E80.61 and R77.20.01

Release Notes

Classification: [Protected]
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.

For more about this release, see the E80.61 home page

Latest Version of this Document
Download the latest version of this document

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 E80.61 and
R77.20.01 Release Notes).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>09 Aug 2015</td>
<td>Updated Supported Client Versions (on page 11)</td>
</tr>
<tr>
<td>27 May 2015</td>
<td>Changes to the Windows versions data</td>
</tr>
<tr>
<td>13 May 2015</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Introduction

Check Point Endpoint Security E80.61 client introduces new Software Blades and features on R77.20.01 Management.

What's New

This release supports all new Software Blades and features of E80.60. It also includes these changes: User and Device Management, Mobile Access and Capsule Workspace, Full Disk Encryption, and Remote Access VPN.

User and Device Management

UDM (User and Device Management) is a web based application that manages a range of user and device related tasks in an organization. A typical user accesses organizational resources from multiple devices: computers, laptops, smartphones, and tablets. UDM provides a unified environment for managing various user and device related tasks, such as provisioning, transparency of access via SmartLog logs, viewing user and device details, certificate management, AD user management, and FDE password recovery (for Endpoint Security clients).

With UDM, security administrators can delegate user and device management tasks to Help Desk administrators. This delegation of responsibilities lets the network security team handle security policy issues and the Help Desk team manage some user access tasks.

UDM includes:

- **Remote Access certificate management**
  - Manage, create, and revoke user certificates for remote access.
  - Use email templates to send information to users on how to connect remotely from their devices.

- **Integration with Active Directory**
  - See all users in the organization and the devices they are using to connect to organizational resources.
  - Change the status of Active Directory users when necessary (expired, disabled, or locked).
  - Manage Active Directory user groups.

- **Integration with SmartLog**
  - See user login and activity logs.
  - Search and filter logs for a specified user.
  - See if a device is connected or disconnected.

- **Integration with Endpoint Security Server**
  - See activity of users and devices.
  - Use Full Disk Encryption password recovery.
  - Active Directory integration.
• Integration with Capsule Cloud
  • See logs of Capsule Cloud users.
  • Send new registration codes to users.

Mobile Access and Capsule Workspace

• Push Notification Configuration
  Configure how push notifications will look in Capsule Workspace and what data is shown in the notifications.

• Link Translation Domain Configurations
  Configure which domains are translated by the Mobile Access gateway. For example, define internal domains and external domains.

• Reverse Proxy for Capsule Docs
  Reverse Proxy for Capsule Docs is now integrated into the release with no need to install a Reverse Proxy Hotfix.

• Kerberos Constrained Delegation support for Mobile Access and Capsule Workspace
  A Single Sign-on method that uses Kerberos authentication for users to access internal resources without the need to enter a password.

See the *Endpoint Security Administration Guide* for details about Reverse Proxy.

See the *R77.30 Mobile Access Administration Guide* for details about other new features.

Full Disk Encryption

• TPM support for version 1.2 and 2.0
• Support for Active Directory groups in Pre-boot

Remote Access VPN

For new features in the Remote Access VPN blade and standalone Remote Access Clients see the *E80.61 Remote Access Clients Release Notes.*
Management Requirements

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

Also see relevant requirements in the R77.20 Release Notes http://supportcontent.checkpoint.com/documentation_download?ID=31853.

Endpoint Security Management Server Supported Operating Systems

- Gaia: All releases
- All editions of Microsoft Windows Server 2003, 2008 and 2012, including all R2 editions
- 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

The R77.20.01 Endpoint Security Management Server supports E80.61 client. This is the only supported Endpoint Security Management Server for E80.61.

The R77.20.01 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 R70.20.01 server. It works with the Network Security Management Server, which can be R75.40 or higher. See the *URL Filtering* chapter of the *Endpoint Security Administration Guide* for installation and configuration instructions.

