the packet capture data</td>
</tr>
</tbody>
</table>

**Example**
```
fwm getpcap -g 192.168.162.1 -u '{0x4d79dc02,0x10000,0x220da8c0,0x1ffffff}'
```

To get the packet capture data from the Security Gateway:

1. Log on to a Log server.
   In Multi-Domain Security Management, use `mds_env` to enter the CMA environment of the log server.
2. Run: `fwm getpcap -g <Gateway> -u '{<CAP_ID>}'`
   By default, the packet capture is saved in the local directory.