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.

Latest Documentation
The latest version of this document is at: (http://supportcontent.checkpoint.com/documentation_download?ID=36189)
To learn more, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the E80.60 home page (http://supportcontent.checkpoint.com/solutions?id=sk102651).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 April 2015</td>
<td>• Updated VMWare support in Endpoint Security Management Server Supported Operating Systems (on page 8)</td>
</tr>
<tr>
<td></td>
<td>• Updated Service Pack requirements and supported blades for Windows Servers in Supported Client Operating Systems (on page 10).</td>
</tr>
<tr>
<td></td>
<td>• Updated Supported Self Encrypting Drives in Full Disk Encryption Requirements (on page 12)</td>
</tr>
<tr>
<td>13 January 2015</td>
<td>In Supported Client Operating Systems (on page 10):</td>
</tr>
<tr>
<td></td>
<td>• Corrected supported Mac OS X versions</td>
</tr>
<tr>
<td></td>
<td>• Updated Capsule Docs note</td>
</tr>
<tr>
<td>4 December 2014</td>
<td>Added Remote Access VPN (on page 7) to the What's New section</td>
</tr>
<tr>
<td>29 October 2014</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

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 E80.60 Release Notes).
Introduction

Check Point Endpoint Security E80.60 introduces new Software Blades and features.

Important!

- The E80.60 Endpoint Security Management Server can be activated only on a management-only computer or appliance. Stand Alone (Security Gateway + Management) deployment is not supported.
- The E80.60 Endpoint Security Server is based on the R77 Management Server. It has all the supported capabilities of a standard Check Point R77 Management Server.
- The E80.60 Endpoint Security Server can manage E80.40 and higher Endpoint Security clients.

What's New

Capsule Docs

The Capsule Docs Software Blade, managed by an on-premises Security Management Server, lets organizations protect and share documents safely within the organization and with business partners, and manage the organizational Capsule Docs policy, monitoring, and deployment through SmartEndpoint.

The Capsule Docs Software Blade comes integrated with the Endpoint Security on Microsoft Windows computers. There is also a non-managed Capsule Docs plugin for supported applications, and the Capsule Docs Viewer. The Viewer does not require administrative privileges or the installation of Microsoft Office or Adobe Acrobat Reader, and gives read-only access to protected documents. The Capsule Docs plugin, which is mainly for the external users, and the Capsule Docs Software Blade give full editing capabilities and these benefits:

Control the parties that can access the data

- Restrict access to individuals, groups or entire organizations.
- Use granular Classification model to assign different permissions for internal and external users.
- Control data distribution (Forward, Copy/Paste, Print).
- Choose contacts from your Outlook address book with whom you usually communicate.
- Prevent unintentional data loss with the help of UserCheck.

Protect data stored on untrusted servers and shared via untrusted channels

- Each protected document remains protected even on untrusted servers.
- Prevent forwarding to unauthorized parties.
- Secure all created documents automatically.

See full audit trail for data access

- All actions on protected documents are logged and are available through SmartView Tracker and SmartLog.
- Follow paper trail for a single document.
- Audit distribution patterns for documents in an organization.
- Monitor access by external parties.
Access protected documents easily from your platform of choice
- Seamless integration with Microsoft Office and Adobe Acrobat on Windows platforms.
- Lightweight Windows Viewer that does not require administrative privileges or Microsoft Office or Adobe Acrobat clients installed.
- Access protected documents from proprietary Apps on Android, and iOS mobile devices.

Full Integration with Organizational Active Directory
- Users that are defined in the Active Directory are automatically provisioned to use Capsule Docs.
- User’s Active Directory account authentication is sufficient to access relevant protected documents.
- Customize Capsule Docs policy for different Users, Organizational Units and Groups.

Check Point Capsule Docs encrypts documents to protect them from unauthorized access. It protects users from unintentional data leaks. It is not possible to prevent all intentional violations made by malicious authorized users and this is not the goal of Check Point Capsule Docs.

URL Filtering
The Check Point Endpoint URL Filtering Software Blade lets an organization control access to web sites by category, user or group. This way it improves network security and enhances user productivity.

User Check technology empowers and educates Endpoint users on web usage policy in real time.

