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 https://www.checkpoint.com/products-solutions/certified-check-point-solutions/.

Check Point E82.10
For more about this release, see the E82.10 home page https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doViewsolutiondetails=&solutionid=sk163578.

More Information

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 http://downloads.checkpoint.com/dc/download.htm?ID=100723.

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 E82.10 Release Notes.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22 December 2019</td>
<td>Adding CVE-2019-8463 as an Install Enhancement</td>
</tr>
<tr>
<td>24 November 2019</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
What's New

New Feature:

- E82.10 adds support for Endpoint on Windows 10 19H2 (version 1909).

Enhancements

- Compliance
  - Fixes an issue when the Compliance blade fails to detect the McAfee Endpoint Security running status if no user is logged in.

- Anti-Malware
  - Fixes an issue where the Endpoint Security client upgrade fails because the Anti-Malware process fails to unload.
  - Fixes an issue for sites blocked by Anti-Malware web protection.
  - Fixes an issue where Endpoint Security significantly slows the Kaspersky Endpoint Protection upgrade process.

- Anti-Ransomware, Behavioral Guard and Forensics
  - Fixes an issue where symbolic links with Anti-Ransomware honeypot restoration may allow Denial of Service attacks.
  - Older Anti-Ransomware honeypots are now deleted on upgrades.
  - Fixes an issue where Anti-Ransomware honeypots are not created on newer locations like program data and app data when upgrading from an earlier version of the product.
  - Fixes an Anti-Ransomware False Positive that can occur due to the VMware Horizon Persona Management application.
  - Improves performance of the injection sensor when many processes are launched in a short period of time.
  - Fixes an issue that may cause the Forensics Analysis to include benign processes when NVIDIA processes are launched prior to the Logon screen appearing.
  - Fixes an issue where the entire Forensic incident is not analyzed if it involves the use of NTFS Alternate Data Streams.
  - Fixes an issue where some IPv6 addresses are not correctly identified as internal IPs for the RDP Brute Force detection in Behavioral Guard.

- Media Encryption and Port Protection
  - Fixes an issue where Media Encryption and Port Protection does not update Offline Data Access utility on an encrypted removable media.

- Full Disk Encryption
  - Fixes a rare issue where an FDE process crashes when switching from BitLocker Management to FDE.

- VPN
  - Includes stability and quality fixes. Supports all the features of previous releases.
  - Improves the log mechanism. Logs will stay on the machine for a longer time.
  - Includes performance improvements with large scale topology.
• Install
  • CVE-2019-8463: Resolves a denial of service vulnerability in releases before E82.10 to prevent service log files storing in non-standard locations.

• General
  • The initial connection to the server does not require the Endpoint Security client to be connected to the domain controller.
  • Fixes an issue for the Endpoint Security client to report its name to display accurately in Deployment reports of Smart Endpoint.
  • Fixes a rare case of BSOD that may happen during an arbitrary process creation.
Management Requirements

- E82.10 clients can be managed by these Endpoint Security Management Servers: R80.30, R80.20, R80.20.M2, R80.10, R77.30.03, R77.30, R77.30 EP6.5, R77.20 EP6.2.
  
  **Note:**
  - SandBlast Agent and Capsule Docs can be managed by the R80.30, R80.20, R80.20.M2 and R77.30.03 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 [http://supportcontent.checkpoint.com/solutions?id=sk152752](http://supportcontent.checkpoint.com/solutions?id=sk152752).


- FDE users that encounter an error when uploading E82.10 to the Endpoint Security Management Server must replace the SmartConsole installation with the version available in the E82.10 home page [https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk163578](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk163578).

# 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 Professio nal</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>
</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>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>
<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>


(**) **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
- 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

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 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. The supported applications are:

- Microsoft Office - Supported versions are described in sk157772 https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk157772.
- Adobe Reader DC
Supported Upgrade Paths

Supported Upgrades for Endpoint Security Client

Upgrade to E82.10 Endpoint Security client is available from versions: E80.64 and higher.

Supported Upgrades for Endpoint Security Client for ATMs

Upgrade to E82.10 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

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetail
s=&solutionid=sk133174&partition=General&product=Endpoint.

Supported Upgrades to Windows 10

For existing Endpoint Security deployments, you must upgrade the clients to **E82.10** 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 E82.10 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 (1903)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>10 (1809)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 (1803)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 (1709)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</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 Pro</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**
  

- **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 E82.10.
Client Deployment


See Deploying Endpoint Security Clients in the:

- **R77.30.03 Endpoint Security Administration Guide**
  http://downloads.checkpoint.com/dc/download.htm?ID=53788

- **R80.20 Endpoint Security Administration Guide**