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=11714
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>29 March 2011</td>
<td>Added instructions about Endpoint Security VPN R75 (&quot;Before Installing or Upgrading&quot; on page 14)</td>
</tr>
<tr>
<td>8 March 2011</td>
<td>Added instructions for installing on IPSO Flash-based appliances with 1GB or 2GB Flash (IP29x, IP39x and IP56x) (&quot;New Installation of R71.30&quot; on page 14)</td>
</tr>
<tr>
<td>11 January 2011</td>
<td>Added Upgrading with the SecurePlatform Embedded Web User Interface (on page 17) and updated the R71.30 Upgrade Packages (on page 16)</td>
</tr>
<tr>
<td>5 January 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 R71.30 Release Notes).
Contents

Important Information.................................................................3
Introduction to R71.30...................................................................5
What's New in R71.30.................................................................5
  Previous Releases Included in R71.30.................................6
  New Terms................................................................................6
Platform Provisions and Requirements........................................7
  Supported Upgrade Paths......................................................7
  Supported Security Products by Platform.............................8
    Security Software Containers by Platform.............................8
    Security Gateway Software Blades by Platform....................9
    Security Management Software Blades by Platform..............10
  Clients and Consoles by Windows Platform........................11
  Minimum System Requirements.............................................11
  Required Disk Space.............................................................12
  Build Numbers.....................................................................13
Installing R71.30........................................................................14
  Before Installing or Upgrading.............................................14
  New Installation of R71.30....................................................14
  Upgrading to R71.30 from Versions Lower than R71..............15
  Upgrading from R71 or Higher to R71.30...............................16
    R71.30 Upgrade Packages................................................16
    Upgrading with the SecurePlatform Web User Interface........17
    Upgrading with the SecurePlatform Embedded Web User Interface......................................................17
    Upgrading with the Command Line....................................17
    Upgrading with SmartUpdate............................................19
  Installing the Client Applications.........................................21
Uninstalling R71.30....................................................................22
Configuring the R71.30 Features...............................................23
  Configuring Support for Check Point Mobile for iPhone and iPad...............................................................24
    Configure the Mobile Access Software Blade.......................24
    Configure iPhone Support..................................................25
    Connect Clients to Web Applications................................25
    Connect Clients to ActiveSync Applications......................27
  Advanced Configuration.......................................................28
  Troubleshooting....................................................................33
  Configuring the R71.30 Provider-1 Features..........................34
    Provider-1 Global Policy Assignment Customization...........34
    Export and Import SmartDashboard Objects........................36
    Provider-1 Command to Restore a Single CMA....................36
    SNMP Monitoring Enhancements.......................................38
    Configuring SNMP Monitoring.........................................38
    Configuration Procedures.................................................39
    Monitoring SNMP Thresholds............................................41
Resolved Issues and Known Limitations....................................42
  Resolved Issues.................................................................42
  Known Limitations..............................................................42
Introduction to R71.30

Thank you for updating to Check Point version R71.30. This version contains new features and resolves various issues for Check Point Software Blades.

Please read this document carefully before installing R71.30.

Note - For more information about R71.30 and to download the software, go to the R71.30 Home Page (http://supportcontent.checkpoint.com/solutions?id=sk59120).

What's New in R71.30

New Remote Access Client Support

- Endpoint Security VPN R75 (SecureClient Next Generation), support for Windows 7 32bit/64bit
- Check Point Mobile for iPhone and iPad
  - Access to Web applications
  - Access to email, calendar, and contacts
  - Two-factor authentication with client certificate and username/password
- SSL Network Extender support for MacOS 10.6 (Snow Leopard) as part of Check Point Mobile Access Provider-1

- Adds SNMP Thresholds to enhance SNMP monitoring & trapping
- Adds tooltip to display name and IP of group objects
- Lets you copy network and host objects between CMAs with easy object export and import from the Object Tree of the SmartDashboard
- Improves SmartDashboard so that global objects function like local objects
  - Tooltip displays the object’s details
  - Double-click opens a read only dialog with the object’s details
- Lets the Customer administrator choose to assign the Global Policy to specific local policy packages
- Lets you use the new cma_restore utility to restore a specific CMA from a backup of the entire Multi-Domain Server

SmartDashboard

- Lets you make changes in SmartDashboard during Policy Installation
- Security Gateway 80 Series R71.30
- Top Services graph in overview page
- Configuration of advanced DHCP options
- Full support for Google Chrome browser

ECMP for OSPF

The OSPF routing protocol in Check Point’s dynamic routing suite explicitly allows Equal-Cost Multi-Path (ECMP) routing, a strategy for routing packets along multiple “best paths” of equal cost. By load balancing traffic over multiple (redundant) routes, ECMP increases network bandwidth.

Check Point’s dynamic routing suite supports up to six simultaneous routes, which means that up to six multiple routes can be used for ECMP. If the routing metric calculations discover more than six paths of equal cost to the same destination, the ECMP feature makes available only the first six.
Previous Releases Included in R71.30

This release includes all features and fixes that were included in R71.20. For more information, refer to:
- R71.20 Release Notes (http://supportcontent.checkpoint.com/documentation_download?id=11238)

New Terms

The following product and technology names have changed for this version.

<table>
<thead>
<tr>
<th>Name Before R71.30</th>
<th>Name Starting with R71.30</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL VPN</td>
<td>Mobile Access</td>
</tr>
</tbody>
</table>
Platform Provisions and Requirements

In This Section

- Supported Upgrade Paths
- Supported Security Products by Platform
- Clients and Consoles by Windows Platform
- Minimum System Requirements
- Required Disk Space
- Build Numbers

Supported Upgrade Paths

R71.30 can be installed on R71, R71.10, or R71.20 Security Gateways, Security Management servers, and Provider-1 MDSs, including 80 Series Security Gateways.

To upgrade from NGX R65 or R70 to R71.30, 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, you must upgrade to R71.20 and then to R71.30. Refer to sk59481 (http://supportcontent.checkpoint.com/solutions?id=sk59481).
- To upgrade Check Point Suite Products before version NGX R65 to R71.30, 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 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>Provider-1 MDS</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>Windows</td>
</tr>
<tr>
<td></td>
<td>Server 2003/2008 (SP1-2) 32bit</td>
</tr>
<tr>
<td></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.

Dedicated Gateways

These dedicated gateways cannot be upgraded to R71.30:

- 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>Secure Platform Embedded</td>
<td>IPSO 6.2 Disk-based</td>
<td>IPSO 6.2 Flash-based</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>Mobile Access</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>✓^4</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; Clustering^1</td>
<td>✓</td>
<td>✓^5</td>
<td>✓</td>
<td>✓</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.
4. Based on IP reputation.
5. Only High Availability 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</td>
<td>✔</td>
</tr>
<tr>
<td>Enterprise Ultimate</td>
<td>✔</td>
</tr>
<tr>
<td>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>
</tbody>
</table>

- **Network Policy Management**
- **Endpoint Policy Management**
- **Logging & Status**
- **Monitoring**
- **SmartProvisioning**
- **Management Portal***
- **User Directory**
- **SmartWorkflow**
- **SmartEvent**
- **SmartReporter**

*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

## Minimum System Requirements

The system requirements for R71.30 are the same as those listed in the R71 Release Notes ([http://supportcontent.checkpoint.com/documentation_download?id=10330](http://supportcontent.checkpoint.com/documentation_download?id=10330)).