The Endpoint URL Filtering Software Blade has these benefits:
- Lets you utilize a database of over 200 million websites, updated in real-time.
- Lets you choose from 64 predefined content categories or create custom categories and URL families.
- Works inside and outside of the organization - policy is enforced on the client.
- Does unified management - lets the administrator configure one Rule Base in SmartDashboard for an Endpoint and a Gateway policy.
- Does unified log reporting through SmartLog.
- Uses Identity Awareness - lets the administrator grant, limit, or block user access, group access, or access from specific machines to individual web sites or categories of web sites.
- Fully integrates the organization's Active Directory.
- Utilizes SSL Inspection.

Media Encryption & Port Protection
This release adds NTFS file system support for encrypted storage devices. NTFS file system lets you encrypt files over 4GB.

Notes -
- Check Point Media Encryption Offline Utility lets you access NTFS encrypted storage devices on non-managed MS Windows computers in admin mode.
- Apple Mac computers do not by default support the NTFS file system. To make an encrypted storage device accessible on a Mac computer, format it as a FAT32.
- To create encrypted NTFS storage on a Windows 7 computer, you must first install SP1 on it.

Anti-Bot
The Anti-Bot Software Blade:
- Uses the ThreatCloud repository to receive updates and queries it for classification of unidentified IP, URL, and DNS resources.
• Prevents damage by blocking bot communication to C&C sites and makes sure that no sensitive information is stolen or sent out of the organization.

The Endpoint Anti-Bot blade uses these procedures to identify bot infected computers:
• Identify the C&C addresses used by criminals to control bots. These web sites are constantly changing and new sites are added on an hourly basis. Bots can attempt to connect to thousands of potentially dangerous sites. It is a challenge to know which sites are legitimate and which are not.

Check Point uses the ThreatCloud repository to find bots based on these procedures.

The ThreatCloud repository contains more than 250 million addresses that were analyzed for bot discovery and more than 2,000 different botnet communication patterns. The ThreatSpect engine uses this information to classify bots and viruses.

The Endpoint Anti-Bot blade gets reputation updates from the ThreatCloud repository. It can query the cloud for new, unclassified URL/DNS resources that it finds.

### Forensics

The Check Point Endpoint Forensics Software Blade monitors files and the registry for suspicious processes and network activity. When the Anti-Malware or the Anti-Bot Client Software Blade, or the Check Point Gateway Software Blade detects an attack, the Check Point Endpoint Forensics Software Blade analyzes the attack, and uploads the complete attack report to the Endpoint Security Management Server.

**Note** - The Check Point Endpoint Forensics Software Blade is not supported on Microsoft Windows XP operating system.

### Full Disk Encryption Features

This release adds support for these features:
• Use of TPM to measure integrity of Pre-boot components.
• Password synchronization between the OS and Pre-boot after Remote Help.
• Fast Initial Encryption Installation Parameter Option - MSI Installer parameter to enable the new Fast Initial Encryption mode, for encryption of only Used Space (not Free Space) on the disk. See sk102026 (http://supportcontent.checkpoint.com/solutions?id=sk102026 ) for details.
• Tokens for Pre-boot authentication.
• Temporary Pre-boot Bypass from a script.
• Full Disk Encryption Drive Slaving Utility.

### Remote Access VPN


### Other Features

• Improved client deployment GUI.
• Easier Policy Server Configuration.
• Configure the length of the Remote Help response.
Management Requirements

This section shows supported operating systems and hardware requirements for Management servers and consoles.

Endpoint Security Management Server Supported Operating Systems

- Gaia: All releases
- All editions of Microsoft Windows Server 2003 and 2008 (including R2 for 2003 and 2008 - for Capsule Docs Management Software Blade support)
- VMware: ESXi 5.1 and 5.5

Endpoint Security Management Server Hardware Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel Pentium Processor E2140 or 2GHz equivalent processor</td>
</tr>
<tr>
<td>Memory</td>
<td>2GB</td>
</tr>
<tr>
<td>Disk Space (for installation)</td>
<td>10GB</td>
</tr>
</tbody>
</table>

Resource consumption is based on the size of your environment. For larger environments, more disk space, memory, and CPU are required.

Supported Security Management Servers

E80.60 Endpoint Security is installed with the R77 Network Security Management Server. This is the only supported Network Security Management Server for E80.60.

The E80.60 Endpoint Security Management Server can be activated only on a management-only computer or appliance. Stand Alone (Security Gateway + Management) deployment is not supported.

