Important Information

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=11238

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

⚠️ Important - Check Point recommends that customers remain up-to-date with the latest
minor releases, as they contain important functional and stability fixes, security
enhancements and protection against new and evolving attacks.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>19 January 2011</td>
<td>Improved formatting and document layout</td>
</tr>
<tr>
<td>29 December 2010</td>
<td>Updated: To upgrade from R70.40 to R71.20, refer to sk59481 (<a href="http://supportcontent.checkpoint.com/solutions?id=sk59481">http://supportcontent.checkpoint.com/solutions?id=sk59481</a>).</td>
</tr>
<tr>
<td>17 October 2010</td>
<td>Updated Upgrading to R71.20 from Versions Lower than R71 (on page 13) to include upgrade from R71</td>
</tr>
<tr>
<td>13 October 2010</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 R71.20 Release Notes).
Important Information ................................................................. 3
Introduction to R71.20 ................................................................... 5
What’s New in R71.20 ................................................................... 5
  Previous Releases Included in R71.20 ........................................... 5
Platform Provisions and Requirements ......................................... 6
  Supported Upgrade Paths ............................................................ 6
  Supported Security Products by Platform .................................... 7
    Security Software Containers by Platform .................................. 7
    Security Gateway Software Blades by Platform ......................... 8
    Security Management Software Blades by Platform .................... 9
  Clients and Consoles by Windows Platform ................................. 10
  Minimum System Requirements .................................................. 10
  Required Disk Space .................................................................. 11
  Build Numbers .......................................................................... 12
Installing R71.20 ......................................................................... 13
  New Installation of R71.20 ........................................................... 13
  Upgrading to R71.20 from Versions Lower than R71 ...................... 13
  Upgrading to R71.20 from R71 and Higher .................................. 14
    R71.20 Upgrade Packages ....................................................... 14
    Upgrading with the SecurePlatform Web User Interface ............. 15
    Upgrading with the Command Line .......................................... 15
    Upgrading with SmartUpdate .................................................. 17
  Installing the Client Applications ................................................. 18
Uninstalling R71.20 ..................................................................... 19
Resolved Issues and Known Limitations ....................................... 20
  Resolved Issues ........................................................................ 20
  Known Limitations .................................................................... 20
Introduction to R71.20

Thank you for updating to Check Point version R71.20. This version contains new features and resolves various issues for Check Point Software Blades.
Please read this document carefully before installing R71.20.

What's New in R71.20

- Central management for Series 80 Appliances
- Installation of Security Management Server on Microsoft Windows 7
- Central management for UTM-1 Edge N Series and Embedded NGX 8.1 gateways
- Provisioning of IPSO 6.2 IP appliances using SmartProvisioning
- Enhanced vsx_util command for improved user experience and additional functionality

Previous Releases Included in R71.20

This release include all features and fixes that were included in R71.10 and R70.40. For more information, see:

- R71.10 Release Notes (http://supportcontent.checkpoint.com/documentation_download?id=10909)
- R70.40 Release Notes (http://supportcontent.checkpoint.com/documentation_download?id=10770)
Platform Provisions and Requirements

In This Section

Supported Upgrade Paths 6
Supported Security Products by Platform 7
Clients and Consoles by Windows Platform 10
Minimum System Requirements 10
Required Disk Space 11
Build Numbers 12

Supported Upgrade Paths

R71.20 can be installed on top of R71 or R71.10 Security Gateways, Security Management servers, and Provider-1 MDSs.

To upgrade from NGX R65 or R70 to R71.20, you must first upgrade to version R71.10. For upgrade instructions, refer to the R71.10 Release Notes (http://supportcontent.checkpoint.com/documentation_download?id=10909).