<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</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>
<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>
<td>✓</td>
</tr>
<tr>
<td>SecureClient</td>
<td>✓</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>
<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>
<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>
<td>✓</td>
</tr>
<tr>
<td>DLP UserCheck™</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
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 (Including installation process)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurePlatform/ Linux</td>
<td>/var - 1.2 GB</td>
<td>root - 200 MB</td>
<td>root - 200 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/opt - 600 MB</td>
<td>/opt - 900 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 400 MB</td>
<td>/var - 1.6 GB</td>
</tr>
<tr>
<td>IPSO Disk-based</td>
<td>/var - 750 MB</td>
<td>/opt - 200 MB</td>
<td>/opt - 350 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 150 MB</td>
<td>/var - 1 GB</td>
</tr>
<tr>
<td>Windows</td>
<td>700 MB</td>
<td>800 MB</td>
<td>1.5 GB</td>
</tr>
<tr>
<td>Solaris</td>
<td>900 MB</td>
<td>450 MB</td>
<td>1.5 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 (Including installation process)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurePlatform</td>
<td>/var - 1.15 GB</td>
<td>root - 150 MB</td>
<td>root - 200 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/opt - 400 MB</td>
<td>/opt - 300 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 150 MB</td>
<td>/var - 1.3 GB</td>
</tr>
<tr>
<td>IPSO Disk-based</td>
<td>/var - 750 MB</td>
<td>/opt - 200 MB</td>
<td>/opt - 200 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 50 MB</td>
<td>/var - 850 MB</td>
</tr>
<tr>
<td>IPSO Flash-based</td>
<td>/preserve - 400 MB</td>
<td>/preserve - 50 MB</td>
<td>/preserve - 650 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var - 50 MB</td>
<td>/var - 300 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/opt - 50 MB</td>
<td>/opt - 50 MB</td>
</tr>
<tr>
<td>Windows</td>
<td>700 MB</td>
<td>250 MB</td>
<td>1.3 GB</td>
</tr>
</tbody>
</table>
# Build Numbers

The following table lists the R71.30 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.

<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>036</td>
<td><code>fw ver -k</code>&lt;br&gt;This is Check Point VPN-1(TM) &amp; FireWall-1(R) R71.30 - Build 036&lt;br&gt;kernel: R71.30 - Build 036</td>
</tr>
<tr>
<td>Security Management</td>
<td>006</td>
<td><code>fwm ver</code>&lt;br&gt;This is Check Point Security Management Server R71.30 - Build 006</td>
</tr>
<tr>
<td>SmartConsole Applications</td>
<td>976601056</td>
<td><code>Help &gt; About Check Point &lt;Application Name&gt;</code>&lt;br&gt;R71.30 (Build 976601056)</td>
</tr>
<tr>
<td>Provider-1 Multi-Domain Server (MDS)</td>
<td>020</td>
<td><code>fwm mds ver</code>&lt;br&gt;This is Check Point Provider-1 Server R71.30 - Build 020</td>
</tr>
<tr>
<td>Provider-1 Multi-Domain GUI (MDG)</td>
<td>976601016</td>
<td><code>Help &gt; About Check Point Provider-1</code>&lt;br&gt;R71.30 (Build 976601016)</td>
</tr>
<tr>
<td>SecurePlatform</td>
<td>976601024</td>
<td><code>splat_ver</code></td>
</tr>
</tbody>
</table>
Installing R71.30

Before Installing or Upgrading

This version includes a deployment package of Endpoint Security VPN R75. By default, Endpoint Connect clients are upgraded automatically to Endpoint Security VPN R75. After you upgrade the Security Management Server and install a policy, users who connect with Endpoint Connect clients get a prompt to accept an automatic upgrade. The included deployment package cannot upgrade SecureClient to Endpoint Security VPN R75. SecureClient users are not affected.

To disable the automatic upgrade of the VPN clients, do this before installing or upgrading the Security Management Server:

2. Set Client upgrade mode to Do not upgrade.

New Installation of R71.30

R71.30 is released as:

- an upgrade to version R71 or higher for all supported platforms
- a clean installation for IPSO Flash-based appliances, including 1GB and 2GB Flash appliances (IP29x, IP39x and IP56x)

To install R71.30 as a new installation on any management server, gateway or log server:

- For IPSO Flash-based appliances: download this installation file from the Check Point Support Center: Check_Point_R71_30_Security_Gateway_IPSO6_2.tgz (http://supportcontent.checkpoint.com/file_download?id=11991)

Then, 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_R71_30_Security_Gateway_IPSO6_2.tgz

- Command Line newpkg -
  (i) Run: newpkg
  (ii) Type the number (1 - 3) for the FTP server or local path where the TGZ is. Enter the IP address, credentials, and pathnames when prompted.
  (iii) Type y to download the TGZ. The file is downloaded and installation starts.
(iv) When prompted for installation type, type 1 to select Install this as a new package. R71.30 is installed under /opt.


  After you successfully install R71.10, install the upgrade package for your platform ("Upgrading from R71 or Higher to R71.30" on page 16).

### Upgrading to R71.30 from Versions Lower than R71

To upgrade from NGX R65 or R70 to R71.30, 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](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 from R71 or Higher to R71.30" on page 16).

**Note** - To upgrade Check Point Suite Products before version NGX R65 to R71.30, you must first upgrade your system to NGX R65.
Upgrading from R71 or Higher to R71.30

This section includes the procedures for installing R71.30 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

- R71.30 Upgrade Packages
- Upgrading with the SecurePlatform Web User Interface
- Upgrading with the SecurePlatform Embedded Web User Interface
- Upgrading with the Command Line
- Upgrading with SmartUpdate