URL Filtering

To use the Endpoint Security URL Filtering Software Blade, you must have a Network Security Management Server and Endpoint Security Management Server in one of these deployments:

- **One-computer deployment** - Network Security Management Server and Endpoint Security Management Server are installed on the same computer
- **Distributed deployment** - Network Security Management Server and Endpoint Security Management Server are installed on different computers and communicate with each other through Secure Internal Communication (SIC)
  
  **Note** - Distributed deployment works only when both servers run on Gaia OS. If at least one of the servers runs on Windows OS, this configuration will not work.

The Endpoint Security URL Filtering Software Blade is installed on an E80.60 Endpoint Security Management Server on R77. It works with the Network Security Management Server, which can be R75.40 or higher. See the *E80.60 Endpoint Security Administration Guide* for configuration instructions.
Supported SmartConsole Platforms

The E80.60 SmartConsole is supported on these platforms:

- Microsoft Windows Server 2008 32 bit
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2003 32-bit, SP1 and SP2
- Microsoft Windows Server 2003 R2 32/64-bit, SP1 and SP2
- Microsoft Windows 8 32/64-bit
- Microsoft Windows 7 Enterprise, Professional, Ultimate editions 32/64-bit
- Microsoft Windows 7 Enterprise, Professional, Ultimate editions 32/64-bit SP1
- Microsoft Windows Vista 32-bit, SP1
- Microsoft Windows XP Professional 32-bit, SP3

Endpoint Policy Management Requirements

These are the minimum requirements to install Endpoint Policy Management on a Security Management Server:

<table>
<thead>
<tr>
<th>Component</th>
<th>Windows</th>
<th>Gaia and SecurePlatform</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel Pentium E2140 2.0 GHz</td>
<td>Intel Pentium E2140 2.0 GHz</td>
</tr>
<tr>
<td>Memory</td>
<td>2048MB</td>
<td>2048MB</td>
</tr>
<tr>
<td>Disk Space</td>
<td>10GB</td>
<td>10GB (current partition)</td>
</tr>
</tbody>
</table>

Note - The network Security Management Server can also be an Endpoint Policy Management server. All deployments support this, other than:
- Standalone
- Multi-Domain Server

This Endpoint Policy Management version supports R77 SmartEvent
- Endpoint Policy Management is not supported on RedHat Enterprise Linux releases

Additional Requirements for Windows

Important - Disable SNMP services before you install the Endpoint Policy Management server.

Make sure that these ports are available on the server:
- 80 Apache HTTP
- 443 Apache SSL
- 8005 Tomcat server
- 8009 Tomcat AJP
- 8080 Tomcat HTTP
- 1080 CPTNL client proxy (relevant for Policy server only)
- 18193 CPTNL server proxy (relevant for EPS server only)
- 81 CPTNL server (relevant for EPS server only)
- 61616 AMQ TCP access
SmartEndpoint Requirements

The minimum hardware requirements to run the SmartConsole, including SmartEndpoint are:

<table>
<thead>
<tr>
<th>Component</th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel Pentium Processor E2140 or 2 GHz equivalent processor</td>
</tr>
<tr>
<td>Memory</td>
<td>2GB</td>
</tr>
<tr>
<td>Available Disk Space</td>
<td>2GB</td>
</tr>
<tr>
<td>Video Adapter</td>
<td>Minimum resolution: 1024 x 768</td>
</tr>
</tbody>
</table>

Supported Languages

The SmartEndpoint Console is available only in English. It supports operating systems in other languages. The supported localized systems are:

- French
- German
- Spanish
- Italian

The Endpoint Security Management Server is supported only in English.

Client Requirements

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

Supported Client Versions

E80.60 Endpoint Security Servers can manage E80.40 and higher Endpoint Security clients.

Supported Client Operating Systems

This release supports the Endpoint Security client on:

Microsoft Windows

- Microsoft Windows 8.1, with or without Update 1
- Microsoft Windows 8
- Microsoft Windows 7 Enterprise, Professional, Ultimate editions 32/64-bit, with or without SP1
- Microsoft Windows XP Professional 32-bit, SP3

Microsoft Windows Server

- Microsoft Windows Server 2003 32 bit, SP2
  Supported Software Blades: Compliance, Anti-Malware
- Microsoft Windows Server 2003 R2, SP2
  Supported Software Blades: Compliance, Anti-Malware
- Microsoft Windows Server 2008 32/64-bit, SP1 or SP2
  Supported Software Blades: Compliance, Anti-Malware, Firewall
- Microsoft Windows Server 2008 R2
  Supported Software Blades: Compliance, Anti-Malware, Firewall
- Microsoft Windows Server 2012
  Supported Software Blades: Compliance, Anti-Malware, Firewall
- Microsoft Windows Server 2012 R2
  Supported Software Blades: Compliance, Anti-Malware, Firewall

**Mac OS X**

- Mac OS X 10.8, 10.9, and 10.10

**Notes**

If you install a client package that includes blades that are not supported on the server, the installation succeeds but only the applicable blades are installed.

