21 August 2016

E80.64 and R77.30.02

Release Notes
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.

Check Point E80.64
For more about this release, see the home page http://supportcontent.checkpoint.com/solutions?id=sk112793.

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=51163.
To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

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 E80.64 and R77.30.02 Release Notes.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21 August 2016</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Contents

Important Information ................................................................................................... 3
Introduction ................................................................................................................... 5
What’s New ................................................................................................................... 5
Platforms and Alignment to R77.30 Jumbo Hotfix .................................................... 5
Management Features .............................................................................................. 5
Full Disk Encryption Features ................................................................................... 5
Media Encryption Features ....................................................................................... 6
Anti-Malware Features ............................................................................................. 6
Capsule Docs Features ............................................................................................. 6
Remote Access VPN Features ................................................................................... 6
SandBlast Agent Features ........................................................................................ 6
Management Requirements .......................................................................................... 7
Server Supported Operating Systems ....................................................................... 7
Server Hardware Requirements ............................................................................... 7
Supported Check Point Versions ............................................................................... 8
Capsule Docs Requirements ..................................................................................... 8
Supported Languages for Management .................................................................... 8
Client Requirements ..................................................................................................... 9
Supported Client Operating Systems ........................................................................ 9
Supported Mobile Operating Systems .................................................................... 9
Supported Languages for Endpoint Security Clients .............................................. 10
Client Hardware Requirements .............................................................................. 10
Full Disk Encryption Requirements ........................................................................ 10
Self-Help Portal ...................................................................................................... 12
Endpoint Offline Management Tool Requirements ................................................. 13
Media Encryption & Port Protection Support .......................................................... 13
Capsule Docs Supported Applications .................................................................... 13
Supported SmartConsole Platforms ........................................................................... 14
SmartEndpoint Requirements ................................................................................ 14
Supported Upgrade Paths ........................................................................................ 15
Supported Upgrades for Endpoint Security Management ....................................... 15
Supported Upgrades for Endpoint Security Client .................................................. 15
Supported Upgrades to Windows 10 ....................................................................... 16
Legacy Full Disk Encryption Support ...................................................................... 16
Legacy Media Encryption Support .......................................................................... 16
Installation and Configuration ..................................................................................... 17
Installing an Endpoint Security Management Server .............................................. 17
Installing the Hotfixes ............................................................................................. 17
Installing Endpoint Security Clients ........................................................................ 18
Installing the SmartConsole .................................................................................... 18
Java Upgrades ........................................................................................................... 19
Known Limitations ...................................................................................................... 19
Introduction

Check Point Endpoint Security E80.64 clients introduce new features and functionality on top of R77.30.02 Management.

What's New

This release supports all Software Blades and features of previous releases. It includes new platform support, technologies, and features.

Platforms and Alignment to R77.30 Jumbo Hotfix

- Windows 10 Anniversary Update (version 1607) support for Endpoint Security clients.
- Endpoint Security Server installation on R77.30 with a dedicated Jumbo Hotfix for Endpoint Security. This Jumbo Hotfix is aligned to take 143 of the R77.30 Jumbo Hotfix.

Management Features

- New Policies & Reports.
- Offline Management Tool for Full Disk Encryption Offline Mode.
- General performance improvements.
- New Client UI look and feel.

Full Disk Encryption Features

- Offline Mode - Provides Endpoint Security client support for computers that are not connected to an Endpoint Security Management Server, with the same level of security as regular deployments. Features include:
  - Policy management.
  - Data recovery and Emergency Access.
  - Logs, Statistics, and Reporting.
  - New Deployment User type for creating Offline Mode users at preboot.
- XTS-AES Encryption on UEFI Systems - Supports new AES algorithms for optimal performance and security:
  - XTS-AES 128 (2x128) encryption.
  - XTS-AES 256 (2x256) encryption.
- Performance optimizations for disk I/O.
- Pre-boot usability improvements.
Media Encryption Features

- Media Encryption Default container size configuration.
- Optical Media Scan support.

Anti-Malware Features

Web Protection from malware.
- Prevent access to suspicious sites.
- Scan downloaded objects using signature and heuristic analysis.

Capsule Docs Features

- Support for new File Types.
- Support for Adobe Acrobat Reader DC.
- New Document Expiration feature- Set an expiration date for protected files. After the expiration date, only the author can access the document.
- Ability to set, change, and remove protection from Microsoft Office and PDF files with a right-click context menu.