R71.30 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 and Upgrade Package</th>
<th>Upgrade Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurePlatform and Linux (Open Servers and Appliances)</td>
<td>• SecurePlatform Web User Interface</td>
</tr>
<tr>
<td>Check_Point_R71.30.Linux.tgz (<a href="http://supportcenter.checkpoint.com/file_download?id=11830">http://supportcenter.checkpoint.com/file_download?id=11830</a>)</td>
<td>• Command Line</td>
</tr>
<tr>
<td>IP SO 6.2 Disk-based</td>
<td>• SmartUpdate</td>
</tr>
<tr>
<td>Check_Point_R71.30.ipso6_2.tgz (<a href="http://supportcenter.checkpoint.com/file_download?id=11831">http://supportcenter.checkpoint.com/file_download?id=11831</a>)</td>
<td>Command Line</td>
</tr>
<tr>
<td>IPSO 6.2 Flash-based</td>
<td>Command Line for IPSO Flash-Based</td>
</tr>
<tr>
<td>Check_Point_R71.30.ipso6_2_Flash.tgz (<a href="http://supportcenter.checkpoint.com/file_download?id=11832">http://supportcenter.checkpoint.com/file_download?id=11832</a>)</td>
<td>Command Line</td>
</tr>
<tr>
<td>Windows</td>
<td>Command Line</td>
</tr>
<tr>
<td>Solaris</td>
<td>Command Line</td>
</tr>
<tr>
<td>SecurePlatform Embedded (Security Gateway Series 80)</td>
<td>SecurePlatform Embedded Web User Interface</td>
</tr>
<tr>
<td>fw1_R71_730156065_HFA30.img (<a href="http://supportcontent.checkpoint.com/file_download?id=11851">http://supportcontent.checkpoint.com/file_download?id=11851</a>)</td>
<td>Command Line</td>
</tr>
</tbody>
</table>
Upgrading with the SecurePlatform Web User Interface

You can install R71.30 on SecurePlatform Security Gateways and Security Management open servers and appliances using the Web User Interface.

To install R71.30 using the Web User Interface:
1. Download the upgrade package for your platform ("R71.30 Upgrade Packages" on page 16).
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 SecurePlatform Embedded Web User Interface

You can install R71.30 on Security Gateway Series 80 appliances using the SecurePlatform Embedded Web User Interface.

To install R71.30 using the SecurePlatform Embedded Web User Interface:
1. Download the upgrade package for your platform ("R71.30 Upgrade Packages" on page 16).
2. Connect to the SecurePlatform Embedded Web User Interface at: https://<appliance_ip>:4344
4. Browse to the downloaded image and click Upload.
5. Save a local image with the Image Backup option.
6. Click Next to start the upgrade.
   - At the end of the installation, the device automatically reboots.
7. Re-login to the machine.
8. Go to Overview > System Information > Version to verify that you installed the correct build:
   - R71 HFA30 (730156065)

Upgrading with the Command Line

You can use these instructions to install R71.30 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 R71.30 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 12).
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 ("R71.30 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.
     
     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.
- 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 R71.30" on page 14).

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 12)