- URL Filtering, Anti-Bot, and Forensics Software Blades are supported on Windows only.
- Anti-Bot, and Check Point Forensic Software Blades are not supported on Windows XP.
- On Windows there is support for both Capsule Docs Plugin and Capsule Docs Viewer. An alpha version of Capsule Docs Viewer is available for Mac OS X, including the ability to unprotect protected documents, based on user permissions.

**Important** - Application Control is not supported on Windows Server.

**To disable Application Control on servers:**

a) Assign the server group or members to a new application control policy.

b) Disable application control in the policy.

c) Install the policy.

**Supported Mobile Operating Systems**

These mobile OS versions support Capsule Docs:

- iOS 5 and higher
- Android 4 and higher

**Supported Languages for Endpoint Security Clients**

The Endpoint Security client is available in these languages:

- English
- French
- German
- Japanese
- Russian
- Czech

**Client Hardware Requirements**

The minimum hardware requirements for client computers that run the Total Endpoint Security Package are:

- 1 GB RAM
- 1 GB free disk space
Full Disk Encryption Requirements

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 8.1 32/64-bit
- Windows 8 32/64-bit
- Windows 8 logo certified hardware with UEFI version 2.3.1
- Windows 7 64-bit

Unlock on LAN Requirements
- MacOS - On Mac, you can use Unlock on LAN on computers that are shipped with OSX 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 logo certified computers that have a built in Ethernet port. The computer must be running Windows 8 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.

See sk93709 to troubleshoot UEFI network connectivity (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 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).

Supported Self Encrypting Drives (SED)
You can use Self Encrypting Drives with Full Disk Encryption. The requirements are:

- Windows 8 UEFI, Windows 8.1 UEFI, or Windows 7 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

These hard disk drives have been explicitly tested and verified with Full Disk Encryption E80.60:

<table>
<thead>
<tr>
<th>Hard Disk Drive Name</th>
<th>Model</th>
<th>Firmware</th>
<th>Opal Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seagate 250 GB Momentus Thin</td>
<td>ST250LT014-9YK14C</td>
<td>0004LVM7</td>
<td>1</td>
</tr>
<tr>
<td>Hitachi Travelstar ZK7320</td>
<td>HITACHI HTS723225A7A365 OPAL</td>
<td>ECB6B80P</td>
<td>1</td>
</tr>
<tr>
<td>Crucial M500 120 GB</td>
<td>Crucial_CT120M500SSD1</td>
<td>MU02</td>
<td>2</td>
</tr>
<tr>
<td>Seagate 500 GB Momentus Thin</td>
<td>ST500LT025-1A5142</td>
<td>0001SDM7</td>
<td>2</td>
</tr>
<tr>
<td>Seagate 500 GB Momentus Thin (FIPS 140-2)</td>
<td>ST500LT015-9WU142</td>
<td>0001SDM7</td>
<td>2</td>
</tr>
<tr>
<td>SanDisk X300s 256 GB</td>
<td>SanDisk_SD7UB3Q256G</td>
<td>X2150300</td>
<td>2</td>
</tr>
</tbody>
</table>
You can use 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 Single Sign-On (SSO) When Resuming from a Hibernated State**

To use SSO from a hibernated state in Windows, the requirements are:

- Windows Vista or higher (Windows XP is not supported with this feature)
- Windows GPO Interactive logon: Do not require CTRL+ALT+DEL must not be disabled.

**Support for TPM**

The TPM is used to enhance security by measuring integrity of Pre-boot components. To use TPM the feature must be enabled in the Full Disk Encryption policy. In addition, these system requirements apply:

- TPM hardware adhering to specification 1.2.
- Windows 7 32/64-bit or higher. (Windows XP is not supported with this feature).

