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=12742
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>16 October 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 R70.50  Release Notes).
Introduction

Thank you for updating to Check Point version R70.50. This release contains new features and resolves various issues for Check Point Software Blades. Please read this document carefully before installing R70.50.

Previous Releases Included in R70.50

This release includes all features and fixes that were included in R70.40 R70.30, R70.20 and R70.1. For more information, see:

- R70.40 Home Page (http://supportcontent.checkpoint.com/solutions?id=sk52181)
- R70.30 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=10694)
- R70.20 Home Page (http://supportcontent.checkpoint.com/solutions?id=sk43168)
- R70.1 Home Page (http://supportcontent.checkpoint.com/solutions?id=sk41810)

Known Limitations and Resolved Issues

- Known Limitations (http://supportcontent.checkpoint.com/solutions?id=sk65069)
- Resolved Issues (http://supportcontent.checkpoint.com/solutions?id=sk65070)

For more information about R70.50 and to download the software, go to the R70.50 Home Page (http://supportcontent.checkpoint.com/solutions?id=sk65068).

What's New

- Stability and performance enhancements.
- VPN Client.
  This version now supports Remote Access Clients E75 series:
  - Endpoint Security VPN R75/E75.10 and above, which replaces SecureClient and Endpoint Connect.
  - Check Point Mobile for Windows E75.10 and above.
  - SecuRemote E75.10 and above.
- UTM-1 Edge 8.2 gateway support.
- Pre-shared secret authentication method for R75 remote access clients.

Upgrade Paths

Upgrade Security Gateway, Security Management server or Provider-1 MDS of these releases:

- R70
- R70.1
- R70.20
- R70.30
- R70.40

If you are using an earlier release, you must first upgrade to R70 before installing this release.
## Supported Security Products by Platform

### Supported Security Gateway Software Blades

<table>
<thead>
<tr>
<th></th>
<th>Check Point</th>
<th>Windows</th>
<th>Crossbeam</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Secure Platform</td>
<td>Secure Platform Embedded</td>
<td>IPSO 6.2 Disk</td>
</tr>
<tr>
<td>Firewall</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>IPSec VPN</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>IPS</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Anti-Virus &amp; Anti-Malware</td>
<td>+</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>URL Filtering</td>
<td>+</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Anti-Spam &amp; Email Security</td>
<td>+</td>
<td>(4)</td>
<td></td>
</tr>
<tr>
<td>Web Security</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Advanced Networking</td>
<td>+</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Acceleration &amp; Clustering (1)</td>
<td>+</td>
<td>(5)</td>
<td>+</td>
</tr>
</tbody>
</table>

**Note** -

1. The maximum number of cluster members in the ClusterXL mode is five. In the third-party mode, the maximum is eight.
2. Clusters are supported on Windows platforms. Acceleration is not supported.
3. Only third-party clusters are supported.
4. Based on IP reputation
5. High Availability only
### Supported Security Management Software Blades

<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>Secure Platform</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>Event Correlation (Eventia Analyzer), Reporting and IPS Event Analysis</td>
<td>+</td>
</tr>
</tbody>
</table>

### Provider-1 Support

<table>
<thead>
<tr>
<th>Product</th>
<th>Platform and Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Secure Platform</td>
</tr>
<tr>
<td>Provider-1 Server (MDS)</td>
<td>+</td>
</tr>
</tbody>
</table>

**Note** - 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.
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>Windows 7 Pro Enterprise Ultimate 32bit</th>
<th>Windows 7 Pro Enterprise Ultimate 64bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartConsole</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td>SP1 Only</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Provider-1 MDG</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td>SP1 Only</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>SecureClient</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>SecureClient</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>SecureClient</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>SecureClient</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint Connect</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint Security VPN client (R75)</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Access VPN clients (E75.10 and above)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Important** - These Endpoint Security clients cannot connect to a SecurePlatform gateway when the WebUI is configured to use port 443:
- SecureClient (Visitor mode only)
- Endpoint Connect
- Endpoint Security VPN client (R75)
- Remote Access VPN clients (E75.10 and above)

You must configure the SecurePlatform WebUI to use a different port for management connections when using Endpoint Security clients.