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 ("R71.30 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:
   ```
   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.
To install with SmartUpdate:

1. Install the upgrade package for your platform ("R71.30 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:
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 R71.30

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

To uninstall R71.30 in Security Management Server deployments:
1. Disable the IPS Event Analysis and/or SmartWorkflow Software Blades. If you already disabled them before upgrading to R71.30, 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/R71.30/UnixUninstallScript
   - Windows platforms:
     (i) Go to: C:\Program files\CheckPoint\CPUninstall\R71.30
     (ii) Run: Uninstall.bat

To uninstall R71.30 in Provider-1 deployments:
1. Disable the R71.30 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 Multi-Domain Server, Domain Log Server and Multi-Domain Log Server:
   /opt/CPUninstall/R71.30/UnixUninstallScript
3. Activate Software Blades that were active before the upgrade to R71.30.

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 R71.30 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 R71.30 and choose Uninstall in the following order:
   - VPN-1 Power/UTM
   - Mobile Access (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.
Configuring the R71.30 Features

In This Section

- Configuring Support for Check Point Mobile for iPhone and iPad 24
- Configuring the R71.30 Provider-1 Features 34
Configuring Support for Check Point Mobile for iPhone and iPad

To connect from the Check Point Mobile app to the Security Gateway, do this workflow:

Note - Make sure you read sk53002 (http://supportcontent.checkpoint.com/solutions?id=sk53002) for details about Two-Factor Authentication with Check Point Mobile for iPhone and iPad.

1. Set up the gateway. ("Configure the Mobile Access Software Blade" on page 24)
2. Enable support for iPhone and iPad on the gateway ("Configure iPhone Support" on page 25).
3. Connect clients:
   - to Web Applications ("Connect Clients to Web Applications" on page 25)
   - to ActiveSync Applications. ("Connect Clients to ActiveSync Applications" on page 27)
4. Install a server certificate signed by a third-party. ("Creating Trust for Client Connections" on page 32)

Configure the Mobile Access Software Blade

Before you enable Check Point Mobile for iPhone and iPad, you must set up the Mobile Access Software Blade.

Enabling Mobile Access Software Blade

When you enable the Mobile Access Software Blade, a wizard opens. In the wizard you set up Web applications and configure user access. When you are done, Mobile Access gets an automatic 30-day evaluation license. For more details about licensing, refer to the R71 SSL VPN Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=10322).

Licensing the Mobile Access Security Gateway

You must get a license for the Mobile Access Software Blade. After the first policy installation on an enabled Mobile Access blade, the automatic license begins to count down the 30 evaluation days. This license gives access to 10 users. If an extension is necessary, you can get a new 30-day license from the User Center, for 50 users.

To get a license:
1. Log in to your account on the Check Point User Center.
2. Open your My Products page.
3. Select the Mobile Access license.
4. Click License.
Configure iPhone Support

You can enable support for iPhone and iPad to allow these devices to access Web applications and ActiveSync with the Check Point Mobile for iPhone and iPad.

Check Point Mobile requires two-factor authentication with a client certificate and username/password. The Mobile Access Software Blade allows username/password authentication with the Mobile Access portal and does not require a client certificate. To enforce the two-factor authentication requirement, disable access to the Mobile Access portal. For more details, refer to sk53002 (http://supportcontent.checkpoint.com/solutions?id=sk53002).

To enable support for iPhone and iPad on the Mobile Access gateway:
1. On the Mobile Access gateway, run:
   `cvpnd_settings set MobileAppAllowed "true"
2. Restart the Mobile Access Software Blade services: `cvpnrestart`

To disable the Mobile Access portal for all other remote access traffic:
- Run: `toggleCvpnPortal off`

To enable the portal for all remote access traffic:
- Run: `toggleCvpnPortal on`

Note - If you use a cluster, repeat each of these actions for all members of a cluster.

Connect Clients to Web Applications

Web applications configured for the Mobile Access Software Blade are also available to users of Check Point Mobile for iPhone and iPad. For more details about Mobile Access, refer to the R71 SSL VPN Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=10322).

Initializing Client Certificates

Check Point Mobile for iPhone and iPad uses two-factor authentication: client certificate and username/password. You must make a registration key for the certificate. The certificate must be signed by the internal CA of the Security Management Server that manages the Mobile Access Security Gateway.

You can only have one certificate at a time for a single user.

To initialize a client certificate:
1. On SmartDashboard, open the properties window of the user.
2. Open Certificates.
3. If a user had a certificate previously, click Revoke to revoke the current client certificate.
4. Click Initiate to initiate a registration key for a new client certificate.
   A Registration Key is generated.
5. Copy the key and send it to the user.

   Note - The device may ask the user for the Activation Key. This is the same as the Registration Key.

   Note - If you use LDAP or AD, when you initiate client certificates it does not make changes to the LDAP or AD server. If you get a message that says otherwise, close the window with the close (X) button.

Connecting Clients to the Site

You can help users the first time they connect to the Mobile Access Web applications from Check Point Mobile for iPhone and iPad.
- Make sure the users have the FQDN of the Mobile Access gateway.
  An IP address will connect, but is not trusted. Therefore, we recommend the FQDN only.

- Make sure each user has the activation key (registration key) for the client certificate.

- If the users see a server certificate warning, and you did not yet install a trusted server certificate signed by a third-party CA, you can tell the users to tap Accept.

- Make sure that each user knows the password for the app is the same password that they use to access the Mobile Access portal.

After a successful sign-in, the user will see the Web applications to which the user has permissions.
Connect Clients to ActiveSync Applications

Configuring ActiveSync Applications