Remote Access VPN Features

- VPN performance enhancements in upload and download paths.
- Support for ATM client.

SandBlast Agent Features

Check Point SandBlast Agent delivers advanced Threat Extraction and Threat Emulation, Forensics, and Anti-Bot to endpoint devices.

Key Benefits

- Defends against multiple attack vectors, including web downloads, external storage devices, lateral movement, or encrypted content.
- Quickly delivers safe, sanitized versions of documents without business interruption.
- Identifies and contains infected hosts to limit damage and spread of malware.
- Continuously collects data about user systems for later forensics use.
- Automatically builds actionable forensics reports with important attack information.
- Integrates monitoring and investigation of security events through SmartEvent and SmartLog.
Key Features

- Check Point SandBlast Agent delivers advanced Threat Extraction and Threat Emulation, Forensics, and Anti-Bot to endpoint devices.
- Threat Emulation for web downloads and for files copied to the file-system.
- Automated Forensic analysis of security events.
- Quarantine of infected hosts.
- Malware removal based on Forensic analysis.
- Threat Extraction for web downloads.

Management Requirements

This section shows supported operating systems and hardware requirements for Management servers and consoles.

Also see relevant requirements in the R77.30 Release Notes http://downloads.checkpoint.com/dc/download.htm?ID=40107.

Server Supported Operating Systems

Endpoint Security Servers are only supported on Gaia. These servers are supported:

- Gaia: Smart-1 series and open platform
- VMware: ESXi 5.1, 5.5, 6.0
- Microsoft Hyper-V 6.3.9600.16384

Server Hardware Requirements

These are the minimum requirements to enable Endpoint Security management on a Security Management Server:

<table>
<thead>
<tr>
<th>Component</th>
<th>All Supported Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel Pentium E2140 2.0 GHz</td>
</tr>
<tr>
<td>Memory</td>
<td>8GB</td>
</tr>
<tr>
<td>Disk Space</td>
<td>80GB</td>
</tr>
</tbody>
</table>

Resource consumption is based on the size of your environment. For larger environments, more disk space, memory, and CPU are required.

⚠️ Note - The network Security Management Server can also be an Endpoint Policy Management server. All deployments support this, except:

- Standalone
- Multi-Domain Server
• This Endpoint Security version supports R77.30 SmartEvent.
• Endpoint Security Servers are not supported on Windows or RedHat Enterprise Linux releases.

Make sure that these ports are available on the server:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>Apache HTTP</td>
<td>Apache HTTP 443 Apache SSL 61616 AMQ TCP access</td>
</tr>
<tr>
<td>8009</td>
<td>Tomcat AJP</td>
<td>8008 Tomcat HTTP 8005 Tomcat server</td>
</tr>
<tr>
<td>1080</td>
<td>CPTNL client proxy</td>
<td>81 CPTNL server 18193 CPTNL server proxy</td>
</tr>
<tr>
<td>(for Policy Servers only)</td>
<td></td>
<td>(for Management Servers only)</td>
</tr>
<tr>
<td>81</td>
<td>CPTNL server</td>
<td>18193 CPTNL server proxy</td>
</tr>
<tr>
<td>(for Management Servers only)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Supported Check Point Versions

E80.64 clients on all supported Windows versions, including Windows 10, can be managed by R77.30.02, R77.30.01 and R77.30 servers.

The Endpoint Security Management Server is supported on a management-only computer or appliance. Standalone (Security Gateway + Management) deployment is not supported.

To get new E80.64 features and capabilities, E80.64 clients must be managed by an R77.30.02 server.

R77.30.02 requires the dedicated R77.30 Jumbo Hotfix for Endpoint Security (aligned with take 143). This integrates security fixes into R77.30.02.

To support E80.64 Client logs in SmartView Tracker for R77.30 and R77.30.01 servers, see sk106662 http://supportcontent.checkpoint.com/solutions?id=sk106662.

For a list of the supported client version for each Management server, see sk107255 http://supportcontent.checkpoint.com/solutions?id=sk107255.

Capsule Docs Requirements


Supported Languages for Management

SmartEndpoint Console is available only in English. It supports operating systems in Japanese.