Notes -

- To upgrade from R70.40 to R71.20, refer to sk59481 (http://supportcontent.checkpoint.com/solutions?id=sk59481).
- To upgrade Check Point Suite Products before version NGX R65 to R71.20, you must first upgrade your system to NGX R65.
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 by Platform

<table>
<thead>
<tr>
<th>Software Blade</th>
<th>Platform and Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Check Point</td>
</tr>
<tr>
<td></td>
<td>Windows</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
</tr>
<tr>
<td></td>
<td>Crossbeam</td>
</tr>
<tr>
<td></td>
<td>Solaris¹</td>
</tr>
<tr>
<td>Secure Platform</td>
<td>IP SO 6.2 Disk-based</td>
</tr>
<tr>
<td>IPSO 6.2</td>
<td></td>
</tr>
<tr>
<td>Flash-based</td>
<td></td>
</tr>
<tr>
<td>Server 2003/2008 (SP1-2) 32bit</td>
<td></td>
</tr>
<tr>
<td>7 Professional Enterprise Ultimate 32bit/64bit</td>
<td></td>
</tr>
<tr>
<td>RHEL 5.0</td>
<td></td>
</tr>
<tr>
<td>RHEL 5.4 kernel 2.6.18 32bit</td>
<td></td>
</tr>
<tr>
<td>X-series</td>
<td></td>
</tr>
<tr>
<td>Ultra-SPARC 8, 9, 10</td>
<td></td>
</tr>
<tr>
<td>Security Management</td>
<td>✓</td>
</tr>
<tr>
<td>Security Gateway</td>
<td>✓</td>
</tr>
<tr>
<td>Provider-1 MDS</td>
<td>✓</td>
</tr>
</tbody>
</table>

Notes for Security Software Containers -

1. We recommend that you install Provider-1 on Sun M-Series servers. We do not recommend that you install Provider-1 on Sun T-Series servers.

Supported Appliances

<table>
<thead>
<tr>
<th>Appliance Name</th>
<th>Security Management</th>
<th>Provider-1 MDS</th>
<th>Security Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart-1</td>
<td>✓</td>
<td>✓ (Models 5, 25, 50)</td>
<td>✓ (Models 50, 150)</td>
</tr>
<tr>
<td>Power-1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>UTM-1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IP Series Disk-based</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IP Series Flash-Based</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Dedicated Gateways

These dedicated gateways cannot be upgraded to R71.20:

- Open Server - DLP, IPS-1 Sensor, VSX
- Appliances - DLP-1, UTM-1 Edge, IPS-1 Sensor, VSX-1
## Security Gateway Software Blades by Platform

<table>
<thead>
<tr>
<th>Software Blade</th>
<th>Platform and Operating System</th>
<th>Check Point</th>
<th>Windows</th>
<th>Crossbeam</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Secure Platform</td>
<td>IPSO 6.2 Disk-based</td>
<td>IPSO 6.2 Flash-based</td>
<td>Server 2003/2008 (SP1-2) 32bit</td>
</tr>
<tr>
<td>Firewall</td>
<td>✓</td>
<td>✓</td>
<td>✓</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>SSL VPN</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DLP</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</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Acceleration &amp; Clustering¹</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓²</td>
</tr>
</tbody>
</table>

**Notes**

1. The maximum number of supported cluster members in ClusterXL mode is five; in third-party mode the maximum is eight.
2. Only Clustering is supported in Windows. Acceleration is not supported.
3. Only third-party clustering is supported.
## Security Management Software Blades by Platform