If users connect to the Exchange server for synchronized email, calendar and contacts, define ActiveSync applications in SmartDashboard.

ActiveSync for iPhone and iPad support is available for Microsoft Exchange Server 2007 SP2 or higher.

To configure ActiveSync on Mobile Access gateways:

1. In SmartDashboard, define a new Web Mail Application in Mobile Access tab > Applications > Web Mail.
   The Web mail service window opens.

   - **Name** - Enter a name that starts with `ActiveSyncApp`.
   - **Outgoing Mail Server (SMTP)** - Select the Exchange server.
   - **Incoming Mail Server (IMAP)** - Select the Exchange server.
   - **SMTP Service** and **IMAP Service** - Select the Exchange server protocol for ActiveSync (http or https).
   - **Mail domain** - Enter the Exchange server Windows domain.
   - **Link in Portal** must be filled, but ignored for the ActiveSync application.

2. Click OK.
3. In Mobile Access tab > Policy, add the new ActiveSyncApp and assign user groups to give users access.
4. Install the policy on the Mobile Access gateway.

Configuring Users to Access ActiveSync Applications

- To access ActiveSync, users must belong to a user group that is allowed to access an ActiveSync application (configured in the previous section).
- Each user must have an email address defined in one of these places:
  - The **Email Address** field in the properties of an internal user object.
  - On an LDAP server (for LDAP users).
- If users are internal users, their Check Point passwords must be identical to their Exchange passwords, otherwise ActiveSync will not work.
Connecting Clients to ActiveSync Applications

Users who see the Mail Setup item can install the ActiveSync profile. This gives users access to their corporate email.

**Note** - OS 3.x iPhones support only one Exchange profile. Before users install the new profile, make sure they remove previously configured profiles (Settings > General > Profiles > Configuration Profiles).

To connect to corporate email (user instructions):
1. Sign in to the Mobile Access site.
2. Tap Mail Setup.
3. Follow the on-screen instructions.
4. When asked for the password, enter the Exchange password.

Advanced Configuration

In This Section

- Advanced Gateway Configuration  28
- Customizing ActiveSync Profiles  30
- Using Multiple Exchange Servers  30
- Supporting ActiveSync for Symbian Devices  31
- Tuning Web Security  32
- Creating Trust for Client Connections  32

Advanced Gateway Configuration

You can customize client authentication, device requirements, certificate details, and ActiveSync behavior.

**Note** - The Link Translation Domain feature is not supported with iPhones. Disable Link Translation Domain on Mobile Access gateways before you connect to them with the iPhone app.

To configure the Mobile Access gateway:
1. For each attribute that you want to configure, run:
   `cvpnd_settings set <attribute_name> "<value>"`
The attributes and the default values are described in the table below.

Note - To check the current value of an attribute run:

cvpnd_settings get <attribute_name>

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| MobileAppAllowed (default value: false)       | Change to true to enable Check Point Mobile for iPhone and iPad features.  
手机应用允许（默认值：false）修改为true以启用Check Point Mobile for iPhone and iPad功能。 |
| MobileAppMinRequiredClientOSVersion (default value: 3.1) | Minimum operating system version for iPhone/iPad. If a client fails this requirement, user sees Your OS version must be upgraded.  
手机应用最小所需的客户端操作系统版本（默认值：3.1）最小的操作系统版本用于iPhone/iPad。如果客户端无法满足此要求，则用户将看到Your OS version must be upgraded。 |
| MobileAppMinRecommendedClientOSVersion (default value: 3.1) | Recommended operating system version for iPhone/iPad.  
手机应用推荐的客户端操作系统版本（默认值：3.1）推荐的操作系统版本用于iPhone/iPad。 |
| MobileAppMinRequiredClientAppVersion (default value: 1.2) | Minimum App version required for iPhone/iPad.  
手机应用最小所需的客户端应用程序版本（默认值：1.2）所需的应用程序版本用于iPhone/iPad。 |
| MobileAppMinRecommendedClientAppVersion (default value: 1.2) | Recommended App version for iPhone/iPad.  
手机应用推荐的客户端应用程序版本（默认值：1.2）推荐的应用程序版本用于iPhone/iPad。 |
| MobileAppClientCertificateNeeded (default value: true) | Enforce certificate requirement to connect to the Mobile Access gateway.  
手机应用客户端证书需要（默认值：true）强制要求证书连接到Mobile Access网关。 |
| MobileAppClientCertMatchUserName (default value: true) | If a client certificate is used, login username must match the username on the client certificate. Enforced only if the certificate is enforced.  
手机应用客户端证书匹配用户名（默认值：true）如果使用客户端证书，则登录用户名必须与客户端证书上的用户名匹配。仅当证书被强制执行时才强制执行。 |
| MobileAppAllowActiveSyncProfileConfig (default value: true) | Make the automatic ActiveSync Profile configuration available to users. If this is true, only users with authorization to access ActiveSync applications see this feature. If this is false, no user sees this feature.  
手机应用允许ActiveSync配置文件（默认值：true）允许将自动ActiveSync配置文件配置给用户。如果为true，则仅具有授权访问ActiveSync应用程序的用户看到此功能。如果为false，则没有用户看到此功能。 |
| MobileAppMinClientOSVersionForProfileConfig (default value: 3.1) | Minimum operating system version for iPhone and iPad to configure ActiveSync with the app. If you want data encryption, change this value from the default to 4.0. Make sure the ActiveSync policy (configured on the Exchange server) enforces data encryption.  
手机应用最小客户端操作系统版本（默认值：3.1）iPhone和iPad用于通过应用程序配置ActiveSync。如果您想要数据加密，请将此值从默认值更改为4.0。确保ActiveSync策略（在Exchange服务器上配置）强制执行数据加密。 |
### Attribute Description

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MobileAppClientSideTimeout (default value: 0)</td>
<td>Timeout (in seconds), controlled by the device. If the active Web application is idle for this amount of time, the end-user is redirected to the login page. This protects sensitive data that a user could have left open on the device. The default zero (0) means that the timeout is taken from the Mobile Access Session option: <em>Disconnect idle sessions</em>.</td>
</tr>
<tr>
<td>MobileAppIncludeLocationInLogs (default value: false)</td>
<td>A GPS feature. When true, iPhones/iPads send physical location data to the gateway, where it is collected and appears in authentication logs.</td>
</tr>
<tr>
<td>ActiveSyncAllowed (default value: true)</td>
<td>Enable ActiveSync features.</td>
</tr>
<tr>
<td>ActiveSyncClientCertificateNeeded (default value: true)</td>
<td>If true, ActiveSync access requires a client certificate.</td>
</tr>
<tr>
<td>ActiveSyncClientCertMatchUserName (default value: true)</td>
<td>If a client certificate is used, and this attribute is true, the certificate must belong to the ActiveSync user.</td>
</tr>
<tr>
<td>ActiveSyncExchangeServerAuthenticationMethod (default value: basic)</td>
<td>Method of forwarding authentication from the Mobile Access gateway to the internal Exchange server. Valid values: basic, digest, ntlm</td>
</tr>
</tbody>
</table>

2. Restart the Mobile Access Software Blade services: cvpnrestart