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>Security Gateway Series 80</td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Smart-1</td>
<td>(Models 5, 25, 50)</td>
<td>(Models 50, 150)</td>
<td></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>
Minimum System Requirements

The system requirements for R70.50 are the same as for R70. See the R70 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=8712) for more information.

Disk Space Requirements

### Required Disk Space - Security Management server or MDS

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Packed &amp; Extracted .tgz File</th>
<th>Final Installation Size</th>
<th>Total Space Required During Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSO Disk-based</td>
<td>/var - 400 MB</td>
<td>/opt - 150 MB /var - 100 MB</td>
<td>/opt - 200 MB /var - 200 MB</td>
</tr>
<tr>
<td>Linux</td>
<td>/var 875 MB</td>
<td>root - 4 MB /opt - 445 MB /var - 300 MB</td>
<td>root - 97 MB /opt - 530 MB /var - 300 MB</td>
</tr>
<tr>
<td>Windows (HFA only)</td>
<td>485 MB</td>
<td>690 MB</td>
<td>685 MB</td>
</tr>
<tr>
<td>Solaris</td>
<td>/var 600 MB</td>
<td>/opt 240 MB /var 100 MB</td>
<td>/opt 285 MB /var 100 MB</td>
</tr>
</tbody>
</table>

### Required Disk Space - Security Gateway

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Packed &amp; Extracted .tgz File</th>
<th>Final Installation Size</th>
<th>Total Space Required During Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSO Disk-based</td>
<td>/var - 400 MB</td>
<td>/opt - 105 MB /var - 0 MB</td>
<td>/opt - 200 MB /var - 100 MB</td>
</tr>
<tr>
<td>IPSO Flash-based</td>
<td>/var - 209 MB</td>
<td>root - 0 MB /opt - 25 MB /var - 0 MB</td>
<td>root - 300 MB /opt - 25 MB /var - 6 MB</td>
</tr>
<tr>
<td>Windows</td>
<td>485 MB</td>
<td>232 MB</td>
<td>363 MB</td>
</tr>
</tbody>
</table>

**Note** - Delete the downloaded .tgz file after extraction to have more disk space for installation.
## Build Numbers

These are the software products, and their build numbers, in this release.

<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>730640028</td>
<td>fw ver</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is Check Point VPN-1(TM) &amp; FireWall-1(R) R70.50 - Build 028</td>
</tr>
<tr>
<td>Security Management</td>
<td>730640003</td>
<td>fwm ver</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is Check Point Security Management Server R70.50 - Build 003</td>
</tr>
<tr>
<td>SmartConsole Applications</td>
<td>730640017</td>
<td>Help &gt; About Check Point &lt;Product&gt; R70.50 (Build 730640017)</td>
</tr>
<tr>
<td>Provider-1 Multi-Domain Server (MDS)</td>
<td>730640005</td>
<td>fwm mds ver</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is Check Point Provider-1 Server R70.50 - Build 005</td>
</tr>
<tr>
<td>Provider-1 Multi-Domain Server (MDG)</td>
<td>730640007</td>
<td>Help &gt; About Check Point Provider-1 R70.50 (Build 730640007)</td>
</tr>
<tr>
<td>SecurePlatform</td>
<td>730640008</td>
<td>ver</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is Check Point SecurePlatform R70.50 Build 008</td>
</tr>
</tbody>
</table>
Installing

R70.50 is an upgrade to versions R70.X. If you are installing a new deployment, first install version R70 as described in the R70 Installation and Upgrade Guide (http://supportcontent.checkpoint.com/documentation_download?ID=8753). We recommend that you also install Eventia Suite R70.

After you install R70, install the release package as an upgrade from R70 to R70.50.

Installing the Client Applications

You must manually download the updated SmartConsole clients from the Check Point Support Center.

To install the SmartConsole:
1. Get Check_Point_R70.50_SmartConsole.Windows.exe from the Download Center (http://supportcontent.checkpoint.com/solutions?id=sk65068).
2. Double-click the file to install the SmartConsole.

To get to the Eventia clients from the SmartDashboard, select Window and then choose IPS Event Analysis, Eventia Reporter or Eventia Analyzer.


