ENDPOINT SECURITY CLIENT

E83.10
for Windows

Release Notes
Check Point Copyright Notice

© 2020 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 E83.10**
For more about this release, see the E83.10 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>22 Jun 2020</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
# Table of Contents

What's New .......................................................................................................................... 5

Management Requirements ............................................................................................... 8

Client Requirements .......................................................................................................... 9
  Supported Client Operating Systems ............................................................................ 9
  Supported Languages for Endpoint Security Clients .................................................. 10
  Client Hardware Requirements .................................................................................... 10
  Full Disk Encryption Requirements ............................................................................. 11
  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 .......................................................................... 13
  Legacy Client Supported Upgrades ............................................................................ 14

Client Deployment ............................................................................................................ 15
What's New

New Features

- Endpoint Security now supports VMware Horizon VDI (Virtual Desktop Infrastructure), persistent and non-persistent. See the Endpoint Security VDI E83.10 Administration Guide.

- Adds a SandBlast Agent Chrome Browser Extension with URL Filtering capabilities.
  
  Note: The feature is available for SandBlast Agent Web Management users. It is in Early Availability mode for Chrome users.

- E83.10 shows a customized icon for encrypted drives.

Enhancements

- Anti-Malware
  
  - Resolves an issue where an Anti-Malware scheduled scan happens even if it is not in the policy.
  
  - Resolves Anti-Malware icon scaling issue.
  
  - Resolves a possible issue where the Anti-Malware process crashes as it shuts down.

- Anti-Ransomware, Behavioral Guard and Forensics
  
  - Behavioral Guard now protects against the Pass The Hash technique for credential theft. Credential Dumping is new as of the previous release.
  
  - Fixes an issue where Anti-Ransomware does not detect a potential attack when the user is not logged in.
  
  - Fixes Anti-Ransomware false positives due to user profile deletions.
  
  - Fixes multiple rare cases of false positives in Anti-Ransomware.
  
  - Fixes an issue where "out of memory" errors occur when the log lists a very large number of backups.
  
  - When you disable Anti-Ransomware, the backup driver no longer operates.
  
  - Improves performance as Forensics now stores fewer named objects such as mutexes and events.
  
  - Improves the performance of Forensics, Behavioral Guard and Threat Hunting with enhancements to our Registry Operation exclusion algorithms that reduce the number of recorded registry operations.

- Firewall and Application Control
  
  - Resolves client network issues after a Firewall driver uninstallation failure.
  
  - Resolves a rare issue where an added Firewall blade sticks in the "Initializing" state.
• Resolves a possible upgrade issue where the Firewall blade does not start due to a WatchDog failure.

• Resolves a rare issue where the Firewall policy is "Not Set" in the client after the policy download from the server.

- **Full Disk Encryption**
  • Resolves a possible issue where the Disk Encryption process crashes during shutdown.

- **Media Encryption and Port Protection**
  • Resolves a removable media icon blink issue for an encrypted partition when Media Scan is enabled.

- **VPN**
  • Improves the work with non-UTF-8 applications. Users can toggle UTF-8 support.
  • Fixes active File Transfer Protocol (FTP) traffic blocks on a standalone VPN client with Firewall.
  • Includes stability and quality fixes. Supports all the features of previous releases.

- **Installation**
  • Resolves a possible issue where uninstalling the Endpoint removes components that are necessary for other applications.
  • Resolves a possible issue where the uninstall fails after the user turns off "Network Protection".
  • Resolves a possible issue where the Endpoint Security client does not run correctly after an operating system upgrade.
  • Resolves a rare issue where the client uninstall fails with Error 1921: "Service Check Point Endpoint Agent (CPDA) could not be stopped".
  • Resolves a rare issue where an upgrade that uses "Dynamic Package" continuously loops after a download fails to resume.
  • The pre-boot language selection choice is now correct after a language update in Windows.
  • Fixes an incompatibility issue with Sophos Antivirus which could not install on a machine with Endpoint Security client on it.

- **Infrastructure**
  • Resolves a rare User Interface (UI) issue where a malware resolution does not show to a user.
  • Resolves a client LogViewer issue where it only shows log records that match the latest log schema.
  • On the Endpoint Security client screen, the Overview list now shows "Anti-Bot and URL Filtering" instead of "Anti-Bot".
• The client User Interface (UI) no longer shows during manual upgrades.
• Resolves URL infections report issues in the User Interface (UI) so that the infections records are not permanent in the client and server UIs.
• Anti-Bot and URL Filtering policy now translates to all supported languages.

General
• Improves the performance of the Endpoint Security core driver to reduce CPU consumption.
Management Requirements

- E83.10 clients can be managed by these Endpoint Security Management Servers: R80.40, R80.30, R80.20, R80.20.M2, R80.10.

  **Note:**
  - BitLocker Management requires R80.40 or version R80.30 with a Hot Fix. See the [BitLocker Management Release Notes](#).
  - SandBlast Agent and Capsule Docs can be managed by the R80.40, R80.30, R80.20, and R80.20.M2 Endpoint Security Management Server. 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 versions older than R80.30, see [sk152752](#).

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

- FDE users that encounter an error when uploading E83.10 to the Endpoint Security Management Server must replace the SmartConsole installation with the version available in the E83.10 [home page](#).

- E80.87 and higher require a management 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, including supported operating systems and hardware requirements.

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 Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 19H2 (version 1909)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</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 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>
<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 Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>All</td>
<td>64-bit</td>
<td></td>
<td>Compliance, Anti-Malware, Firewall, SandBlast Agent features, Capsule Docs (Standalone Client)</td>
</tr>
<tr>
<td>2016 (*)</td>
<td>All</td>
<td>64-bit</td>
<td></td>
<td>Compliance, Anti-Malware, Firewall, SandBlast Agent features, Capsule Docs (Standalone Client)</td>
</tr>
<tr>
<td>2012</td>
<td>All</td>
<td>64-bit</td>
<td></td>
<td>Compliance, Anti-Malware, Firewall, SandBlast Agent features, 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 features, Capsule Docs (Standalone Client)</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 Features</th>
</tr>
</thead>
<tbody>
<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 features, Capsule Docs (Standalone Client)</td>
</tr>
</tbody>
</table>

(*) To support Endpoint Compliance rules for Windows Server 2016 on versions older than R80.20, see [sk122136](#).

(**) **Note** - Terminal Servers are not supported.

(***') **Note** - 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 Languages for Endpoint Security Clients**

The Endpoint Security client is available in these languages:

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

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 other similar Drive Cache Technologies. See 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.
- **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.

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.
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, to test a UEFI computer for compatibility 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, 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. 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 E83.10 Endpoint Security client is available from versions: E80.64 and higher.

Supported Upgrades for Endpoint Security Client for ATMs

Upgrade to E83.10 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 E83.10 and then upgrade the operating system to Windows 10 (version 1909).

Upgrades to Windows 10 (version 1903) with an Endpoint Security client version earlier than E81.10 are blocked by Microsoft.

The E83.10 client supports upgrades to Windows 10 (version 1909) 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 Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 (version 1903)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</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>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>

Note - Upgrade to Windows 10 LTSC (version 1809) is not supported.
Important for Windows 10 in-place OS upgrades to Windows 10 (version 1909):

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 needed.

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 E83.10.
Client Deployment

Download the E83.10 client from the E83.10 Endpoint Security Client for Windows home page.

See Deploying Endpoint Security Clients in this Guide:

- R80.40 Endpoint Security Administration Guide