Endpoint Security Management Server is supported only in English.
Client Requirements

This section shows supported operating systems and hardware requirements for Endpoint Security clients.

Supported Client Operating Systems

**Microsoft Windows**

<table>
<thead>
<tr>
<th>Version</th>
<th>Editions</th>
<th>Arch.</th>
<th>SPs or Updates</th>
<th>Supported Blades</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 (version 1511)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>10 (version 1607)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>8.1</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td>Update 1</td>
<td>All</td>
</tr>
<tr>
<td>7</td>
<td>Enterprise Professional</td>
<td>32/64-bit</td>
<td>SP1</td>
<td>All</td>
</tr>
</tbody>
</table>

**Microsoft Windows Server**

<table>
<thead>
<tr>
<th>Version</th>
<th>Editions</th>
<th>Arch.</th>
<th>SPs or Updates</th>
<th>Supported Blades</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>All</td>
<td>64-bit</td>
<td></td>
<td>Compliance, Anti-Malware, Firewall, Capsule Docs, SandBlast Agent Blades</td>
</tr>
<tr>
<td>2012 R2</td>
<td>All</td>
<td>64-bit</td>
<td></td>
<td>Compliance, Anti-Malware, Firewall, Capsule Docs, SandBlast Agent Blades</td>
</tr>
<tr>
<td>2008 R2</td>
<td>All</td>
<td>32/64-bit</td>
<td></td>
<td>Compliance, Anti-Malware, Firewall, Capsule Docs, SandBlast Agent Blades</td>
</tr>
</tbody>
</table>

**Notes** - If you install a client package with blades that are not supported on the server, the installation succeeds but only the supported blades are installed.

Supported Mobile Operating Systems

These mobile OS versions support Capsule Docs:

- iOS 5 and higher
- Android 4 and higher
Supported Languages for Endpoint Security Clients

The Endpoint Security client is available in these languages:

- English
- Czech
- French
- German
- Italian
- Japanese
- Polish
- Russian
- Spanish

Client Hardware Requirements

The minimum hardware requirements for client computers to run the Total Endpoint Security Package are:

- 2 GB RAM
- 2 GB free disk space

Full Disk Encryption Requirements

Full Disk Encryption clients must have:

- 32MB of continuous free space on the client’s system volume

Note - During deployment of the Full Disk Encryption blade on the client, the Full Disk Encryption service automatically defragments the volume to create the 32MB of continuous free space, and suspends the Windows hibernation feature while the disk is encrypted.

Clients must NOT have:

- RAID.
- Partitions that are part of stripe or volume sets.
- Hybrid Drive or other similar Drive Cache Technologies. See sk107381 http://supportcontent.checkpoint.com/solutions?id=sk107381.
- The root directory cannot be compressed. Subdirectories of the root directory can be compressed.

UEFI Requirements

The new UEFI firmware that replaces BIOS on some computers contains new functionality that is used by Full Disk Encryption. Full Disk Encryption in UEFI mode requirements are:

- Windows 10 32/64-bit
- Windows 8.1 Update 1 32/64-bit
- Windows 7 64-bit
Unlock on LAN Requirements

- **Mac OS** - On Mac, you can use Unlock on LAN on computers that are shipped with OS X Lion or higher. You can also use Unlock on LAN with some earlier computers, if a firmware update is applied to the computer [http://support.apple.com/kb/HT4904](http://support.apple.com/kb/HT4904).

- **Windows** - On Windows, you can use Unlock on LAN on computers that support UEFI Network Protocol. UEFI Network Protocol is on Windows 8 logo certified computers that have a built in Ethernet port. The computer must be running Windows 8 in native UEFI mode and Compatibility Module Support (CSM) must not be enabled. On some computers, UEFI Network support must be manually enabled in the BIOS setup.


UEFI “Absolute Pointer” Keyboard-less Tablet Touch Requirements

Support for Pre-boot touch input on tablets (64-bit) requires:

- A Windows 8 logo certified computer
- The UEFI firmware must implement the UEFI Absolute Pointer protocol


Self Encrypting Drives (SED)

You can use Self Encrypting Drives with Full Disk Encryption. The requirements are:

- Supported Windows versions in UEFI mode
- UEFI firmware that implements the UEFI ATA Pass-through protocol or the UEFI Security Command Protocol
- TCG Opal compliant drives version 1.0 or 2.0

Check Point tested SED support with the drives in the table below. This is not a complete list of supported drives. The list shows drives explicitly tested by Check Point and known to satisfy the requirements for a Self Encrypting Drive.

