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 E80.65
For more about this release, see the home page http://supportcontent.checkpoint.com/solutions?id=sk115512.

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=53790.
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 E80.65 and R77.30.03 Release Notes.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21 May 2017</td>
<td>Updated Client Hardware Requirements (on page 9)</td>
</tr>
<tr>
<td>01 March 2017</td>
<td>Improved formatting and document layout</td>
</tr>
<tr>
<td>13 February 2017</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Introduction

Check Point Endpoint Security E80.65 clients introduce new features and functionality on top of R77.30.03 Management.

What's New

This release supports all Software Blades and features of previous releases.
It includes new SandBlast Agent features and enhancements and support for new VPN features.

Anti-Ransomware

As part of the Forensics blade, Anti-Ransomware constantly monitors files and processes for unusual activity. Before a ransomware attack can encrypt files, Anti-Ransomware backs up files to a safe location. After the attack is stopped, it deletes files involved in the attack and restores the original files from the backup location.

Improved Browser Extension

The SandBlast Agent Browser Extension protects against malicious files that come from Internet sources. It supports Google Chrome for Threat Emulation, Threat Extraction, and Zero phishing.
The new Zero Phishing feature provides:
• **Phishing Prevention** - Checks different characteristics of a website to make sure that a site does not pretend to be a different site and use personal information maliciously.
• **Password Reuse Prevention** - Alerts users not to use their corporate password in non-corporate domains.

Simple Integration with Third Party Anti-Virus Vendors

Forensics can use information from the Windows Event Log to monitor and analyze malware events from third party anti-virus vendors.
• Works with most common vendors without manual configuration.
• Events are detected when the client is online or offline.
See sk116024 http://supportcontent.checkpoint.com/solutions?id=sk116024 for more information.

SandBlast Agent Dynamic Updates

SandBlast Agent dynamic updates enable stronger security for endpoints, with regular updates to SandBlast Agent files. This keeps clients protected from the latest threats.
Support for Multiple Login Options and Dynamic ID

E80.65 Remote Access VPN clients have the ability to connect to an IPsec VPN gateway that is configured with Multiple Login Options.

One of the authentication factors can be **Dynamic ID** - Users who successfully complete the first-phase authentication can be challenged to provide an additional credential: a Dynamic ID One Time Password (OTP). The OTP is sent by text message or email.

The new support requires an R80.10 or higher IPsec VPN gateway.


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>Number of cores</td>
<td>4</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
</tr>
<tr>
<td>Disk Space</td>
<td>100 GB</td>
</tr>
</tbody>
</table>

The requirements for External Endpoint Policy Servers are similar. Resource consumption is based on the size of your environment. For larger environments, more disk space, memory, and CPU are required.

- This Endpoint Security version supports R77.30 and R80 SmartLog.
- Endpoint Security Servers are not supported on Windows or RedHat Enterprise Linux releases.
Supported Check Point Versions

E80.65 clients on all supported Windows versions, including Windows 10, can be managed by R77.30.03, R77.30.02, 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 E80.65 features and capabilities, E80.65 clients must be managed by an R77.30.03 server.

R77.30.03 requires the dedicated R77.30 Jumbo Hotfix for Endpoint Security (aligned with take 143). This integrates security fixes into R77.30.03.

To support E80.65 Client logs in SmartView Tracker for R77.30 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 in English and 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>
</tbody>
</table>
**Client Requirements**

<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>7</td>
<td>Enterprise Professional</td>
<td>32/64-bit</td>
<td>SP1 Microsoft update KB3033929</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>Microsoft update KB3033929</td>
<td>Compliance, Anti-Malware, Firewall, Capsule Docs, SandBlast Agent Blades</td>
</tr>
</tbody>
</table>

**VMware ESXi**

<table>
<thead>
<tr>
<th>Version</th>
<th>Supported Blades</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1, 5.5, 6.0</td>
<td>All except: Full Disk Encryption and Media Encryption &amp; Port Protection</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.
- 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
You can use sk93032 to test your device for touch support

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
See sk108092 http://supportcontent.checkpoint.com/solutions?id=sk108092 for a list of drives explicitly tested by Check Point.

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)

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

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 or higher 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 R77.30.03 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</td>
<td>32/64-bit</td>
<td></td>
</tr>
<tr>
<td>8.1</td>
<td>Pro</td>
<td>32/64-bit</td>
<td>Update 1 (optional)</td>
</tr>
<tr>
<td>8</td>
<td>Pro</td>
<td>64-bit</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Enterprise Professional Ultimate</td>
<td>32/64-bit</td>
<td>SP1 Microsoft Update KB3033929</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 R2</td>
<td>All</td>
<td>32/64-bit</td>
<td>SP1 Microsoft Update KB3033929</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>4 GB</td>
</tr>
<tr>
<td>Available Disk Space</td>
<td>2 GB</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 12) 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 and R77.30.02 to R77.30.03 with the R77.30.03 Hotfix ("In-Place Upgrade" on page 15).

- Advanced Upgrade from R77.30.01 or R77.30.02 to R77.30.03 ("Advanced Upgrade" on page 16)

For other versions, see Endpoint Security Server Supported Upgrade Paths in sk109196 http://supportcontent.checkpoint.com/solutions?id=sk109196.

You can only install a hotfix on top of R77.30.03 if the hotfix explicitly supports an upgrade from R77.30.03.