To install the Provider-1 MDG:
1. Get Check_Point_R70.50_MDG.Windows.exe from the Download Center (http://supportcontent.checkpoint.com/solutions?id=sk65068).
2. Double-click the file to install the Provider-1 MDG.

Upgrading to R70.50 from R70

This section contains procedures for upgrading Security Gateways and management servers to R70.50.

- If you do not have version R70 or higher installed, first install R70 or upgrade to R70. The clean installation procedures are in the R70 Installation and Upgrade Guide (http://supportcontent.checkpoint.com/documentation_download?ID=8753).

- If you installed R70 without the Eventia Suite, you do not have to install it at this time. The R70.50 installation package installs the Eventia applications automatically. Enable and configure the Eventia Suite components. For details, see the R70.30 Installation and Upgrade Guide (http://supportcontent.checkpoint.com/documentation_download?ID=10658).


We recommend that you backup your system before installing this release. For SecurePlatform, you can use snapshots for backup purposes. See the Snapshot Image Management section of the R70 SecurePlatform/SecurePlatform Pro Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=8744).

Updating Customized INSPECT Files

The management server contains some INSPECT (*.def) files, typically located in the $FWDIR/lib directory. This release includes one or more updated INSPECT files, which replace the INSPECT files currently in
use. If your deployment only uses original Check Point INSPECT files, the updated INSPECT files install without user intervention.

If your deployment contains some customized INSPECT files, none of the new INSPECT files replace the old ones. The following message appears:

The updated inspect files were NOT installed due to signature mismatches or errors.  
To complete the installation replace the inspect files.  
Inspect files that were not replaced may lead to unexpected behavior!  
To force update of the inspect files run: update_inspect_files -f

If the INSPECT files are not replaced (signature mismatch message displayed), you must update all INSPECT files, even if the files were manually customized.

Important - You must replace the previous versions of the INSPECT files. If you fail to do so, unexpected behavior may result.

To update all INSPECT files:
1. Examine your customized INSPECT files. To see which INSPECT files were not replaced, refer to the logs:
   - Unix - /opt/CPInstLog/update_inspect_files_R70.50.log
   - Windows - C:\Program Files\CheckPoint\CPInstLog\update_inspect_files_R70.50.log
   If the files were not replaced due to manual customization, the log shows:
     <filename>.def was changed by user, signature didn't match!
2. Open the files listed in update_inspect_files_R70.50.log. Find the customized lines.
3. Run update_inspect_files -f. The log shows that <filename>.def was replaced.
4. Merge your customized content (as shown in the previous steps) into the new INSPECT file(s).
5. Re-install the Security Policy to activate the new INSPECT files.

R70.50 Upgrade Packages

Before upgrading from R70 or higher, download the upgrade package for your platform from the Check Point Support Center (http://supportcontent.checkpoint.com/solutions?id=sk65068):

<table>
<thead>
<tr>
<th>Platform</th>
<th>Upgrade Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurePlatform, Power-1, UTM-1, Smart-1 and Linux</td>
<td>Check_Point_R70.50_Upgrade.Splat.tgz</td>
</tr>
<tr>
<td>IPSO 6.2 - Disk-based</td>
<td>Check_Point_R70.50_Upgrade.IPSO6_2.tgz</td>
</tr>
<tr>
<td>IPSO 6.2 - Flash-based</td>
<td>Check_Point_R70.50_Upgrade.IPSO6_2_Flash.tgz</td>
</tr>
<tr>
<td>Windows</td>
<td>Check_Point_R70.50_Upgrade.Windows.tgz</td>
</tr>
<tr>
<td>Solaris Security Management</td>
<td>Check_Point_R70.50_Upgrade.Solaris.tgz</td>
</tr>
</tbody>
</table>

Upgrading with the Web User Interface

You can install R70.50 on SecurePlatform Security Gateways, Security Management open servers, and appliances using the Web User Interface.