   - If you use a cluster, copy the `$CVPNDIR/conf/cvpnd.C` file to all cluster members and restart the services on each.

### Customizing ActiveSync Profiles

ActiveSync Exchange features are configured by an *iPhone Configuration Profile*. Check Point Mobile for iPhone and iPad automatically creates an individual profile for each user, with an embedded client certificate. It uses the parameters of the ActiveSync application objects that you define.

You can customize the profile. For example, if you have multiple Exchange servers, you can configure multiple profiles. We use this example to show how to customize profiles with the ActiveSync parameters. To do a simpler customization (for example, to change the profile names), do only the steps that tell how to change the configuration file.

### Using Multiple Exchange Servers

If you have multiple Exchange servers, you can use them all with ActiveSync, if:
- You use Active Directory.
- Each group of users is assigned to one Exchange server.

**To configure ActiveSync for multiple Exchange servers:**

1. Add a new ActiveSyncApp for each Exchange server.
2. In Policy > Access to Applications, assign each AD group to one of these applications.
   - Each Exchange Server ActiveSyncApp can have multiple AD groups assigned to it, but no group can be assigned to more than one server.
   - Exchange Server 1 is used by ActiveSyncAppCP, and Exchange Server 2 is used by ActiveSyncApp_bck.
One group, Partners, is assigned to ActiveSyncAppCP. Users in Partners get their email from Exchange Server 1.

Two groups, Customers and Mobile-vpn-user, are assigned to ActiveSyncApp_bck. Users in these groups get their email from Exchange Server 2.

3. Configure the profiles and Exchange server domains. Set the attributes below according to these guidelines:
   - Each attribute must have the same number of elements as the other attributes, in the same sequence.
   - Elements are separated by commas, without spaces.
   - If there is a space in one of the element values, you must use quotes around the full element list.
   - For each attribute that you want to configure, run:
     `cvpnd_settings set <attribute_name> "<value>"

   The attributes are described in the table below.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MobileAppProfileNames ()</td>
<td>List of profiles. Each profile name must match a configured ActiveSync application.</td>
</tr>
<tr>
<td></td>
<td>A typical ActiveSync application object is actually a WebMail application object beginning with the name ActiveSyncApp.</td>
</tr>
<tr>
<td>MobileAppProfileDisplayNames ()</td>
<td>How the user sees the profiles.</td>
</tr>
<tr>
<td>MobileAppExchangeDomainNames ()</td>
<td>Exchange Server domains of each profile.</td>
</tr>
<tr>
<td>MobileAppSslvpnHostNames ()</td>
<td>Which Mobile Access gateway to use as a proxy for each ActiveSync profile.</td>
</tr>
<tr>
<td></td>
<td>Even if multiple profiles use the same gateway, it must be listed as many times as there are profiles.</td>
</tr>
</tbody>
</table>

   **Example:**
   
   ```
   :MobileAppProfileNames (ActiveSyncApp_1,ActiveSyncApp_2,ActiveSyncApp_3)
   :MobileAppProfileDisplayNames ("NY,London,Berlin")
   :MobileAppExchangeDomainNames (AD,mydomain.co.uk,ad.example.co.de)
   :MobileAppSslvpnHostNames (sslvpn.ex.com,sslvpn.ex.com,sslvpn.ex.com)
   ```

4. Restart the Mobile Access Software Blade services: `cvpnrestart`

   If you use a cluster, copy the `$CVPNDIR/conf/cvpnd.C` file to all cluster members and restart the services on each.

5. Install Policy.

**Supporting ActiveSync for Symbian Devices**

Mobile devices with the Symbian OS behave differently than iPhones and iPads. A Symbian device presents its client certificate automatically only if the first URL it accesses on the gateway demands the certificate. If the URL does not request the certificate, the device never presents it. This is an issue because this supplement enforces client certificate authentication by default.
To make sure Symbian devices can use ActiveSync:

1. Use `sysconfig` to define a dedicated virtual IP address on the Mobile Access gateway.
2. Define a dedicated FQDN for Symbian clients.
   
   For example: `symbian.sslvpn.example.com`
3. Configure the DNS servers to map the dedicated FQDN to the virtual IP.
4. On the gateway, back up `/etc/rc.local` and open it.
5. Add these `fw ctl` commands to `/etc/rc.local`:

   ```shell
   # The force_client_cert_auth flag enables Symbian support.
   fw ctl set int force_client_cert_auth 1
   # The IP address below is an example of the virtual IP.
   fw ctl set string client_cert_auth_dest_ip 192.0.2.40
   ```
6. Run the script or reboot the gateway.

**Tuning Web Security**

We recommend using the local IPS Web Intelligence protections that are automatically configured and activated when you enable the Mobile Access blade. If you want to use the IPS profile that you assign to the Security Gateway instead of the local file, make sure that crucial protections are active so that your Security Gateway stays secure.

To change to a Security Gateway IPS profile configuration for Mobile Access instead of the local configuration:

1. Edit the IPS profile assigned to the Security Gateway to include Mobile Access protections.
2. Run:

   ```shell
   cvpnd_settings set use_ws_local_configuration false
   ```
3. When prompted, backup `$CPDIR/conf/cvpnd.C`
4. Restart the Mobile Access processes: `cvpnstop, cvpnstart`

To switch back to the local, automatic IPS settings for Mobile Access:

1. Run:

   ```shell
   cvpnd_settings set use_ws_local_configuration true
   ```
2. Restart the Mobile Access processes: `cvpnstop, cvpnstart`

**Creating Trust for Client Connections**

Check Point Mobile clients must trust the gateway. If users see a message that the server is not trusted, the gateway does not have a server certificate that is signed by a third-party.

Make sure that the server certificate of the Mobile Access gateway is signed by a trusted third-party Certification Authority (for example, EnTrust). This CA must be also trusted by the device. The certificate must replace the self-signed (ICA) certificate.

**Generating the Certificate Signing Request**

First, generate a Certificate Signing Request (CSR). The CSR is for a server certificate, because the gateway acts as a server to the clients.

⚠️ Note - This procedure creates private key files. If private key files with the same names already exist on the machine, they are overwritten without warning.

1. From the gateway command line, log in to expert mode.
2. Run:

   ```shell
   cpopenssl req -new -out <CSR file> -keyout <private key file> -config $CPDIR/conf/openssl.cnf
   ```

   This command generates a private key. You see this output:

   ```shell
   Generating a 2048 bit RSA private key
   ```
3. Enter a password and confirm. You see this message:

```
writing new private key to 'server1.key'
Enter PEM pass phrase:
```

You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank. For some fields there will be a default value. If you enter '.', the field will be left blank.

Fill in the data.

- The **Common Name** field is mandatory. This field must have the Fully Qualified Domain Name (FQDN). This is the site that users access. For example: `portal.example.com`.
- All other fields are optional.

4. Send the CSR file to a trusted certificate authority. Make sure to request a **Signed Certificate** in PEM format. Keep the `.key` private key file.

### Installing the Signed Certificate

Install the Third Party signed certificate to create Trust between the Mobile Access Software Blade and the clients.

**To install the signed certificate:**

1. Get the Signed Certificate for Mobile Access from the certificate authority.
   - If the signed certificate is in P12 or P7B format, convert these files to PEM format.
     - To convert a P12 File to PEM format: Run the `$CVPNDIR/bin/p12ToPem` script. See sk30997.
     - To convert a P7B File to PEM format: Run the `$CVPNDIR/bin/p7bToPem` script. See sk31589.

2. Install the `*.crt` file with the `*.key` file that was generated by **CSR_gen**.
   a) If you already have a signed certificate file, back up this directory from a gateway or cluster member:
     ```
     $CVPNDIR/var/ssl
     ```
   b) Run:
     ```
     $CVPNDIR/bin/InstallCert <certfile> <keyfile> '<passwd>'
     ```
   c) Run: `cvpnrestart`

3. If you use clusters:
   a) **Copy all** `$CVPNDIR/var/ssl/server*` files to the same path on all other cluster members.
   b) **On each member that the files are copied to,** run: `cvpnrestart`

4. Run: `certificate_signing_utility -upgrade`
   - If your environment is Provider-1, run this command on the CMA.

5. Install the policy.

6. Make sure that the new certificate is presented by the gateway portal to clients.

   **Note** - You may have to do Install Policy more than once.

### Troubleshooting

**Getting Logs from Clients**

To resolve issues with client devices, tell the users to send you the logs. The iPhone or iPad must have an SMTP account set up.

**Tell the user to:**

1. Tap the **Information** icon. (Before login, this is on the top right. After login, this is on the bottom right.)
2. Tap the **Send Logs** button on the navigation bar.
   If the user does not have an email account configured on the iPhone, a message shows the user that one must be configured. After this is done, the user must open Check Point Mobile Access again. When an email account is configured, the email page opens. The logs are attached.

   **Note** - The email account that the iPhone uses to send the email is the default account. This might not be your organization's ActiveSync account.

   If the iPhone is not configured for a destination email address for logs, the email that opens has an empty **To** field. The user can enter the destination address now, or set up a default destination address for Check Point Mobile logs.

   **To set up a default destination address:**
   1. Tap the iPhone **Settings** icon.
   2. Scroll down to the Check Point **Mobile** icon and tap it.
   3. In the **Mobile** global settings, enter the address in **Logs eMail**.

### Disabling Client SSO

Single Sign On (SSO) lets users in a session connect to the Mobile Access gateway without authenticating when the application is invoked again. If a user cannot access the gateway while SSO is enabled, disable it.

**To disable SSO on a client, tell the user to:**
1. Tap the iPhone **Settings** icon.
2. Scroll down to the Check Point **Mobile** icon and tap it.
3. In the **Mobile** global settings, tap the **Single Sign On > Enabled** switch.

---

### Configuring the R71.30 Provider-1 Features

**In This Section**

- Provider-1 Global Policy Assignment Customization
- Export and Import SmartDashboard Objects
- Provider-1 Command to Restore a Single CMA
- SNMP Monitoring Enhancements
- Configuring SNMP Monitoring
- Configuration Procedures
- Monitoring SNMP Thresholds

#### Provider-1 Global Policy Assignment Customization

When you assign Global Policy on a Customer, you can customize the Global Policy assignment and choose to assign it to specified policies of the Customer. In earlier releases you could only assign the Global Policy to all policies or no policies on the Customer.

#### Using Global Policy Customization

When you install this release, the Global Policy Customization feature is automatically available from the MDG. Each time that you assign Global Policy, you can specify which policies of each Customer will receive the Global Policy.
Customizing the Assignment

To customize the Global Policy Assignment for all Customers:
1. In the Global Policies view of the MDG, select the root Provider-1 object.
2. From the toolbar select Manage > Customize Global Policy Assignment.
3. In the Select Policies that will receive global policy window, choose on which policies to assign the Global Policy. Move the policies between the Assign on and Do not assign on panes with the Assign and Remove buttons.
4. Click OK.

The next time that you Assign or Reassign Global Policy, the settings are applied to the Customer’s CMAs.

To customize the Global Policy Assignment for a specified Global Policy or Customer:
1. In the Global Policies view of the MDG, select a Customer or Global Policy object.
2. Right-click the object and select Assign/Install Global Policy or Reassign/Install Global Policy. You can also select the same options from the Manage menu.
3. In the window that opens, click Customize.
4. In the Select Policies that will receive global policy window, choose on which policies to assign the Global Policy. Move the policies between the Assign on and Do not assign on panes with the Assign and Remove buttons.
5. Click OK.

The next time that you Assign or Reassign Global Policy, the settings are applied to the Customer’s CMAs.

Seeing the Assignments in the MDG

You can see an overview of the Global Policy status of the Customers from the Global Policies view of the MDG.

- In the Assign Global Policy On column of the primary pane, see a summary of the Global Policy assigned for each Customer. The column can contain these values and icons:
  - **All** - All policies on the Customer have Global Policy assigned.
  - **Partial** - Some policies on the Customer have Global Policy assigned. The numbers shown are how many policies have the assignment out of the total number on the Customer. For example, 3/5 means that 3 out of 5 available policies have Global Policy assigned.
  - **None** - None of the policies on the Customer have Global Policy assigned.
  - A **green checkmark** - Means that the policies are assigned according to the current customization settings.
  - A **red exclamation point** - Means that the customization is set in the MDG but the changes are not assigned on the CMAs. The changes are assigned when you Assign Global Policy.

- In the right pane of the Global Policies view, see the details of the Global Policy assignment for the selected Customer.
  - **Assign Global Policy on** - Lists the names of the policies that have Global Policy assigned.
  - **Do Not Assign Global Policy on** - Lists the names of the policies that do not have Global Policy assigned.

Click Customize Global Policy Assignment to edit the settings.
Permissions and Global Policy Customization

Administrators with these permissions can see and edit the customized Global Policy assignments for a Customer:

- Provider-1 SuperUser
- Customer SuperUser
- Global Manager with read\write permissions on the Global Database and full Read\Write permissions on the Customer

Administrators with these permissions can see the customized Global Policy assignments for a Customer but not edit them:

- Global Managers without the permissions described above.
- Customer Managers to whom the Customer is assigned.

Export and Import SmartDashboard Objects

You can export and import many types of Network objects from the Objects Tree: Host Nodes, Networks, Address Ranges, and Groups. Groups for export can only contain the other exportable objects. You can use this to copy object between CMAs.

To export an existing Network object:
1. Right-click on the object from the object tree or object list and select Export.
   The Browse for Folder window opens.
2. Select the location that the object will be exported to and Click OK.
   The object is exported to that location with the file name <object_name>.ckp.

You can import exported objects into a SmartDashboard of the same version.

Import a Network object that has been exported in one of these ways:

- Drag the object into the Object Tree.
- In the Object List of the SmartDashboard, click Action > Import.

Notes -

- You cannot export a Network object if it has a reference to an object that is not exportable, for example, a gateway.
- You can select multiple objects to export at once. Each object is saved in a separate file.
- Group objects are exported as one file that contains the data of all of the dependant Network objects.

Provider-1 Command to Restore a Single CMA

A new Provider-1 command, \texttt{cma\_restore} lets you restore a single CMA in a disaster recovery situation.

\texttt{cma\_restore} 

\textbf{Description} 
This command restores a CMA in a situation when one CMA has failed but the rest of the Multi-Domain Server environment is intact.

\textbf{Important} - This is not an upgrade tool. Use it only in situations where one CMA has failed but the rest of the Multi-Domain Server environment is intact.
To use the `cma_restore` command, you must have an exported_mds file that you create with the `mds_setup` command.

**To create an exported_mds file:**

1. Mount the Provider-1 installation CD onto the relevant subdirectory.
2. Change the directory to the mounted CD directory.
3. Browse to either the Solaris or Linux directory, depending on the operating system of your Multi-Domain Server machine.
4. Run: `./mds_setup`.
5. Select the Export option from the list.
   This option extracts the database and configuration settings from a Multi-Domain Server and its associated CMAs. It stores the data in a single `exported_mds.<timestamp>.tgz` file.
6. When prompted, enter the location where you want to store the tgz file.

You can do this procedure periodically instead of, or in addition to, `MDS_backup` to make sure that you have a backup file of your MDS that you can also use to restore an individual CMA. The `backup_mds` and `restore_mds` commands let you restore an entire MDS but not just one or more individual CMAs.

**Usage**

