Check Point
SOFTWARE TECHNOLOGIES LTD.

5 March 2018

ENDPOINT SECURITY CLIENTS E80.81

Release Notes

Check Point
SOFTWARE TECHNOLOGIES LTD
INFINITY

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.

Check Point E80.81

For more about this release, see the E80.81 Endpoint Security Client for Windows home page http://supportcontent.checkpoint.com/solutions?id=sk123051.

Latest Version of this Document

Download the latest version of this document http://downloads.checkpoint.com/dc/download.htm?ID=61509.

To learn more, visit the Check Point Support Center http://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 E80.81 Release Notes.

Revision History

Date	Description
6 Mar 2018	First release of this document

Contents

What's New

This release supports all Software Blades and features of previous releases.

New Features

- **Full Disk Encryption** - Support for NVMe-based Opal Self Encrypting Drives.
- **Anti-Exploit** - ROP exploit protection for the Firefox browser.

Enhancements

Anti-Bot

- Improved triggering of the forensics report when the URL contains specific characters.

Anti-Ransomware

- Optimization of the size of the backup database.
- Reduced the number of false positives by improving the handling of the exclusions policy.
- Invalid paths are removed from the exclusions policy.
- Honeypot files are deleted after the client is upgraded.

Anti-Exploit

- Improved interoperability with Capsule Docs.
- Improved compatibility with third-party Microsoft Office add-ins.

SandBlast Agent for Browsers - Web Extension

- Improved handling of policy settings that are updated through the Windows registry.

Management Requirements

E80.81 clients can be managed by these Endpoint Security Management Servers: 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 R77.30.03 Endpoint Security Management Server.

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

There is a new SmartConsole that supports E80.81 for each release of the Endpoint Security Management Server. Download the SmartConsole for your server release from the E80.81 Endpoint Security client for Windows home page http://supportcontent.checkpoint.com/solutions?id=sk123051. 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 E80.81 logs in SmartLog or SmartView Tracker for R77.30 servers, you must update the log schema. See sk106662 http://supportcontent.checkpoint.com/solutions?id=sk106662.

Client Requirements

This section shows supported operating systems and hardware requirements for Endpoint Security clients.

Supported Client Operating Systems

Microsoft Windows

Version	Editions	Arch.	SPs or Updates	Supported Blades
10 (version 1709) 10 (version 1703) 10 (version 1607) 10 LTSB (version 1607)	Enterprise Pro	32/64-bit		All
8.1	Enterprise Pro	32/64-bit	Update 1	All
7	Enterprise Professional	32/64-bit	SP1 Microsoft update KB3033929	All

Microsoft Windows Server

Version	Editions	Arch.	SPs or Updates	Supported Blades
2016 (*)	All	64-bit		Compliance, Anti-Malware, Firewall, SandBlast Agent Blades, Capsule Docs (Standalone Client)
2012	All	64-bit		Compliance, Anti-Malware, Firewall, SandBlast Agent Blades, Capsule Docs (Standalone Client)
2012 R2	All	64-bit		Compliance, Anti-Malware, Firewall, SandBlast Agent Blades, Capsule Docs (Standalone Client)
2008 R2	All	32/64-bit	Microsoft update KB3033929	Compliance, Anti-Malware, Firewall, SandBlast Agent Blades, Capsule Docs (Standalone Client)

(*) To support Endpoint Compliance rules you must install a server Hotfix. See sk122136 http://supportcontent.checkpoint.com/solutions?id=sk122136.

VMware ESXi

Version	Supported Blades
5.1, 5.5, 6.0	All except: Full Disk Encryption and Media Encryption & Port Protection

Note - If you install a client package with blades that are not supported on the server, the installation succeeds but only the supported blades 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 the Full Disk Encryption blade 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.

See sk93345 http://supportcontent.checkpoint.com/solutions?id=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 2016 32/64 bit
- Microsoft Office 2013 32/64-bit
- Microsoft Office 2010 32/64-bit
- Microsoft Office 2007 32-bit
- Microsoft Office 2003 32-bit (English version)
- Adobe Reader DC
- Adobe Reader 8 - 11
- Adobe Acrobat Pro 8 and 9

Supported Upgrade Paths

Supported Upgrades for Endpoint Security Client

Upgrade to E80.81 Endpoint Security client is available from versions:
E80.80, E80.72, E80.71, E80.70, E80.65, E80.64.

For earlier versions, contact Check Point Support.

Supported Upgrades to Windows 10

For existing Endpoint Security deployments, you must upgrade the clients to E80.81 and then upgrade the operating system to Windows 10 (version 1709)

Upgrades to Windows 10 (version1709) with an earlier version of the Endpoint Security client are blocked by Microsoft.

The E80.81 client supports upgrades to Windows 10 (version 1709) from these earlier versions of Windows:

Version	Editions	Arch.	SPs or Updates	Supported Blades
10 (version 1703) 10 (version 1607)	Enterprise Pro	32/64-bit		All
8.1	Enterprise Pro	32/64-bit	Update 1	All
7	Enterprise Professional	32/64-bit	SP1	All

Important for Windows 10 in-place OS upgrades to Windows 10 (version 1709):

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 necessary.

Legacy Client Supported Upgrades

- **Legacy Media Encryption client:**
  See sk99116 http://supportcontent.checkpoint.com/solutions?id=sk99116 for supported legacy Media Encryption upgrades.
- **Legacy Full Disk Encryption client:**
  The supported upgrade path for the legacy Full Disk Encryption client is from 7.5.1 to E80.81.

Client Deployment

Download the E80.81 client from the E80.81 Endpoint Security Client for Windows home page http://supportcontent.checkpoint.com/solutions?id=sk123051.

See *Deploying Endpoint Security Clients* in the *R77.30.03 Endpoint Security Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=53788.