09 September 2021

ENDPOINT SECURITY
CLIENT FOR WINDOWS

E85.10

Release Notes
Check Point Copyright Notice

© 2021 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:
Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:
Refer to the Copyright page for a list of our trademarks.
Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.
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.

Certifications
For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point E85.10
For more about this release, see the E85.10 home page.

Latest Version of this Document
Open the latest version of this document in a Web browser. Download the latest version of this document in PDF format.

Feedback
Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>09 September 2021</td>
<td>Correction: Compatibility Module Support (CSM) to Compatibility Support Module (CSM) in &quot;Unlock on LAN Requirements&quot; on page 10</td>
</tr>
<tr>
<td>21 June 2021</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
# Table of Contents

- **What's New** ................................................................. 5
  - New Features .................................................................. 5
  - Enhancements .............................................................. 5

- **Management Server Requirements** .................................. 6
- **Client Requirements** ......................................................... 7
  - Supported Client Operating Systems ................................. 7
  - Supported Harmony Endpoint Browser Extension for Windows .................................................................. 9
  - Supported Languages for Endpoint Security Clients ................................................................. 9
  - Client Hardware Requirements ........................................ 9
  - Full Disk Encryption Requirements .................................. 10
  - Media Encryption & Port Protection Support ...................... 12
  - Capsule Docs Supported Applications ................................. 12

- **Supported Upgrade Paths** ................................................. 13
  - Supported Upgrades for Endpoint Security Client ............... 13
  - Supported Upgrades for Endpoint Security Client for ATMs ................................................................ 13
  - Supported Upgrades to Windows 10 .................................. 14
  - Legacy Client Supported Upgrades .................................... 15

- **Client Deployment** .............................................................. 16
What's New

New Features

- Sandblast Agent is now called Harmony Endpoint.
- Added Portuguese translations to the Client UI.
- During an upgrade from E85.10, the firewall stays connected.
- For standalone VPN clients (Endpoint Security VPN, Check Point Mobile, SecuRemote), there is an option to suppress the firewall compliance warning, if the firewall is not part of the installation.
- Customers can now execute PowerShell scripts on client machines, using push operations. See sk173414.
- Added a new sensor to extract the contents of newly created Batch files. This data can be viewed in the Forensics reports, as well as in Threat Hunting.
- New Outlook sensor installed as an add-in is now available to report high-level email data to Threat Hunting. In addition, attacks that started with an email attachment now show the email details in Forensics. Note: Contents of the email are not stored.
- Threat Hunting includes the ability to view MAC addresses for every computer sending data.
- There is a new CLI utility to restore all files from the backup and restoration folder manually.
- Enables you to assign the "Connected" policies to a configured inner source location, instead of to the Endpoint Security Management Server. This allows you to distinguish if the Endpoint Security Client is in the organization network or not.
- Browser Extension New Capability: Enforce Safe Search: The Administrator can compel his Endpoint users to use the "Safe Search" feature when they employ the Google, Bing and Yahoo search engines. "Enforcing Safe Search" is done by configuring the Web-protection policy. The Endpoint user is unable to change these settings. For more information about Safe Search, refer to: https://support.google.com/websearch/answer/510?co=GENIE.Platform%3DAndroid&hl=en

Enhancements

For the complete list of enhancements, refer to sk173386.
Management Server Requirements

- You can manage the E85.10 clients with these Endpoint Security Management Servers: R81, R80.40, R80.30, R80.20, R80.20.M2, and R80.10.

  **Notes:**
  
  - BitLocker Management requires R80.40 or version R80.30 with a Hotfix. See the [BitLocker Management Release Notes](#).
  - You can manage Harmony Endpoint and Capsule Docs with these Endpoint Security Management Servers: R80.40, R80.30, R80.20, and R80.20.M2. See the server requirements in the Release Notes for your server release.

- The new Threat Emulation report format is available with E80.90 clients and higher. To enable the feature on Endpoint Security Management Server versions older than R80.30, see [sk152752](#).

- Anti-Malware in the E80.89 client and higher requires a Management Server update to support receiving signatures updates from the Endpoint Security Management Server. See [sk141033](#).

- Full Disk Encryption users that receive an error when uploading E85.10 to the Endpoint Security Management Server must replace the SmartConsole installation with the version available in the E85.10 [home page](#).

- Clients E80.87 and higher require a Management Server update to view the logs on SmartLog on Endpoint Security Management Server versions older than R80.20. See [sk106662](#).
Client Requirements

This section shows the requirements for Endpoint Security clients.

## Supported Client Operating Systems

### Microsoft Windows

<table>
<thead>
<tr>
<th>Version</th>
<th>Editions</th>
<th>Architecture</th>
<th>SPs or Updates</th>
<th>Supported Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 21H1 (version 2103)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>10 20H2 (version 2009)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 20H1 (version 2004)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 19H2 (version 1909)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 19H1 (version 1903)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 LTSC (version 1809)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 (version 1809)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 (version 1803)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 (version 1709)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 LTSE (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>
<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>Architecture</th>
<th>SPs or Updates</th>
<th>Supported Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>All</td>
<td>64-bit</td>
<td></td>
<td>Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Capsule Docs (Standalone Client), Media Encryption and Port Protection.</td>
</tr>
<tr>
<td>2016</td>
<td>All</td>
<td>64-bit</td>
<td></td>
<td>Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Capsule Docs (Standalone Client).</td>
</tr>
<tr>
<td>2012</td>
<td>All</td>
<td>64-bit</td>
<td></td>
<td>Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, 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, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, 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, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Capsule Docs (Standalone Client)</td>
</tr>
</tbody>
</table>

**Notes:**

- To support Endpoint Compliance rules for Windows Server 2016 on versions older than R80.20, see [sk122136](https://www.symantec.com/security_response).  
- Terminal Servers are not supported.  
- Windows Server CORE is not supported.