```
cma_restore -f <full path to an exported_mds file>
```

The utility stops the Multi-Domain Server before it starts the restore. Then it shows a list of the CMAs in the export file. Enter the names of the CMA or CMAs to be restored.

**Example**
```
/var/opt/user@mind# cma_restore -f
/var/opt/exported_mds.16Jun2010-140530.tgz

Warning: cma_restore.sh restores selected CMAs, overwriting their existing copy.
   If the restored CMA is not found on this MDS, restoration will not take place.

Your MDS should NOT be running while you restore CMAs.
cma_restore.sh will now stop the MDS.
Do you want to continue [yes/no] ? y
Stopping CMAs
Number of CMAs stopped so far: 1 out of 2
Number of CMAs stopped so far: 2 out of 2
Stopping MDS
MDS stopped

--- Starting Restore Procedure ---
Checking for installed components. This may take a few seconds.
Please wait...
The following CMAs can be restored:
mind1
mind2
Which CMAs to restore? (list names separated by a space)
mind1
Restoring CMA mind1
mind1 successfully restored

--- Restore operation has finished.
The MDS can be started now.
---
DONE.
A log file was created: /opt/CPmds-R71/log/cma_restore.20Jun2010-165103.log
```
SNMP Monitoring Enhancements

This release lets you configure a variety of SNMP Thresholds that generate SNMP traps, or alerts. You can use the thresholds to monitor many system components automatically without requesting information from each object or device. The categories of thresholds that you can configure include:

- Hardware
- High Availability
- Networking
- Resources
- Log Server Connectivity

Some categories apply only to some machines or deployments.

In each category are many individual thresholds that you can set. For example, the hardware category includes alerts for the state of the RAID disk, the state of the temperature sensor, the state of the fan speed sensor, and others. For each individual threshold, you can configure:

- If it is enabled or disabled
- How frequently alerts are sent
- The severity of the alert
- The threshold point (if necessary)
- Where the alerts are sent to

You can also configure some settings globally, such as how often alerts are sent and where they are sent to.

Types of Alerts

There are two different types of alerts:

- **Active alerts** are sent when a threshold point is passed or the status of a monitored component is problematic.
- **Clear alerts** are sent when the problem is resolved and the component has returned to its normal value. Clear alerts look like active alerts but the severity is set to 0.

Configuring SNMP Monitoring

Configure the SNMP monitoring thresholds in the command line of the Security Management server. When you install the policy on the gateways the SNMP monitoring thresholds are applied globally to all gateways.

Configuring in Provider-1

In a Provider-1 environment, you can configure thresholds on the Multi-Domain Server and on each individual CMA. Thresholds that you configure on the Multi-Domain Server are for the Multi-Domain Server only. Thresholds that you configure for a CMA are for that CMA and its gateways. If a threshold applies to the Multi-Domain Server and the CMA gateways, set it on the Multi-Domain Server and CMA. However, in this situation you might only get alerts from the Multi-Domain Server if the threshold is passed.

For example, because the Multi-Domain Server and CMA are on the same machine, if the CPU threshold is passed, it applies to both of them. However, only the Multi-Domain Server generates alerts.

You can see the Provider-1 level for each threshold with the `threshold_config` utility.

- If the Provider-1 level for a threshold is **Multi-Domain Server**, alerts are generated for the Multi-Domain Server when the threshold point is passed.
- If the Provider-1 level for a threshold is **Multi-Domain Server, CMA**, alerts are generated for the Multi-Domain Server and CMAs separately when the threshold point is passed.
Configuring a Local Gateway Policy

You can configure SNMP thresholds locally on a gateway with the same procedure that you do on a Security Management server. However, each time you install a policy on the gateway, the local settings are erased and it reverts to the global SNMP threshold settings.

You can use the `threshold_config` utility to save the configuration file and load it again later. Or you can manually back up the configuration file so that you can copy the configuration to the gateway again after you install the policy.

On SecurePlatform and Linux, the configuration file that you can back up is: `$FWDIR/conf/thresholds.conf`

On Windows the configuration file that you can back up is: `%FWDIR%\conf\thresholds.conf`

Configuration Procedures

There is one primary command to configure the thresholds in the command line, `threshold_config`. You must be in expert mode to run it. After you run `threshold_config`, follow the on-screen instructions to make selections and configure the global settings and each threshold.

When you run `threshold_config`, you get these options:

- **Show policy name** - Shows you the name configured for the threshold policy.
- **Set policy name** - Lets you set a name for the threshold policy.
- **Save policy** - Lets you save the policy.
- **Save policy to file** - Lets you export the policy to a file.
- **Load policy from file** - Lets you import a threshold policy from a file.
- **Configure global alert settings** - Lets you configure global settings for how frequently alerts are sent and how many alerts are sent.
- **Configure alert destinations** - Lets you configure a location or locations where the SNMP alerts are sent.
- **View thresholds overview** - Shows a list of all thresholds that you can set including: The category of the threshold, if it is active or disabled, the threshold point (if relevant), and a short description of what it monitors.
- **Configure thresholds** - Open the list of threshold categories to let you select thresholds to configure.

Configure Global Alert Settings

If you select **Configure global alert settings**, you can configure global settings for how frequently alerts are sent and how many alerts are sent. You can also configure these settings for each threshold. If a threshold does not have its own alert settings, it uses the global settings by default.

You can configure these options:

- **Enter Alert Repetitions** - How many alerts will be sent when an active alert is triggered. If you enter 0, alerts will be sent until the problem is fixed.
- **Enter Alert Repetitions Delay** - How long the system waits between sending active alerts.
- **Enter Clear Alert Repetitions** - How many clear alerts will be sent after a threshold returns to a normal value.
- **Enter Clear Alert Repetitions Delay** - How long the system waits between sending clear alerts.

Configure Alert Destinations

If you select **Configure Alert Destinations**, you can add and remove destinations for where the alerts are sent. You can also see a list of the configured destinations. A destination is usually an NMS (Network Management System) or a Check Point log server.

After you enter the details for a destination, the CLI asks if you want the destination to apply to all thresholds.
If you enter yes, alerts for all thresholds are sent to that destination, unless you remove the destination from an individual threshold.

If you enter no, no alerts are sent to that destination by default. However, for each individual threshold, you can configure the destinations and you can add destinations that were not applied to all thresholds.

For each threshold, you can choose to which of the alert destinations its alerts are sent. If you do not define alert destination settings for a threshold, it sends alerts to all of the destinations that you applied to all thresholds.

For each alert destination enter:
- Name - An identifying name.
- IP - The IP address of the destination.
- Port - Through which port it is accessed
- Ver - the version on SNMP that it uses
- Other data - Some versions of SNMP require more data. Enter the data that is supplied for that SNMP version.

### Configure Thresholds

If you select Configure thresholds, you see a list of the categories of thresholds, including:
- Hardware
- High Availability
- Networking
- Resources
- Log Server Connectivity

Some categories apply only to some machines or deployments. For example, Hardware applies only to Check Point appliances and High Availability applies only to clusters or high availability deployments.

Select a category to see the thresholds in it. Each threshold can have these options:
- **Enable/Disable Threshold** - If the threshold is enabled, the system sends alerts when there is a problem. If it is disabled it does not generate alerts.
- **Set Severity** - You can give each threshold a severity setting. The options are: Low, Medium, High, and Critical. The severity level shows in the alerts and in SmartView Monitor and lets you know quickly how important the alert is.
- **Set Repetitions** - Set how frequently and how many alerts will be sent when the threshold is passed. If you do not configure this, it uses the global alert settings.
- **Set Threshold Point** - Enter the value that will cause active alerts when it is passed. Enter the number only, without a unit of measurement.
- **Configure Alert Destinations** - See all of the configured alert destinations. By default, active alerts and clear alerts are sent to the destinations. You can change this for each destination. Select the destination and you see these options:
  - **Remove from destinations** - If you select this, alerts for this threshold are not sent to the selected destination.
  - **Add a destination** - If you configured a destination in the global alert destinations but did not apply it to all thresholds, you can add it to the threshold.
  - **Disable clear alerts** - If you select this, clear alerts for this threshold are not sent to the selected destination. Active alerts are sent.

### Completing the Configuration

To complete threshold configuration and activate the settings:
- On the Security Management server, install the policy on all gateways.
For a local gateway threshold policy or a Provider-1 Multi-Domain Server environment, restart the CPD process using the `cpwd_admin` utility:

a) Run: `cpwd_admin stop -name CPD -path "$CPDIR/bin/cpd_admin" -command "cpd_admin stop"`

b) Run: `cpwd_admin start -name CPD -path "$CPDIR/bin/cpd" -command "cpd"`

### Monitoring SNMP Thresholds

You can see an overview of the SNMP thresholds that you configure in SmartView Monitor.

To see an overview of the SNMP thresholds:

1. Open SmartView Monitor and select a gateway.
2. In the summary of the gateway data that open in the bottom pane, click **System Information**.
3. In the new pane that opens, click **Thresholds**.
4. In the pane that opens, you can see these details:

   - **General Info** - A summary of the total SNMP Threshold policy.
     - **Policy name** - The name that you set for the policy in the CLI.
     - **State** - If the policy is enabled or disabled.
     - **Thresholds** - How many thresholds are enabled.
     - **Active events** - How many thresholds are currently sending alerts.
     - **Generated Events** - How many thresholds went from not active to active since the policy was installed.

   - **Active Events** - Details for the thresholds that are currently sending alerts.
     - **Name** - The name of the alert (given in the CLI)
     - **Category** - The category of the alert (given in the CLI), for example, Hardware or Resources.
     - **MIB object** - The name of the object as recorded in the .mib file.
     - **MIB object's value** - The value of the object when the threshold became active, as recorded in the .mib file.
     - **State** - The current state of the object, either active or clearing (passed the threshold but is returning to normal value.
     - **Severity** - The severity of that threshold, as you configured for it in the CLI.
     - **Activation time** - When the alert was first sent.

   - **Alert Destinations** - A list of the destinations that alerts are sent to.
     - **Name** - The name of the location.
     - **Type** - The type of location, for example, a log server or NMS.
     - **State** - If logs are being sent from the gateway or Security Management server to the destination machine.
     - **Alert Count** - How many alerts were sent to the destination from when the policy was started.

   - **Errors** - Shows thresholds that cannot be monitored. For example, the gateway cannot monitor RAID sensors on a machine that does not have RAID sensors. Therefore it will show an error for the RAID Sensor Threshold.
     - **Threshold Name** - The name of the threshold with an error.
     - **Error** - A description of the error.
     - **Time of Error** - When the error first occurred.
Resolved Issues and Known Limitations

Resolved Issues

Resolved Issues in R71.30 are in sk59123 (http://supportcontent.checkpoint.com/solutions?id=sk59123).

Known Limitations

Known Limitations for R71.30 are in sk59122 (http://supportcontent.checkpoint.com/solutions?id=sk59122).