<table>
<thead>
<tr>
<th>Hard Disk Drive Name</th>
<th>Opal Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seagate 250 GB Momentus Thin</td>
<td>1</td>
</tr>
<tr>
<td>Hitachi Travelstar ZK7320</td>
<td>1</td>
</tr>
<tr>
<td>Crucial M500 120 GB</td>
<td>2</td>
</tr>
<tr>
<td>Seagate 500 GB Momentus Thin</td>
<td>2</td>
</tr>
<tr>
<td>Seagate 500 GB Momentus Thin (FIPS 140-2)</td>
<td>2</td>
</tr>
<tr>
<td>SanDisk X300s 256 GB</td>
<td>2</td>
</tr>
<tr>
<td>Samsung 850 EVO 120GB</td>
<td>2</td>
</tr>
<tr>
<td>Intel SSD Pro 2500 180GB</td>
<td>2</td>
</tr>
<tr>
<td>Intel SSD 535 Series 360GB</td>
<td>2</td>
</tr>
</tbody>
</table>
### Self-Help Portal

The Self-Help Portal (SHP) adds Full Disk Encryption functionality to let users reset their own passwords. To use the Self-Help Portal, the user must register to the portal first.

The Self-Help Portal only works with Active Directory users. Make sure that the Endpoint Security Active Directory Scanner is configured and that the Active Directory is scanned.

The portal is available for desktop and mobile devices. These browsers and devices are supported:

**Mobile:**
- Google Chrome 41 or higher (Android 4 or higher)
- Android Browser (Android 4 or higher)
- Safari iOS 6.1.3 or higher

**Desktop:**
- Internet Explorer 9-11
- Mozilla Firefox 36.0.1 or higher
- Google Chrome 41 or higher

---

### Support for Single Sign-On (SSO) When Resuming from a Hibernated State

To use SSO from a hibernated state in Windows, the requirements are:

- Windows Vista or higher (Windows XP is not supported with this feature)
- **Windows GPO Interactive logon: Do not require CTRL+ALT+DEL** must not be disabled.

### Support for TPM

The TPM is used to enhance security by measuring integrity of Pre-boot components. To use TPM, you must enable it in the Full Disk Encryption policy. These system requirements apply:

- TPM hardware, according to specification 1.2 or 2.0
- Windows 7 32/64-bit or higher (Windows XP is not supported)

---

### Hard Disk Drive Name

<table>
<thead>
<tr>
<th>Hard Disk Drive Name</th>
<th>Opal Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>SK hynix SC305 128GB</td>
<td>2</td>
</tr>
<tr>
<td>SK hynix SC300 256GB</td>
<td>2</td>
</tr>
<tr>
<td>SK hynix SC300 512GB</td>
<td>2</td>
</tr>
</tbody>
</table>


---

**Client Requirements**

---

**E80.64 and R77.30.02 Release Notes**

---
Endpoint Offline Management Tool Requirements

Before you install the tool on a computer, make sure it has these prerequisites:

- We strongly recommend that the computer be protected by Firewall and Anti-Malware.
- Users must have administrator privileges.
- Microsoft Visual C++ 2008 SP1 Redistributable Package must be installed.
- .NET Framework 4.5 must be installed.

Media Encryption & Port Protection Support

Storage Devices:

- Standard USB 2.0 and 3.0 devices
- eSATA devices
- CD/DVD devices
- SD cards

Capsule Docs Supported Applications

After Capsule Docs clients are installed, they work in all supported applications:

- Microsoft Office 2016 32/64-bit
- Microsoft Office 2013 32/64-bit
- Microsoft Office 2010 32/64-bit
- Microsoft Office 2007 32-bit
- Microsoft Office 2003 32-bit (English version)
- Adobe Reader 8 - 11 and DC
- Adobe Acrobat Pro 8 and 9
Supported SmartConsole Platforms

The R77.30.02 SmartConsole is supported on these platforms:

**Microsoft Windows**

<table>
<thead>
<tr>
<th>Version</th>
<th>Editions</th>
<th>Arch.</th>
<th>SPs or Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Enterprise Pro 10</td>
<td>32/64-bit</td>
<td></td>
</tr>
<tr>
<td>8.1</td>
<td>Standard Enterprise Pro</td>
<td>32/64-bit</td>
<td>Update 1 (optional)</td>
</tr>
<tr>
<td>8</td>
<td>Standard Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Enterprise Professional Ultimate</td>
<td>32/64-bit</td>
<td>SP1</td>
</tr>
</tbody>
</table>

**Microsoft Windows Server**

<table>
<thead>
<tr>
<th>Version</th>
<th>Editions</th>
<th>Arch.</th>
<th>SPs or Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>All</td>
<td>64-bit</td>
<td></td>
</tr>
<tr>
<td>2012 R2</td>
<td>All</td>
<td>64-bit</td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>All</td>
<td>32/64-bit</td>
<td>SP1 or SP2</td>
</tr>
<tr>
<td>2008 R2</td>
<td>All</td>
<td>32/64-bit</td>
<td></td>
</tr>
</tbody>
</table>

**SmartEndpoint Requirements**

The minimum hardware requirements to run the SmartConsole, including SmartEndpoint are:

<table>
<thead>
<tr>
<th>Component</th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel Pentium Processor E2140 or 2 GHz equivalent processor</td>
</tr>
<tr>
<td>Memory</td>
<td>2GB</td>
</tr>
<tr>
<td>Available Disk Space</td>
<td>2GB</td>
</tr>
<tr>
<td>Video Adapter</td>
<td>Minimum resolution: 1024 x 768</td>
</tr>
</tbody>
</table>
Supported Windows versions:
SmartEndpoint supports all platforms listed in Supported SmartConsole Platforms (on page 14) with this additional requirement:
Microsoft Windows Servers 2008 (all editions) requires .NET Framework 4.5 installed before you install SmartEndpoint. If .NET 4.5 is not installed, the reports in the Reporting tab do not work correctly.

Supported Upgrade Paths

Supported Upgrades for Endpoint Security Management

These Endpoint Security Management Server upgrades are supported:
- In-place Upgrade from R77.30 to R77.30.02 with the R77.30.02 Hotfix
- Advanced Upgrade from R77.20.01 or R77.30.01 to R77.30.02

For other versions, you must upgrade to R77.30 and then install the R77.30.02 Hotfix.

To upgrade to R77.30.02 from R77.20.01 or R77.30.01 with Advanced Upgrade on Gaia:
2. Extract the files to a temporary folder.
3. Run: ./migrate export R77.30.02_migration_tools_Gaia.tgz
4. Copy the TGZ file to a fresh R77.30.02 computer and use the local migrate tools
   [FWDIR/bin/upgrade_tools] to run: ./migrate import R77.30.02_migration_tools_Gaia.tgz
5. Copy the MSI and Drivers folders from the original computer to the new computer.

You can only install a hotfix on top of R77.30.02 if the hotfix explicitly supports an upgrade from R77.30.02.

Supported Upgrades for Endpoint Security Client

Upgrade to E80.64 Endpoint Security client is available for versions E80.51, E80.61, and E80.62.
For earlier versions, contact Check Point Support.
Capsule Docs upgrades are supported from E80.60.

Note - The WebCheck Software Blade is not supported. If you have it installed from a previous version, you must remove it before you upgrade to this version.
Supported Upgrades to Windows 10

For existing Endpoint Security deployments, you must upgrade the clients to E80.64 and then upgrade the operating system to Windows 10 (version 1607).

Upgrades to Windows 10 (version 1607) with an earlier version of the Endpoint Security client are blocked by Microsoft.

The E80.64 client supports upgrades to Windows 10 (version 1607) from these earlier versions of Windows:

<table>
<thead>
<tr>
<th>Version</th>
<th>Editions</th>
<th>Arch.</th>
<th>SPs or Updates</th>
<th>Supported Blades</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 (version 1511)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>8.1</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td>Update 1</td>
<td>All</td>
</tr>
<tr>
<td>7</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td>SP1</td>
<td>All</td>
</tr>
</tbody>
</table>

Important for Windows 10 in-place upgrades to Windows 10 (version 1607):

If clients have Full Disk Encryption, see sk112246 http://supportcontent.checkpoint.com/solutions?id=sk112246.