**Media Encryption & Port Protection Support**

**Storage Devices:**

- Standard USB 2.0 and 3.0 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 2013 32/64-bit
- Microsoft Office 2010 32/64-bit
- Microsoft Office 2007 32-bit
- Microsoft Office 2003 32-bit (English version)
- Adobe Reader 8 - 11
- Adobe Acrobat Pro 8 and 9

**Supported Upgrade Paths**

**Supported Upgrades for Endpoint Security Client**

Upgrade to E80.60 Endpoint Security client is available for these versions:

- E80.20 and higher

**Note** - The WebCheck Software Blade is not supported. If you have it installed from a previous version, you must remove it before you upgrade to E80.60.
Supported Upgrades for Endpoint Security Management

Endpoint Security Management Server upgrade to E80.60 is available for these versions:

- R76
- R77
- E80.60 previous builds

Only Advanced Upgrades are supported.

Legacy Full Disk Encryption Support

You can upgrade to Full Disk Encryption in E80.60 from:

- FDE EW 6.3.1
- R73 and higher

Legacy Media Encryption Support

See sk99116 (http://supportcontent.checkpoint.com/solutions?id=sk99116 ) for supported legacy Media Encryption upgrades.

Installation and Configuration

Before you install this release, make sure you have all requirements.

Installing Endpoint Security Management Server

In all non-standalone deployments, the Network Security Management Server can also be an Endpoint Security Management Server. You can enable the Endpoint Security Management Server after the Network Security Management Server installation completes. Endpoint Security E80.60 is installed with the R77.

For installation and upgrade instructions, use the procedures in the R77 Installation and Upgrade Guides.

For upgrades to E80.60, only Advanced Upgrade procedures are supported.

Important: Upgrades FROM E80.60 TO R77.x are not supported.

For automatic provisioning of users for Capsule Docs, users and computers must be scanned by the Endpoint Security Active Directory Scanner. For the Active Directory Scanner to work, you must assign Read permissions to the Active Directory path and to the folder with deleted objects, and configure the Active Directory Scanner on the Endpoint Security Management Server.

For Capsule Docs to work, the Endpoint Security Management Server must be in the organization's domain or configured to resolve Active Directory DNS names.

Sharing Protected Documents Externally

To make sure that the users inside the organization can share Capsule Docs protected documents with users outside of the organization and mobile users, make sure to configure:

- An SMTP server with the Endpoint Security Management Server, to send email outside of the organization without the use of SSL
- A reverse proxy server that shares dedicated internal URLs with the external networks
Note - To make the configuration of the reverse proxy server more secure, make sure the server holds a valid certificate issued by an authorized Certificate Authority, and the number of connections per IP address and the total number of concurrent connections is limited.

For more information on reverse proxy configuration, see the *E80.60 Endpoint Security Administration Guide*.

### Installing Endpoint Security Clients

For instructions on installation of Endpoint Security clients, see the *E80.60 Endpoint Security Management Server Administration Guide* ([http://supportcontent.checkpoint.com/solutions?id=sk102651](http://supportcontent.checkpoint.com/solutions?id=sk102651)).

### Installing E80.60 SmartConsole

To install E80.60 SmartConsole:


Note - If you have another version of SmartConsole installed on your computer, you must first uninstall it, then install the E80.60 SmartConsole.

### Build Numbers

These build numbers are included in the release:

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Components</td>
<td>8.6.532</td>
</tr>
<tr>
<td>Anti-Bot</td>
<td>8.60.1.350</td>
</tr>
<tr>
<td>Anti-Malware</td>
<td>8.3.4.7</td>
</tr>
<tr>
<td>Compliance</td>
<td>8.60.1.303</td>
</tr>
<tr>
<td>Forensics</td>
<td>8.60.1.329</td>
</tr>
<tr>
<td>Media Encryption &amp; Port Protection</td>
<td>8.60.0.311</td>
</tr>
<tr>
<td>Firewall &amp; Application Control</td>
<td>8.60.307</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>86.0.103.26</td>
</tr>
<tr>
<td>Remote Access VPN</td>
<td>986000275</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>80.6.0.64</td>
</tr>
</tbody>
</table>

### Known Limitations

Known Limitations for this release are in sk102652 ([http://supportcontent.checkpoint.com/solutions?id=sk102652](http://supportcontent.checkpoint.com/solutions?id=sk102652)).