### Supported SmartConsole Platforms

The R77.20.01 SmartConsole is supported on these platforms:

**Microsoft Windows**

<table>
<thead>
<tr>
<th>Version</th>
<th>Editions</th>
<th>Arch.</th>
<th>SPs or Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Standard Enterprise Pro</td>
<td>32/64-bit</td>
<td>Update 1 (optional)</td>
</tr>
<tr>
<td>8</td>
<td>Standard Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Enterprise Professional Ultimate</td>
<td>32/64-bit</td>
<td>SP1 (optional)</td>
</tr>
<tr>
<td>Vista</td>
<td>Enterprise Ultimate</td>
<td>32-bit</td>
<td>SP1</td>
</tr>
<tr>
<td>XP</td>
<td>Professional</td>
<td>32-bit</td>
<td>SP3</td>
</tr>
</tbody>
</table>

**Microsoft Windows Server**

<table>
<thead>
<tr>
<th>Version</th>
<th>Editions</th>
<th>Arch.</th>
<th>SPs or Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>All</td>
<td>64-bit</td>
<td></td>
</tr>
<tr>
<td>2012 R2</td>
<td>All</td>
<td>64-bit</td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>All</td>
<td>32/64-bit</td>
<td>SP1 or SP2</td>
</tr>
<tr>
<td>2008 R2</td>
<td>All</td>
<td>32/64-bit</td>
<td></td>
</tr>
</tbody>
</table>

Also see SmartEndpoint Hardware and Software Requirements (on page 9).
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 R77.20 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 Hardware and Software 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>
</tbody>
</table>
Component | Windows  
--- | ---  
Available Disk Space | 2GB  
Video Adapter | Minimum resolution: 1024 x 768

**Supported Windows versions:**

SmartEndpoint supports all platforms listed in Supported SmartConsole Platforms (on page 8) with these exceptions:

- Microsoft Windows Server 2003 (all editions) is NOT supported.
- Microsoft Windows Servers 2008 (all editions) requires .NET Framework 4.5 installed before you install SmartEndpoint. If .NET 4.5 is not installed, the reports in the **Reporting** tab do not work correctly.

**UDM Hardware and Software Requirements**

The minimum recommended hardware requirements for the UDM machine:

<table>
<thead>
<tr>
<th>Component</th>
<th>Windows</th>
<th>Linux</th>
<th>Gaia &amp; SecurePlatform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel Pentium Processor E2140 or 2 GHz equivalent processor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Free Disk Space</td>
<td>10GB</td>
<td>10GB</td>
<td>20GB (installation includes OS)</td>
</tr>
<tr>
<td>Memory</td>
<td>2GB</td>
<td>2GB</td>
<td>2GB</td>
</tr>
<tr>
<td>Network Adapter</td>
<td>One or more</td>
<td>One or more</td>
<td>One or more</td>
</tr>
</tbody>
</table>

**Supported Windows versions**

- Windows Server 2008 (32-bit and 64-bit) SP1, SP2
- Windows Server 2003 (32-bit) SP1, SP2

**Supported Browsers:**

- Internet Explorer 8 and higher
- Chrome
- Firefox
- Safari
- Opera

**Supported Languages for Management**

The SmartEndpoint Console is available only in English. It supports operating systems in Japanese.

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

R77.20.01 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

<table>
<thead>
<tr>
<th>Version</th>
<th>Editions</th>
<th>Arch.</th>
<th>SPs or Updates</th>
<th>Supported Blades</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Standard Enterprise Pro</td>
<td>32/64-bit</td>
<td>Update 1 (optional)</td>
<td>All</td>
</tr>
<tr>
<td>8</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>7</td>
<td>Enterprise Ultimate</td>
<td>32/64-bit</td>
<td>SP1 (optional)</td>
<td>All</td>
</tr>
<tr>
<td>XP</td>
<td>Professional</td>
<td>32-bit</td>
<td>SP3</td>
<td>All except: Anti-Bot, and Forensics</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 Blades</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>All</td>
<td>64-bit</td>
<td></td>
<td>Compliance, Anti-Malware, Firewall</td>
</tr>
<tr>
<td>2012 R2</td>
<td>All</td>
<td>64-bit</td>
<td></td>
<td>Compliance, Anti-Malware, Firewall</td>
</tr>
<tr>
<td>2008</td>
<td>All</td>
<td>32/64-bit</td>
<td>SP1 or SP2</td>
<td>Compliance, Anti-Malware, Firewall</td>
</tr>
<tr>
<td>2008 R2</td>
<td>All</td>
<td>32/64-bit</td>
<td></td>
<td>Compliance, Anti-Malware, Firewall</td>
</tr>
<tr>
<td>2003</td>
<td>All</td>
<td>32-bit</td>
<td>SP2</td>
<td>Compliance, Anti-Malware</td>
</tr>
<tr>
<td>2003 R2</td>
<td>All</td>
<td>32-bit</td>
<td>SP2</td>
<td>Compliance, Anti-Malware</td>
</tr>
</tbody>
</table>
Mac OS X

