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 E80.96**
For more about this release, see the E80.96 home page

**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

To learn more, visit the Check Point Support Center

**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 E80.96 Release Notes.

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 April 2019</td>
<td>First release of this document.</td>
</tr>
</tbody>
</table>
Contents

Important Information ................................................................................................... 3
What’s New ................................................................................................................... 5
Management Requirements .......................................................................................... 7
Client Requirements ....................................................................................................... 8
  Supported Client Operating Systems ........................................................................ 8
  Supported Languages for Endpoint Security Clients ................................................ 9
  Client Hardware Requirements ................................................................................. 9
  Full Disk Encryption Requirements ......................................................................... 10
  Media Encryption & Port Protection Support ............................................................ 11
  Capsule Docs Supported Applications .................................................................... 11
Supported Upgrade Paths .............................................................................................. 12
  Supported Upgrades for Endpoint Security Client ................................................ 12
  Supported Upgrades for Endpoint Security Client for ATMs ................................... 12
  Supported Upgrades to Windows 10 ....................................................................... 12
  Legacy Client Supported Upgrades ......................................................................... 13
Client Deployment ....................................................................................................... 14
What's New

Enhancements

- Anti-Malware
  - Resolves a rare issue where Anti Malware protection does not run after an upgrade.
  - Fixes an issue where Anti-Malware shows an incorrect status in UI in some cases. This is only relevant to the E2 package.
  - Fixes an issue where sometimes the OfflineUpdater tool fails to update the signatures database on the client side.

- Capsule Docs
  - Fixes an issue that may cause a failure in an upgrade or in an uninstall process.

- Anti-Ransomware, Behavioral Guard and Forensics
  - The latest version of the Anti-Ransomware Honeypots are now correctly installed when upgrading from previous versions.
  - Anti-Ransomware Honeypots no longer stop working if they receive a second Anti-Ransomware policy update.
  - Disabling Forensics now correctly disables Anti-Ransomware completely, including removing all Anti-Ransomware Honeypot files.
  - Fixes an issue where Process information is corrupted before inserting into the Forensics Database. With the fix, the number of instances of unknown processes in a Forensics report is dramatically reduced.
  - Fixes a rare case where the last received Forensics, Anti-Ransomware and Behavioral Guard policies are not saved and used when the client cannot connect to the Management Server.
  - Fixes a rare crash in Forensics when receiving policy before the full Forensics initialization is complete.
  - Fixes an issue where certain exclusions for Anti-Ransomware are not enforced if the user logs in before the full service initialization is complete.

- Threat Emulation and Anti-Exploit
  - Resolves an issue where, in some cases, Threat Emulation may not deploy the SBA4B Chrome extension if a user has other (non-Check Point) extensions.
  - Makes sure that Threat Emulation avoids a crash when the database is very large.
  - Anti-Exploit now turns off completely when used with a third party Anti-Virus. Check Point’s Anti-Malware will not cause Anti-Exploit to disable.
  - Fixes a very rare issue where Anti-Exploit does not completely parse the policy from the Management.

- Install / Uninstall
  - Fixes a rare case where an unrequired reboot occurs after upgrade.
  - Resolves a rare issue where a crash happens on an uninstall and upgrade.
  - Changes the upgrade retry frequency and removes unnecessary user interface popups.
• Removes a "Validation failed" message that shows in error during an upgrade from an old version.
• Updates the list of supported Windows 10 versions in Compliance blade to include versions 1809 and 1803.

• Infrastructure
  • Fixes an issue where the Full Disk Encryption policy is sometimes not updated.
  • Improves the security of the client when using hard linked files:
    ▪ CVE-2019-8452: Prior to Check Point Endpoint Security client for Windows E80.96, a hard-link from the log file archive to any file on the system changes permission so that all users can access the linked file. Doing this on files with limited access gains the local attacker higher privileges to the file.
    ▪ CVE-2019-8454: Prior to Check Point Endpoint Security client for Windows E80.96, a local attacker can create a hard-link between a file to which Endpoint Security client for Windows writes and another BAT file. Then, by impersonating the WPAD server, the attacker can write BAT commands into that file to be run later by the user or the system.

• General
  • Reduces end-user popups and notifications to the items that require user knowledge or intervention.
Management Requirements

E80.96 clients can be managed by these Endpoint Security Management Servers: 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 R80.20, R80.20.M2 and R77.30.03 Endpoint Security Management Server.

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

There are new SmartConsoles that support E80.96. Download SmartConsole from the E80.96 Endpoint Security client for Windows home page
http://supportcontent.checkpoint.com/solutions?id=sk150012. If you have another version of SmartConsole installed on your computer, you must first uninstall it, and then install the SmartConsole for this release.

Important - Download SmartConsole with the E80.96 client to avoid "signature verification failed" messages when uploading the client to the SmartConsole.

To support SmartLog or SmartView Tracker reporting for all supported servers (except R80.20), you must update the log schema. Follow instructions in 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 (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></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 (version 1703)</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 you must install a server Hotfix. See sk122136 http://supportcontent.checkpoint.com/solutions?id=sk122136.

(**) Note - Terminal Servers are 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

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 2016 32/64 bit
- Microsoft Office 2013 32/64-bit
- Microsoft Office 2010 32/64-bit
- Microsoft Office 2007 32-bit
- Adobe Reader DC
Supported Upgrade Paths

Supported Upgrades for Endpoint Security Client

Upgrade to E80.96 Endpoint Security client is available from versions:
E80.64 and higher.

Supported Upgrades for Endpoint Security Client for ATMs

Upgrade to E80.96 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 E80.96 and then upgrade the operating system to Windows 10 (version 1809)

Upgrades to Windows 10 (version 1809) with an earlier version of the Endpoint Security client are blocked by Microsoft.

The E80.96 client supports upgrades to Windows 10 (version 1809) 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 (1803)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>10 (1709)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>10 (1703)</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 Pro</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 1809):
If clients have Full Disk Encryption, see sk120667 http://supportcontent.checkpoint.com/solutions?id=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 E80.96.
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**