Endpoint Security Clients

E80.70

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 E80.70
For more about this release, see the E80.70 home page http://supportcontent.checkpoint.com/solutions?id=sk117155.

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=55384
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 E80.70 Release Notes.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 May 2017</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Introduction

Check Point Endpoint Security E80.70 clients introduce new Operating System support and features.

What's New

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

Remote Access VPN

- Option to exclude local network traffic when Hub mode (Route all traffic) is configured.
- Register to hotspots with the computer’s default browser instead of the client’s embedded browser.
- Support for Multiple Login Options (from E80.65).

Third Generation OneCheck

The Full Disk Encryption OneCheck Logon features are improved to continue to work transparently with new versions of operating systems.

As part of the improvements, the Single Sign-on behavior has changed from previous releases. If the CTRL+ALT+DEL sequence is enforced from the group policy, users are always prompted to enter the CTRL+ALT+DEL sequence even if Single Sign-on is enabled. If a user enters the sequence within 60 seconds, the Single Sign-on process continues. If a user waits longer than 60 seconds, the regular logon window is shown. The time count begins when Check Point services are started on the client.

The local setting for enforcement of CTRL+ALT+DEL (that can be configured with Netplwiz.exe) is always set not to enforce CTRL+ALT+DEL. If the group policy is set, it has precedence over the local setting.

SandBlast Agent

The SandBlast Web Extension is supported on Internet Explorer 11. While the Web Extension is enabled automatically for Google Chrome, for Internet Explorer it is disabled by default. To enable it see Enabling the SandBlast Web Extension (on page 11).
Management Requirements

E80.70 clients can be managed by these Endpoint Security Management Servers: R77.30.03, R77.30.02, and R77.30.

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

There is a new SmartConsole that supports E80.70 for each server version.

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 1703)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>10 (version 1607)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 (version 1511)</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>
<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, SandBlast Agent Blades, Capsule Docs (Standalone Client)</td>
</tr>
<tr>
<td>2012 R2</td>
<td>All</td>
<td>64-bit</td>
<td></td>
<td>Compliance, Anti-Malware, Firewall, SandBlast Agent Blades, Capsule Docs (Standalone Client)</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, SandBlast Agent Blades, Capsule Docs (Standalone Client)</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 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.
- 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


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)

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 E80.70 Endpoint Security client is available for versions: E80.62 HF1, E80.64, E80.65, and E80.51 EP6.0.
For earlier versions, contact Check Point Support.

Supported Upgrades to Windows 10

For existing Endpoint Security deployments, you must upgrade the clients to E80.70 and then upgrade the operating system to Windows 10 (version 1703)
Upgrades to Windows 10 (version 1703) with an earlier version of the Endpoint Security client are blocked by Microsoft.
The E80.70 client supports upgrades to Windows 10 (version 1703) 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 1607)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<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 OS upgrades to Windows 10 (version 1703):**

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 E80.70 Full Disk Encryption from R73 and higher and 7.5.1 and higher.

**Legacy Media Encryption Support**


**Client Deployment**

Download the E80.70 client from the homepage [http://supportcontent.checkpoint.com/solutions?id=sk117155].

Installing the SmartConsole

To install the SmartConsole:

Download the SmartConsole for your server version from the home page [http://supportcontent.checkpoint.com/solutions?id=sk117155] 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 SmartConsole for this version.

Enabling the SandBlast Web Extension

Each Web Download Protection action from SmartEndpoint is a line in GuiDBedit with the class name `ep_orgp_te_web_downloads_protection_action`. By default there are three lines but there can be more if you created custom actions. Edit each line to enable the Web Extension on Internet Explorer for all users.

To enable the SandBlast Web Extension on Internet Explorer:

1. In GuiDBedit, go to `ep_orgp_te_policy_tbl`.
2. In each line with the class name `ep_orgp_te_web_downloads_protection_action`, find the field `browser_extensions_additional_data` and add the value: `ie_extension_disabled=false`.
3. Save the changes.
4. Open SmartEndpoint.
5. Make a small change in a SandBlast Agent Threat Emulation rule, which will cause it to load changes from GuiDBedit.
6. Install policy in SmartEndpoint.

Known Limitations

See sk117156 http://supportcontent.checkpoint.com/solutions?id=sk117156 for known limitations that apply to this release.