<table>
<thead>
<tr>
<th>Software Blade</th>
<th>Platform and Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Check Point</td>
</tr>
<tr>
<td>Secure Platform</td>
<td></td>
</tr>
<tr>
<td>IPSO 6.2 Disk-based</td>
<td></td>
</tr>
<tr>
<td>Server 2003/2008 (SP1-2) 32bit</td>
<td></td>
</tr>
<tr>
<td>7 Professional Enterprise Ultimate 32bit/64bit</td>
<td></td>
</tr>
<tr>
<td>RHEL 5.0 RHEL 5.4 kernel 2.6.18 32bit</td>
<td></td>
</tr>
<tr>
<td>Ultra-SPARC 8, 9, 10</td>
<td></td>
</tr>
<tr>
<td>Network Policy Management</td>
<td>✓</td>
</tr>
<tr>
<td>Endpoint Policy Management</td>
<td>✓</td>
</tr>
<tr>
<td>Logging &amp; Status</td>
<td>✓</td>
</tr>
<tr>
<td>Monitoring</td>
<td>✓</td>
</tr>
<tr>
<td>SmartProvisioning</td>
<td>✓</td>
</tr>
<tr>
<td>Management Portal*</td>
<td>✓</td>
</tr>
<tr>
<td>User Directory</td>
<td>✓</td>
</tr>
<tr>
<td>SmartWorkflow</td>
<td>✓</td>
</tr>
<tr>
<td>SmartEvent</td>
<td>✓</td>
</tr>
<tr>
<td>SmartReporter</td>
<td>✓</td>
</tr>
</tbody>
</table>

* Management Portal is supported on the following Web browsers: Internet Explorer 6 and 7, and Mozilla Firefox 1.5 - 3.0
Clients and Consoles by Windows Platform

<table>
<thead>
<tr>
<th>Check Point Product</th>
<th>XP Pro (SP3)</th>
<th>XP Home (SP3)</th>
<th>Server 2003 (SP1-2) 32bit</th>
<th>Vista (SP1) 32bit</th>
<th>Vista (SP1) 64bit</th>
<th>Server 2008 (SP1-2) 32bit</th>
<th>7 Professional Enterprise Ultimate 32bit</th>
<th>7 Professional Enterprise Ultimate 64bit</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>Provider-1 MDG</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>SSL Network Extender</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Endpoint Security Client</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Endpoint Connect Client</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>
</tbody>
</table>

Minimum System Requirements

The system requirements for R71.20 are the same as those listed in the R71 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=10330).
## Required Disk Space

***Note*** - It is safe to delete the downloaded .tgz file after it is extracted in order to allow more disk space for installation.

### Required Disk Space for Installation on a Security Management Server or MDS

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Packed and Extracted .tgz File</th>
<th>Installation Size</th>
<th>Total Space Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurePlatform</td>
<td>/var - 1.1 GB</td>
<td>root - 250 MB</td>
<td>root - 250 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/opt - 350 MB</td>
<td>/opt - 350 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 300 MB</td>
<td>/var - 1.4 GB</td>
</tr>
<tr>
<td>IPSO Disk-based</td>
<td>/var - 700 MB</td>
<td>/opt - 250 MB</td>
<td>/opt - 250 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 150 MB</td>
<td>/var - 850</td>
</tr>
<tr>
<td>Linux</td>
<td>1.1 GB</td>
<td>450 MB</td>
<td>1.55 GB</td>
</tr>
<tr>
<td>Windows</td>
<td>700 MB</td>
<td>600 MB</td>
<td>1.3 GB</td>
</tr>
<tr>
<td>Solaris</td>
<td>950 MB</td>
<td>400 MB</td>
<td>1.35 GB</td>
</tr>
</tbody>
</table>

### Required Disk Space for Installation on a Security Gateway

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Packed and Extracted .tgz File</th>
<th>Installation Size</th>
<th>Total Space Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurePlatform</td>
<td>/var - 1.1 GB</td>
<td>root - 200 MB</td>
<td>root - 200 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/opt - 300 MB</td>
<td>/opt - 300 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 300 MB</td>
<td>/var - 1.4 GB</td>
</tr>
<tr>
<td>IPSO Disk-based</td>
<td>/var - 700 MB</td>
<td>/opt - 200 MB</td>
<td>/opt - 200 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 150 MB</td>
<td>/var - 850 MB</td>
</tr>
<tr>
<td>IPSO Flash-based</td>
<td>/preserve - 400 MB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>650 MB</td>
<td>250 MB</td>
<td>900 MB</td>
</tr>
</tbody>
</table>
Build Numbers

The following table lists the R71.20 software products available in this release, and their build numbers. To verify each product's build number, use the given command format or direction within the GUI.