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 for Endpoint Security Client

Upgrade to E80.65 Endpoint Security client is available for versions E80.51, E80.61, E80.62, and E80.64.

For earlier versions, contact Check Point Support.

Capsule Docs upgrades are supported from E80.60.

Supported Upgrades to Windows 10

For existing Endpoint Security deployments, you must upgrade the clients to E80.64 or E80.65 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 and E80.65 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 Professional</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

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 E80.65 Full Disk Encryption from R73 and higher.

Legacy Media Encryption Support

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

Installing an Endpoint Security Management Server
Get all files from the home page. (http://supportcontent.checkpoint.com/solutions?id=sk115512)

To install an R77.30.03 Endpoint Security Management Server:

   Or use an existing R77.30 installation.
2. Install the R77.30 Jumbo Hotfix for Endpoint Security. This is not necessary in an upgrade from R77.30.02.
3. Install the R77.30.03 Hotfix.
Installing the Hotfixes

Get all files from the home page. ([http://supportcontent.checkpoint.com/solutions?id=sk115512](http://supportcontent.checkpoint.com/solutions?id=sk115512))

If you upgrade to this release from R77.30.02, it is not necessary to install the R77.30 Jumbo Hotfix for Endpoint Security. Install only the R77.30.03 Hotfix.

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 R77.30.03 Hotfix:
1. Download the R77.30.03 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 R77.30.03.Gaia.tgz`
   - `./UnixInstallScript`
5. Reboot.
6. If you have Java 32-bit, upgrade to Java 64-bit ("Java Upgrades" on page 17).

In-Place Upgrade

Perform an in-place upgrade from R77.30 and R77.30.02 to R77.30.03 on the same machine.

In an environment with High Availability, Endpoint Policy Servers, or Remote Help Servers, you must upgrade in this order:
1. Upgrade the primary Endpoint Security Management Server.
2. Upgrade the secondary Endpoint Security Management Server.
3. Upgrade Endpoint Policy Servers and Remote Help Servers. The upgrade order among these components is not important.

To upgrade to R77.30.03 with an in-place upgrade:
- For upgrades from R77.30 - Install both Hotfixes, as described in Installing the Hotfixes (on page 15).
- For upgrades from R77.30.02 - Install only the R77.30.03 Hotfix, as described in Installing the Hotfixes (on page 15).
Advanced Upgrade

Perform an Advanced Upgrade from an existing to R77.30.01 or R77.30.02 Endpoint Security Management Server to a new, clean Endpoint Security Management Server on Gaia. Export the Endpoint Security database from the existing server and import it to the new server.

In an environment with High Availability, Endpoint Policy Servers, or Remote Help Servers:

1. After you complete the Advanced Upgrade of the primary Endpoint Security Management Server, you must install other servers as new installations and connect or sync them with the primary Endpoint Security Management Server. Use the instructions in the Endpoint Security Administration Guide.

2. In SmartDashboard, make sure that you delete server objects from the old installation and create new objects for new R77.30.03 servers.

To upgrade to R77.30.03 with Advanced Upgrade:

1. Install a new R77.30.03 Endpoint Security Management Server as described in Installing an Endpoint Security Management Server (on page 14).


3. Extract the files to a temporary folder on the existing Endpoint Security Management Server.

4. Export the database from the existing Endpoint Security Management Server.

   `<filename>` is a name that you choose for the .tgz file.

   • To automatically include all client MSI packages, run:
     ```bash
     ./migrate export --include-uepm-msi-files <filename>.tgz
     ```

   • To export files without MSI packages, run:
     ```bash
     ./migrate export <filename>.tgz
     ```

5. Copy the TGZ file to the new R77.30.03 Endpoint Security Management Server that you created.

6. On the new R77.30.03 Endpoint Security Management Server, use the local migrate tools (`$FWDIR/bin/upgrade_tools`) to run one of these commands.

   `<filename>` is the name of the .tgz file, as you entered it during the export.

   • To automatically include all client MSI packages, run:
     ```bash
     $FWDIR/bin/upgrade_tools/migrate import --include-uepm-msi-files <filename>.tgz
     ```

   • To import files without MSI packages, run:
     ```bash
     $FWDIR/bin/upgrade_tools/migrate import <filename>.tgz
     ```

7. If you did not export and import the MSI packages to the new server in the previous steps, copy them manually:

   a) Copy `$FWDIR/conf/SMC_Files/uepm/msi` from the source server to the same location on the target server.

   b) On the target server, change the permissions for the MSI folders. Run:

      (i) `cd $FWDIR/conf/SMC_Files/uepm`
      (ii) `chmod -R u+rwx,g+rwx,o-rwx msi/`
      (iii) `find msi/ -type d -exec chmod g+s {} \`

   c) Make sure that the permissions were changed correctly.
Installing Endpoint Security Clients

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

Installing the SmartConsole

To install the R77.30.03 SmartConsole:

Download the SmartConsole from the home page [http://supportcontent.checkpoint.com/solutions?id=sk115512](http://supportcontent.checkpoint.com/solutions?id=sk115512) 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 R77.30.03 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 sk115513 [http://supportcontent.checkpoint.com/solutions?id=sk115513](http://supportcontent.checkpoint.com/solutions?id=sk115513) for known limitations that apply to this release.