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 E80.90
For more about this release, see the E80.90 home page http://supportcontent.checkpoint.com/solutions?id=sk143452.

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=78886.
To learn more, visit the Check Point Support Center https://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 E80.90 Release Notes.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26 February 2019</td>
<td>Release to add a version to the supported client operating system list</td>
</tr>
<tr>
<td>13 January 2019</td>
<td>Release to correct the supported client operating system list</td>
</tr>
<tr>
<td>06 January 2019</td>
<td>Release to add support for Windows Server 2019</td>
</tr>
<tr>
<td>31 December 2018</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
What's New

New Features

- Windows 10 October 2018 Update Support.
- Enhanced Fileless and Malicious Powershell Detections engine extending Behavioral Guard capabilities.
  - This new engine provides a multi-phase ability to detect malicious PowerShell usage that is unique.
  - Includes full AMSI (Advanced Malware Scan Interface) integration to get, analyze and report decoded scripts.
- Forensic report overhaul with a new style and enhanced reputation integration.
  - Completely redesigned Overview and General screens.
  - Many small usability and visual enhancements throughout the report.
  - View decoded script content as part of the report itself.
  - See the enhancements section below for additional information.
- Forensics now has major performance improvements.
  - There is a major reduction (roughly 50% fewer events) in the amount of data stored.
    - This results in lower IO usage and better performance.
  - See the enhancements below for the full list of performance enhancements.
- Forensics Analysis takes on average 20% less time to complete.
  - For larger reports the time taken will be further reduced.
- Stack Pivoting detection was turned on as a new exploit detection technique for Anti-Exploit.
  - Stack Pivoting involves trying to create a fake stack from attacker controlled memory.
- Anti-Exploit now default protects the Equation Editor process.
  This helps to cover the following CVEs:
  - CVE-2017-11882
  - CVE-2018-0802
  - CVE-2018-0812

Enhancements

- Anti-Ransomware, Behavioral Guard and Forensics
  - Enhances Behavioral Guard with the ability to do deep inspections of both behavior and script content of PowerShell and Fileless attacks.
  - Improves Forensic reports with decoded PowerShell scripts from AMSI integration.
    - This feature is only available in Windows 10.
  - Adds many new suspicious events for the Forensic report, including new PowerShell related suspicious events.
  - Fixes a crash occurring when Forensics, Anti-Ransomware and Behavior Guard are processing an existing policy while receiving a new policy.
• Fixes a rare issue with large continuous CPU utilization when the Forensics service is unable to communicate with the driver.

• Improves Forensic performance by adding static exclusions for well known file operations. This addition alone can reduce the number of file operations stored by up to 80% on some machines.

• Improves Forensics performance by adding dynamic exclusions for file operations based on a new heuristic. This can reduce the number of file operations stored by up to 30%.

• Improves Forensic performance by dynamically excluding registry operations based on a new heuristic. On average, 10% of registry operations are now excluded.

• Fixes an issue which caused duplication of log events in Forensics.

• Improves Entry Point calculations across multiple scenarios to be more accurate in the Forensic Report.

• Fixes a majority of issues where the Entry Point of an attack could be empty. Now there should almost always be an Entry Point.

• Improves the Forensics report so that Command Prompts (cmd.exe) opened for typing no longer appear in the Forensic report, but may appear in the Entry Point instead.

• Improves the Forensic Analysis to consider following files in the argument of processes already included as part of the incident.

• The Forensics report now shows the termination status for every process present in the report.

• Fixes an issue that could lead to incomplete termination of processes involved in a Ransomware incident.

• Processes showing in a report that are closed at the time of the generation of the report will now correctly show as terminated, even if the remediation policy for termination is disabled.

• Fixes an issue where some Forensic report icons may be missing when upgrading to E80.89. The icons are now present when upgrading to E80.90.

• Fixes an issue with the scroll bar not appearing correctly if there are multiple nodes in the Entry Point view of the Forensics Report.

• Fixes a Forensics Analysis issue where script processes like PowerShell do not appear in the report when Cmd is involved and the script process is not the trigger.

• Process arguments and script contents are now encoded in the Forensic reports. This prevents the deletion of the reports by Anti-Viruses looking for specific signatures found in the argument or script content.

• Adds support to include the Malware Family from URL reputation if present in the Forensic report.

• Fixes an issue which could result in the User Name appearing empty in the Forensic Report.

• Fixes a visual issue in the Forensic report where the distance between processes could be very large if a process has a lot of lines of text.

• Updates the default exclusions for Anti-Ransomware.
• Threat Emulation and Anti-Exploit
  • Anti-Exploit now has an additional exploit prevention technology called stack pivoting.
  • Anti-Exploit now protects Equation Editor from known and unknown exploit attempts.

• Anti-Bot
  • Fixes a crash when the Anti-Bot database is held by another process in the system.

• SandBlast Agent Updater
  • Adds support for Static Analysis updates running in parallel to other updates using the Updater.
    Fixes an issue where the wrong service is restarted when updating two products together.
Management Requirements

E80.90 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 E80.90. Download SmartConsole from the E80.90 Endpoint Security client for Windows home page http://supportcontent.checkpoint.com/solutions?id=sk143452. If you have another version of SmartConsole installed on your computer, you must first uninstall it, and then install the SmartConsole for this release.

**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>All</td>
<td>All</td>
</tr>
<tr>
<td>10 (version 1803)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td>Update 1</td>
<td>All</td>
</tr>
<tr>
<td>10 (version 1709)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td>SP1 Microsoft update KB3033929</td>
<td>All</td>
</tr>
<tr>
<td>10 (version 1703)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td>Microsoft update KB3033929</td>
<td>All</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>All</td>
<td>All</td>
</tr>
<tr>
<td>7</td>
<td>Enterprise Professional</td>
<td>32/64-bit</td>
<td>All</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.

### 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 E80.90 Endpoint Security client is available from versions:
E80.64 and higher.

Upgrade from EP6.0 to E80.90.

For earlier versions, contact Check Point Support
https://www.checkpoint.com/support-services/contact-support/.

Supported Upgrades for Endpoint Security Client for ATMs

Upgrade to E80.90 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 **E80.90** 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 E80.90 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 (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 Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>10 (version 1703)</td>
<td>Enterprise Professional</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 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 E80.90.
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**