Take 55 of R71.20 consists of the following builds:

<table>
<thead>
<tr>
<th>Software Blade / Product</th>
<th>Build No.</th>
<th>Verifying Build No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Gateway</td>
<td>025</td>
<td>fw ver -k</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is Check Point VPN-1(TM) &amp; FireWall-1(R) R71.20 - Build 025</td>
</tr>
<tr>
<td>Security Management</td>
<td>009</td>
<td>fwm ver</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is Check Point Security Management Server R71.20 - Build 009</td>
</tr>
<tr>
<td>SmartConsole Applications</td>
<td>039</td>
<td>Help &gt; About Check Point &lt;Application Name&gt; R71.20 (Build 976620039)</td>
</tr>
<tr>
<td>Provider-1 Multi-Domain Server (MDS)</td>
<td>011</td>
<td>fwm mds ver</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is Check Point Provider-1 Server R71.20 - Build 011</td>
</tr>
<tr>
<td>Provider-1 Multi-Domain GUI (MDG)</td>
<td>010</td>
<td>Help &gt; About Check Point Provider-1 R71.20 (Build 976620010)</td>
</tr>
<tr>
<td>SecurePlatform</td>
<td>019</td>
<td>splat_ver</td>
</tr>
</tbody>
</table>
Installing R71.20

New Installation of R71.20

R71.20 is released as an upgrade to version R71 or higher and as a clean install for Windows 7.

To install R71.20 as a new installation on any management server, gateway or log server:

- For Windows 7 open servers, download the installation file from the Check Point Support Center:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Image/File Name</th>
</tr>
</thead>
</table>

Important -

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


- For all other platforms, you must first install version R71.10. For installation instructions, refer to the R71.10 Release Notes (http://supportcontent.checkpoint.com/documentation_download?id=10909). After you successfully install R71.10, install the upgrade package for your platform ("Upgrading to R71.20 from R71 and Higher" on page 14).

Upgrading to R71.20 from Versions Lower than R71

To upgrade from NGX R65 or R70 to R71.20, you must first upgrade to version R71.10 or R71. For upgrade instructions, refer to the R71.10 Release Notes (http://supportcontent.checkpoint.com/documentation_download?id=10909).

After you successfully upgrade to R71.10 or R71, install the upgrade package for your platform ("Upgrading to R71.20 from R71 and Higher" on page 14).

Note - To upgrade Check Point Suite Products before version NGX R65 to R71.20, you must first upgrade your system to NGX R65.
Upgrading to R71.20 from R71 and Higher

This section includes the procedures for installing R71.20 on management servers, gateways and log servers that already have R71 or higher installed.

We recommend that you backup your system before installing this release package. For SecurePlatform, you can use snapshots which are discussed in the Snapshot Image Management section of the R71 SecurePlatform Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=10313).

Included Topics

- R71.20 Upgrade Packages
- Upgrading with the SecurePlatform Web User Interface
- Upgrading with the Command Line
- Upgrading with SmartUpdate

R71.20 Upgrade Packages

Before upgrading from R71 or higher, download the upgrade package for your platform from the Check Point Support Center:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Upgrade Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSO 6.2 Disk-based</td>
<td>Check_Point_R71.20.ipso6_2.tgz (<a href="http://supportcenter.checkpoint.com/file_download?id=11635">http://supportcenter.checkpoint.com/file_download?id=11635</a>)</td>
</tr>
<tr>
<td>IPSO 6.2 Flash-based</td>
<td>Check_Point_R71.20.ipso6_2_Flash.tgz (<a href="http://supportcenter.checkpoint.com/file_download?id=11636">http://supportcenter.checkpoint.com/file_download?id=11636</a>)</td>
</tr>
</tbody>
</table>
Upgrading with the SecurePlatform Web User Interface

You can install R71.20 on SecurePlatform Security Gateways and Security Management open servers and appliances using the Web User Interface.