To install R70.50 using the Web User Interface:
1. Download the upgrade package for your platform.
2. Connect to the SecurePlatform Web User Interface:
   - Open server: https://<IP>
   - Appliance: https://<IP>:443
3. Go to the **Upgrade** page:
   - Open server: **Device > Upgrade**
   - Appliance: **Appliance > Upgrade**
4. In the **Upgrade Steps** pane, select a file.
5. Click **Upload package**.
6. Save a snapshot or image.
   - Open server: In the Safe Upgrade window, make sure the **Save a snapshot of the current system** option is selected.
   - **Important** - Make sure that all GUI applications are closed. Take a snapshot of the computer before you upgrade.
   - Appliance: In the Save an Image before Upgrade window, make sure the **Save an image of the current running system before the upgrade option** is selected.
7. On open servers, click **Start Upgrade**.
   When the installation program completes, the device automatically reboots.
8. Log in to the computer.
   - **Important** - After upgrading, move the snapshot file from the Windows Desktop to a folder with a name that does not contain spaces. You must do this before you can restore the computer.

### Upgrading with the CLI

You can use these instructions to install R70.50 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 R70.50 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.
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 to the temporary directory using SFTP, SCP, or another secure utility.
6. Go to the temporary directory and extract the .tgz package.
   - On non-Windows platforms, run: `gzip -zxvf <file name>`
   - On Windows platforms, use an archive utility such as WinZip.
7. Start the installation routine:
   - **Important** - Before installing on Provider-1, run `mdsenv` and then `mdsstop`. If this is not done, the system will experience functionality issues.
   - We 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. Do the instructions on the screen to install the applicable 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 you complete the installation on all computers, install the security policy on gateways and servers as appropriate.

### CLI Installation for IPSO Flash-Based Appliances

**Notes**
- IPSO Flash-based platforms are supported for use as Security Gateways only.
- Installation using Network Voyager is not supported and can result in system instability. You must install this version using the CLI only.

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

1. Delete all Check Point packages earlier than R70, and then delete earlier release tgz files. You can do this with Network Voyager or with the command shell:
   - Using Network Voyager:
     a) Select **Configuration > System Configuration > Packages > Delete Packages**.
     b) Select the old installation packages, and then click **Apply**.
     c) Delete the old tgz files.
     d) Click **Apply**.
   - Using the command shell, run these 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 appliance that is not in use, delete it using Network Voyager:
   a) Select **Configuration > System Configuration > Images > Manage Images**.
   b) Click **Delete IPSO Images**.
   c) Select the IPSO image to delete, and click **Apply**.

3. Make sure that there is sufficient free disk space (*Disk Space Requirements* on page 9) for the installation of the packages:

**To install and activate this version on an IPSO Flash-based Appliance:**

1. Copy the upgrade package for IPSO Flash-based appliances to `/var/tmp` on the IP Appliance using FTP.
   **Note** - The installation package must be located in the `/var/tmp` directory.

2. Go 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 applicable components. When prompted, stop all Check Point processes.
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 on the Security Management Server using the Command Line ("Upgrading with the CLI" on page 13).
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 can 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.

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, press y to reboot the computer.
Uninstalling

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

To uninstall R70.50 from a Security Gateways or Security Management Server:
1. Disable the R70.50 IPS Event Analysis and/or SmartWorkflow Software Blades.
   To do this, disable the Software Blades in the Security Management server object.
2. If you want to revert to a version lower than R70.40, delete all Security Gateway 80 objects that were
   created in SmartDashboard.
3. On each management server and dedicated log server:
   - All non-Windows platforms:
     Run: /opt/CPUninstall/R70.50/UnixUninstallScript
   - Windows platforms:
     (i) Go to: C:\Program files\CheckPoint\CPUninstall\R70.50
     (ii) Run: Uninstall.bat

To uninstall R70.50 in Provider-1 deployments:
1. Deactivate R70.50 on each CMA:
   a) Login to the Provider-1 MDG.
   b) In Versions & Blades Updates, right click this update and select Deactivate.
2. Run this command on each Provider-1 MDS, CLM and MLM:
   /opt/CPUninstall/R70.50/UnixUninstallScript
3. Activate all Software Blades that were active before the upgrade to R70.50.

Note - After you uninstall R70.50 from SecurePlatform, the command line login prompt and
the WebUI still show R70.50 as the installed version. This is because some packages
related to the SecurePlatform operating system do not uninstall. Use the fw ver
command to see the correct current version.