If clients have Media Encryption & Port Protection, they must reboot again after the upgrade to make Media Encryption & Port Protection and Anti-Malware fully functional. A reboot message after the upgrade shows that the client is repaired and a reboot is necessary.

Legacy Full Disk Encryption Support

You can upgrade to E80.64 Full Disk Encryption from R73 and higher.

Legacy Media Encryption Support

Installation and Configuration

Before you install this release, make sure you have all requirements.

Installing an Endpoint Security Management Server

In all non-standalone deployments, the Network Security Management Server can also be an Endpoint Security Management Server. You can enable the Endpoint Security Management Server after the Network Security Management Server installation completes. Endpoint Security E80.64 clients work with the R77.30.02 server.

Get all files from the home page. [http://supportcontent.checkpoint.com/solutions?id=sk112793]

To install R77.30.02 on a Security Management Server:

1. Install R77.30 or upgrade to R77.30. Use the procedures in the R77.30 Release Notes [http://downloads.checkpoint.com/dc/download.htm?id=40107].
   Or use an existing R77.30 installation.
2. Install the R77.30 Jumbo Hotfix for Endpoint Security.
3. Install the R77.30.02 Hotfix.

Notes for Capsule Docs

• For automatic provisioning of users for Capsule Docs, users and computers must be scanned by the Endpoint Security Active Directory Scanner. For the Active Directory Scanner to work, you must assign Read permissions to the Active Directory path and to the folder with deleted objects, and configure the Active Directory Scanner on the Endpoint Security Management Server.

• For Capsule Docs to work, the Endpoint Security Management Server must be in the organization’s domain or configured to resolve Active Directory DNS names.

Installing the Hotfixes

Get all files from the home page. [http://supportcontent.checkpoint.com/solutions?id=sk112793]

To install the R77.30 Jumbo Hotfix for Endpoint Security:

1. Back up your R77.30 Security Management Server.
2. Create a temporary directory.
3. Download the installation file.
4. Save the file to a temporary directory.
5. Connect to the management server with SSH.
6. Run these commands in expert mode:
   • `tar -zxvf R77.30_jhf_T143_EP.tgz`
   • `./UnixInstallScript`
7. Reboot.
To install the R77.30.02 Hotfix:

1. Download the R77.30.02 installation file.
2. Save the file to a temporary directory.
3. Connect to the management server with SSH.
4. Run these commands in expert mode:
   - ```
     tar -zxvf R77.30.02.Gaia.tgz
     ```
   - ```
     ./UnixInstallScript
     ```
5. Reboot.
6. If you have Java 32-bit, upgrade to Java 64-bit ("Java Upgrades" on page 19).

Installing Endpoint Security Clients

For instructions on installation of Endpoint Security clients, see the *Endpoint Security Administration Guide*.

Installing the SmartConsole

To install the R77.30.02 SmartConsole:

Download the SmartConsole from the home page [http://supportcontent.checkpoint.com/solutions?id=sk112793](http://supportcontent.checkpoint.com/solutions?id=sk112793) and run it.

**Note** - If you have another version of R77.30 SmartConsole installed on your computer, you must first uninstall it, and then install the R77.30.02 SmartConsole.
Java Upgrades

By default, Endpoint Security Server installed on Gaia OS runs Java 32-bit. Endpoint Security Server also supports Java 64-bit, which provides better performance for systems with RAM size equal to or larger than 4GB.

To use an Endpoint Security Server in 64-bit mode, you must configure Gaia OS to automatically boot to the 64-bit kernel edition and upgrade Java to 64-bit.

To use an Endpoint Security Server in 64-bit mode:
1. Connect to command line on Gaia OS.
2. Log in to clish.
   Run: set edition 64-bit
4. Save the Gaia Database.
   Run: save config
5. Reboot the computer.
6. Make sure that the Gaia OS booted with the 64-bit kernel edition.
   Run: show version all

To upgrade to Java 64-bit:
Run: $UEPMDIR/system/utils/replace_ibm_jre_to_64_bit

To revert to Java 32-bit:
Run: $UEPMDIR/system/utils/replace_ibm_jre_to_64_bit uninstall

Known Limitations

See sk112794 http://supportcontent.checkpoint.com/solutions?id=sk112794 for known limitations that apply to this release.