**To install R71.20 using the Web User Interface:**
1. Download the upgrade package for your platform ("R71.20 Upgrade Packages" on page 14).
2. Connect to the SecurePlatform Web User Interface:
   - Open server: https://<IP>
   - Appliance: https://<IP>:4434
3. Open the Upgrade page:
   - Open server: Device > Upgrade
   - Appliance: Appliance > Upgrade
4. In the Upgrade Steps pane, browse to the downloaded file.
5. Click the Upload package button.
6. In the Safe Upgrade step, make sure the Save a snapshot of the current system check box is selected.
   - Important - Make sure all GUI applications are closed and take a snapshot of the machine before you upgrade.
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.

Upgrading with the Command Line

You can use these instructions to install R71.20 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.

**Notes**
- To install on Check Point appliances with SecurePlatform, you must use the Web User Interface or SmartUpdate.
- Installation on IPSO platforms using Network Voyager is not supported. You must install using the CLI.

**To install R71.20 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 11).
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 ("R71.20 Upgrade Packages" on page 14) 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.
Note - You can safely delete the .tgz file once it has been extracted.

7. Start the installation routine:

   Important -
   Before installing on Provider-1, run:
   
   mdsenv
   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 any 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.

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

1. Delete any Check Point packages that are earlier than R71, 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 11)

**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 ("R71.20 Upgrade Packages" on page 14) to /var/tmp on the IP appliance through ftp.
   
   ![Note](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:
   
   ```
   tar -zxvf <file name>
   ```
4. Delete the tgz package by running:
   
   ```
   rm -rf <file name>
   ```
5. Run
   
   ```
   ./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 except for Solaris and Linux RHEL 5.0.

**To install with SmartUpdate:**

1. Install the upgrade package for your platform ("R71.20 Upgrade Packages" on page 14) on the Security Management Server using the Command Line ("Upgrading with the Command Line" on page 15).
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.
4. Open the Package Repository: **Packages > View Repository**.
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_R71.20_Windows.exe (http://supportcenter.checkpoint.com/file_download?id=11639).
2. Double-click the file to install the SmartConsole.

To install the Provider-1 MDG:
2. Double-click the file to install the Provider-1 MDG.
Uninstalling R71.20

---

**Note** - Uninstallation from IPSO flash-based appliances is not supported.

**To uninstall R71.20 in Security Management Server deployments:**

1. Disable the R71.20 IPS Event Analysis and/or SmartWorkflow Software Blades. If you already disabled them before upgrading to R71.20, 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/R71.20/UnixUninstallScript`
   - **Windows platforms:**
     1. Go to: `C:\Program files\CheckPoint\CPUninstall\R71.20`
     2. Run: `Uninstall.bat`

**To uninstall R71.20 in Provider-1 deployments:**

1. Disable the R71.20 from each CMA as follows:
   a) Login to the Provider-1 MDG.
   b) In Versions & Blades Updates, right click and select Deactivate.

2. Run this command on each Provider-1 MDS, CLM and MLM:
   `/opt/CPUninstall/R71.20/UnixUninstallScript`

3. Activate Software Blades that were active before the upgrade to R71.20.

---

**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 R71.20 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 R71.20 and choose Uninstall in the following order:
   - **VPN-1 Power/UTM**
   - **SSL VPN** (for SecurePlatform gateways, if installed)

   **Note** - All packages must be Uninstalled except for the SecurePlatform package that cannot be Uninstalled from SecurePlatform gateways.

5. On Windows platforms, reboot manually.

---
Resolved Issues and Known Limitations

Resolved Issues

Resolved Issues in R71.20 are in sk54961 (http://supportcontent.checkpoint.com/solutions?id=sk54961).

Known Limitations

Known Limitations for R71.20 are in sk54960 (http://supportcontent.checkpoint.com/solutions?id=sk54960).