5 December 2017

ENDPOINT SECURITY
CLIENTS
E80.71

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 E80.71
For more about this release, see the E80.71 home page http://supportcontent.checkpoint.com/solutions?id=sk119676.

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=56991.
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 Endpoint Security Clients E80.71 Release Notes.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>05 Dec 2017</td>
<td>Updated What’s New in SandBlast Agent (&quot;What’s New&quot; on page 5), and Management Requirements (on page 6)</td>
</tr>
<tr>
<td></td>
<td>Fixed the link to the Endpoint Security Administration Guide (&quot;Client Deployment&quot; on page 11).</td>
</tr>
<tr>
<td>30 Nov 2017</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Introduction

Check Point Endpoint Security E80.71 clients introduces support for the Windows 10 Fall Creators Update Operating System, and other features.

What's New

This release supports all Software Blades and features of previous releases.
It adds support for Windows 10 Fall Creators Update (version 1709) and support for new and improved features.

In-place OS Upgrade Support
For in-place upgrades with the Full Disk Encryption Blade, refer to sk120667 http://supportcontent.checkpoint.com/solutions?id=sk120667

General Client Enhancements
- UserCheck Ultra HD Screens Support

Full Disk Encryption
- XTS-AES 128/256-bit encryption for BIOS systems
- Allow encryption algorithm change from AES-CBC to XTS-AES with seamless re-encryption, on UEFI-based computers.

Note- The XTS-AES encryption options require a management backend that supports them.

SandBlast Agent
- Anti-Exploit – Detects and prevents exploit-based attacks. Anti-Exploit gives protection by default to Web browsers, Microsoft Office applications, Adobe Acrobat Reader, and Adobe Flash Player. Anti-Exploit is able to detect and prevent the exploit attempt, before the attack downloads the malware and executes the malicious payload. If configured to Prevent mode, on detection Anti-Exploit shuts down the process being exploited and generates a forensics report. See sk121793 http://supportcontent.checkpoint.com/solutions?id=sk121793.

- SandBlast Agent for Browsers extension is upgraded to a new version and is now also supported on Internet Explorer 11. See sk108695 http://supportcontent.checkpoint.com/solutions?id=sk108695.

Media Encryption & Port Protection
- CryptoCore 4.0 support – Improved encryption speed, and a new password protection scheme.
  Note - Previous Media Encryption versions cannot authenticate with a password on media that is encrypted with the new version. However, Remote Help and Automatic access do work. The new Media Encryption version opens old and new versions.
Remote Access VPN


- Device Guard support – the Remote Access clients can be installed on a Microsoft Windows computer with Device Guard enabled.

- High DPI support - Support for devices with High-dots-per-inch (DPI) display.


Management Requirements

E80.71 clients can be managed by these Endpoint Security Management Servers: R80.10, R77.30.03, R77.30.02, R77.30, R77.30 EP6.5, R77.20 EP6.2.

Note - SandBlast Agent and Capsule Docs can be managed by these Endpoint Security Management Servers: R77.30.02 or R77.30.03.

See the server requirements in the release notes for your server version.

There is a new SmartConsole that supports E80.71 for each server version. Download it from the E80.71 home page http://supportcontent.checkpoint.com/solutions?id=sk119676.

To support E80.71 logs in SmartLog or SmartView Tracker for R77.30 servers, you must update the log schema. See sk106662 http://supportcontent.checkpoint.com/solutions?id=sk106662.

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 1709)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>10 (version 1703)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 (version 1607)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 LTSB (version 1607)</td>
<td></td>
<td></td>
<td></td>
<td></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

### 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>7</td>
<td>Enterprise Professional</td>
<td>32/64-bit</td>
<td>SP1 Microsoft update KB3033929</td>
<td>All</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 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 being 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 or Windows 10 logo certified computers that have a built-in Ethernet port. The computer must be running Windows 8 or Windows 10 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.

To troubleshoot UEFI network connectivity, see sk93709 http://supportcontent.checkpoint.com/solutions?id=sk93709.

UEFI "Absolute Pointer" Keyboard-less Tablet Touch Requirements

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

- A Windows 8 or Windows 10 logo certified computer
- The UEFI firmware must implement the UEFI Absolute Pointer protocol

You can use sk93032 to test your device for touch support http://supportcontent.checkpoint.com/solutions?id=sk93032.
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 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. This system requirement applies:

- TPM hardware, according to specification 1.2 or 2.0

Media Encryption & Port Protection Support

Storage Devices:
- USB 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 Upgrade Paths

Supported Upgrades for Endpoint Security Client

Upgrade to E80.71 Endpoint Security client is available from versions:
E80.51 EP6.0, E80.64, E80.65, E80.70.
For earlier versions, contact Check Point Support.

Supported Upgrades to Windows 10

For existing Endpoint Security deployments, you must upgrade the clients to E80.71 and then upgrade the operating system to Windows 10 (version 1709)
Upgrades to Windows 10 (version1709) with an earlier version of the Endpoint Security client are blocked by Microsoft.
The E80.71 client supports upgrades to Windows 10 (version 1709) 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 1703)</td>
<td>Enterprise</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>10 (version 1607)</td>
<td>Pro</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.1</td>
<td>Enterprise</td>
<td>32/64-bit</td>
<td>Update 1</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>Professional</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Enterprise</td>
<td>32/64-bit</td>
<td>SP1</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>Professional</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Important for Windows 10 in-place OS upgrades to Windows 10 (version 1709):
If clients have Full Disk Encryption, see sk120667
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 Supported Upgrades

You can upgrade to E80.71 Full Disk Encryption from R73 and higher and 7.5.1 and higher.

Legacy Media Encryption Supported Upgrades

Client Deployment


Installing the SmartConsole

To install the SmartConsole:

Download the SmartConsole for your server version from the E80.71 home page http://supportcontent.checkpoint.com/solutions?id=sk119676.

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

Known Limitations

See sk119677 http://supportcontent.checkpoint.com/solutions?id=sk119677 for known limitations that apply to this release.