<table>
<thead>
<tr>
<th>Version</th>
<th>Supported Blades</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10</td>
<td>All except: URL Filtering, Anti-Bot, Anti-Malware, and Forensics, Limited version of Capsule Docs Viewer</td>
</tr>
<tr>
<td>10.9</td>
<td>All except: URL Filtering, Anti-Bot, Anti-Malware, and Forensics, Limited version of Capsule Docs Viewer</td>
</tr>
<tr>
<td>10.8</td>
<td>All except: URL Filtering, Anti-Bot, Anti-Malware, and Forensics, Limited version of Capsule Docs Viewer</td>
</tr>
</tbody>
</table>

**Note** - 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.

**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
- Czech
- French
- German
- Italian
- Japanese
- Russian
- Spanish
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.


**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 E80.61:

<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 or 2.0.
- 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:

- Microsoft Office 2013 32/64-bit
- Microsoft Office 2010 32/64-bit
Supported Upgrade Paths

Supported Upgrades for Endpoint Security Client

Upgrade to E80.61 Endpoint Security client is available for these versions:

- E80.20 and higher
- Capsule Docs upgrades are supported from E80.60.

**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 this version.

Supported Upgrades for Endpoint Security Management

Endpoint Security Management Server upgrade to R77.20.01 is available for these versions:

- R76
- R77
- R77.10
- R77.20
- R77.20.01 previous builds

Hotfixes are only supported on top of R77.20.01 if the hotfix explicitly supports upgrade from R77.20.01.

Legacy Full Disk Encryption Support

You can upgrade to Full Disk Encryption in E80.61 from:

- FDE EW 6.3.1
- R73 and higher

Legacy Media Encryption Support

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 E80.61 clients work with the R77.20.01 server.

Installing with the R77.20.01 Hotfix

For installation and upgrade instructions, use the procedures in the R77 Installation and Upgrade Guides to install or upgrade to R77.20. Then install the R77.20.01 hotfix from sk105123 [http://supportcontent.checkpoint.com/solutions?id=sk105123]. You can also install the R77.20.01 hotfix on an existing R77.20 installation.

Notes for Capsule Docs

- 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.

Notes for URL Filtering


Installing the R77.20.01 Hotfix

To install R77.20.01 on a Windows Security Management Server:

2. Download the R77.20.01 installation file: R77.20.01_Windows.tgz and save it on the Security Management Server.
3. Extract the file.
4. Run: Setup.exe
5. Reboot.

To install R77.20.01 on a Gaia Security Management Server:

2. Create a temporary directory.
3. Download the R77.20.01 installation file: R77.20.01_Linux.tgz
4. Save the file to the temporary directory.
5. In the temporary directory, run: `tar -zxvf R77.20.01_Linux.tgz`
6. Run the installation: `./UnixInstallScript`
7. Reboot.

### Installing Endpoint Security Clients

For instructions on installation of Endpoint Security clients, see the *Endpoint Security Administration Guide*.

### Installing the SmartConsole

To install the R77.20.01 SmartConsole:

Download the SmartConsole from the home page and run it.

**Note** - If you have another version of SmartConsole installed on your computer, you must first uninstall it, then install the R77.20.01 SmartConsole.

### 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 *Endpoint Security Administration Guide*. 
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>8.7.025</td>
</tr>
<tr>
<td>Anti-Bot</td>
<td>8.60.1.835</td>
</tr>
<tr>
<td>Anti-Malware</td>
<td>8.3.4.7</td>
</tr>
<tr>
<td>Compliance</td>
<td>8.60.1.803</td>
</tr>
<tr>
<td>Capsule Docs</td>
<td>91.1.468</td>
</tr>
<tr>
<td>Forensics</td>
<td>8.60.1.586</td>
</tr>
<tr>
<td>Media Encryption &amp; Port Protection</td>
<td>8.60.0.808</td>
</tr>
<tr>
<td>Firewall &amp; Application Control</td>
<td>8.60.814</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>86.0.108.26</td>
</tr>
<tr>
<td>Remote Access VPN</td>
<td>986000319</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>86.0.1.827</td>
</tr>
</tbody>
</table>

Known Limitations and Resolved Issues

For known limitations that apply to this release, see sk105124

For issues resolved in this release, see sk105125