## VMware ESXi

<table>
<thead>
<tr>
<th>Version</th>
<th>Supported Features</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>

**Note** - If you install a client package with features that are not supported on the server, the installation succeeds but only the supported features are installed.
Supported Harmony Endpoint Browser Extension for Windows

Harmony Endpoint Browser Extension for Windows clients browsers support:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Chrome</th>
<th>Microsoft Edge (Chromium)</th>
<th>Firefox</th>
<th>Internet Explorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Download Protection</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Credential Theft protection including Zero-Phishing and Corporate-password-reuse protection</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>URL Filtering (for Web Management users only)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
</tr>
</tbody>
</table>

Note - Activation of the extension on Firefox ESR requires the user's manual approval.

Supported Languages for Endpoint Security Clients

The Endpoint Security client is available in these languages:

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

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

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

- 8 GB RAM
- 6 GB free disk space
Full Disk Encryption Requirements

This section applies to Check Point Full Disk Encryption and not BitLocker Management.

Full Disk Encryption clients must have:

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

**Note** - During deployment of Full Disk Encryption 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 equivalent Drive Cache Technologies. See [sk107381](#).
- The root directory that is compressed (compressed sub-directories of the root directory are supported).

**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 use Unlock on LAN with some earlier computers, if a firmware update is applied to the computer.

  - **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 Support Module (CSM) must not be enabled. On some computers, UEFI Network support must be manually enabled in the BIOS setup.

For troubleshooting the UEFI network connectivity issues, see [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

See [sk93032](#) for information about touch support on your device.
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 for a list of drives explicitly tested by Check Point.

See sk93345 for information about compatibility of a UEFI computer with SED Opal encryption for Check Point Full Disk Encryption.

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, based on 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 operate in all supported applications.

The supported applications are:
- Microsoft Office - Supported versions are described in sk157772
- Adobe Reader DC
Supported Upgrade Paths

Supported Upgrades for Endpoint Security Client

Upgrade to the E85.10 Endpoint Security client is available from E81.00 and higher.

Supported Upgrades for Endpoint Security Client for ATMs

Upgrade to E85.10 Endpoint Security client for ATMs is available from:

- E80.86 and higher Endpoint Security client for ATMs
- E80.71 Endpoint Security client for ATMs
- E80.64 Remote Access VPN client for ATMs
- E75.30 Remote Access VPN client for ATMs

For more information and downloads, see sk133174.
Supported Upgrades to Windows 10

- For existing Endpoint Security deployments, you must upgrade the clients to E85.10 and then upgrade the operating system to Windows 10 (version 2103).
- Upgrades to Windows 10 (version 2004) with an Endpoint Security client version earlier than E83.15 are blocked by Microsoft.
- Upgrades to Windows 10 (version 1903) with an Endpoint Security client version earlier than E81.10 are blocked by Microsoft.
- The E85.10 client supports upgrades to Windows 10 (version 2103) from these earlier versions of Windows:

<table>
<thead>
<tr>
<th>Version</th>
<th>Editions</th>
<th>Architecture</th>
<th>SPs or Updates</th>
<th>Supported Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 (version 2009)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>10 (version 2004)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>10 (version 1909)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>10 (version 1903)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td>Update 1</td>
<td>All</td>
</tr>
<tr>
<td>10 (version 1809)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>10 (version 1803)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>10 (version 1709)</td>
<td>Enterprise Professional</td>
<td>32/64-bit</td>
<td>SP1</td>
<td>All</td>
</tr>
<tr>
<td>8.1</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></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>

**Note** - Upgrade to Windows 10 LTSC (version 1809) is not supported.

**Important Note for Windows 10 (version 1709 and earlier):**
Clients with **Media Encryption and Port Protection** must reboot again after the upgrade to make MEPP fully functional. A reboot message after the upgrade shows the client as repaired and a reboot is necessary. This is a requirement for Windows 10 (version 1709 and earlier).

**Important for Windows 10 in-place OS upgrades to Windows 10 (version 1909):**
If clients have **Full Disk Encryption**, see sk120667.
Legacy Client Supported Upgrades

- **Legacy Media Encryption client**
  See [sk99116](#) for supported legacy Media Encryption upgrades.

- **Legacy Full Disk Encryption client**
  The supported upgrade path for the legacy Full Disk Encryption client is to upgrade from 7.5.1 to E80.82, and then from E80.82 to E85.10.

  !important - Follow [sk110420](#) to upgrade from E80.82 to E81.10 or higher before you upgrade to E85.10
Client Deployment

Download the E85.10 client from the E85.10 home page.

See the Endpoint Security Administration Guide for your version > Chapter Deploying Endpoint Security Clients.