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 E80.62
For more about this release, see the 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 E80.62 and R77.30.01  Release Notes.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 January 2016</td>
<td>Updated Full Disk Encryption Requirements (on page 14) to say: Windows 8 logo certified hardware with UEFI version 2.3.1 or higher.</td>
</tr>
<tr>
<td>17 December 2015</td>
<td>Clarified that E80.62 clients on all supported Windows versions, including Windows 10, can be managed by R77.20.01, R77.20, and R77.30 servers.</td>
</tr>
<tr>
<td>07 December 2015</td>
<td>First release of this document.</td>
</tr>
</tbody>
</table>
Introduction

Check Point Endpoint Security E80.62 clients introduce new features and functionality on top of R77.30.01 Management.

UDM introduces new features on R77.30.01 Management.

Check Point Endpoint Security R77.30.01 and E80.62 HFA 1 is also available. See sk110852 http://supportcontent.checkpoint.com/solutions?id=sk110852.

What's New

This release supports all Software Blades and features of previous releases. It includes new platform support, technologies, and features.

Windows 10 Support

This version supports clean install on Windows 10 and upgrades to Windows 10. See Supported Upgrades to Windows 10 (on page 19).

TLS 1.2 Support

The TLS 1.2 protocol is supported for:

- E80.62 Remote Access VPN clients.
- Capsule Docs Plugin
- Capsule Docs Viewer

UDM Suspicious Activity Monitoring

Mobile Access Suspicious Account Activity Monitoring in UDM includes these new features for Mobile Access clients:

- Increase the visibility of security incidents by involving end-users with potential security incidents related to their Mobile Access or Capsule Workspace account.
- SMS or Email notification to end-users upon security incidents on their account.
- An Alert landing page with information on the security incident, available from SMS or Email.
- These security incidents are monitored:
  - Too many consecutive failed logins to the account.
  - Too many consecutive failed attempts to unlock Capsule Workspace.
  - Account access from new/unknown devices.
  - Reuse of certificates across different devices.
• A Self Service Portal for end users:
  • Shows a history of account access activities.
  • Shows a history of account security incidents.
  • Lets end-users respond to security incidents, by informing the IT Security, Remote Wiping a device and changing the account password.
  • Lists Devices used to access the account.

Remote Access VPN

Full Disk Encryption
This release includes these encryption changes:
• Changed the padding algorithm for RSA encryption from PKCS#1 1.5 to OAEP padding.
• Changed the key encryption algorithm to NIST AES key wrapping, according to Special Publication 800-38F.
• TPM key encryption uses AES-256-CBC with PKCS#7 padding.

New Capsule Docs Capabilities

Data Classification
• Classify data without encryption.
• Allow integration with 3rd party vendors. For example, DLP solutions.
• Support document markings for Office.
• Full audit trail for data access through SmartLog:
  • Document Audit Trail
  • Distribution patterns in the organization

Bulk Protection Services
Capsule Docs Bulk Protection Services applies protection to documents based on location and properties. The protection is based on your configuration. See sk110852 http://supportcontent.checkpoint.com/solutions?id=sk110852.

There are two options to manage Bulk Protection Services:
• Content-Aware File Protection for CIFS and NFS-compatible Network Locations - Protection is applied through a network gateway with the DLP Software Blade to files that match specified data types.
• File Protection for Windows-based Servers and Workstations - Protection is applied locally and runs on the Windows computer. Continuous monitoring on specific targets is also available to protect new files as soon as they are created. See the Capsule Docs Bulk Protection Guide http://supportcontent.checkpoint.com/documentation_download?ID=43507.
Content-Aware Protection for Mail Attachments

This feature enables DLP Gateway administrators to set protect actions for email. It provides:

- Seamless experience - Automatic protection based on administrator configuration.
- Flexibility - The administrator can allow sending protected documents, and allow or block attachments.
- Content Awareness - Different protection settings for different types of data.
- Access Control - The authorized user list can include defined users and groups and/or e-mail sender/recipient.
- End User Education - UserCheck alerts the user to the organization security policy.


Capsule Docs Development Tools

Capsule Docs Development tools let you use your own applications for document protection.

- Apply Capsule Docs protection to files.
- Remove Capsule Docs protection from files.
- Inspect the file protection status.

There are different types of Capsule Docs Protection API:

- Capsule Docs Protection Services - WebServices API on the management server.
- Capsule Docs Protection Tool - command line utility.


Author Permissions for Groups

Authorized groups can be marked as author groups in the Capsule Docs menu. Users in that group are granted author permissions on the document.

Default Authors

The administrator can define the role of each authorized entity in the initial access list which is assigned to newly protected documents.

Client Communication through Proxy Servers with Authentication

The Check Point Capsule Docs Plugin and Capsule Docs Viewer support a proxy server to communicate with the Endpoint Security Management Server. This is done with NTLM/Negotiate authentication.
Management Requirements

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

Also see relevant requirements in the R77.30 Release Notes http://downloads.checkpoint.com/dc/download.htm?ID=40107.

Endpoint Security Management Server Supported Operating Systems

- Gaia: Smart-1 series and open platform
- All editions of Microsoft Windows Server 2008 and 2012, including all R2 editions
- VMware: ESXi 5.1 and 5.5

Endpoint Security Management Server Hardware Requirements

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

<table>
<thead>
<tr>
<th>Component</th>
<th>All Supported Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel Pentium E2140 2.0 GHz</td>
</tr>
<tr>
<td>Memory</td>
<td>2GB</td>
</tr>
<tr>
<td>Disk Space</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.

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 R77.30 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

### Supported Check Point Versions

To get new E80.62 features and capabilities, E80.62 clients must be managed by an R77.30.01 server.

E80.62 clients on all supported Windows versions, including Windows 10, can be managed by R77.20.01, R77.20, and R77.30 servers. New features are not supported with these servers.

- For R77.20 and R77.30 it is necessary to use a log schema update script to show logs from E80.62 clients (see sk106662 http://supportcontent.checkpoint.com/solutions?id=sk106662)
- For a list of the supported client version for each Management server, see sk107255 http://supportcontent.checkpoint.com/solutions?id=sk107255.

The R77.30.01 Endpoint Security Management Server can be activated only on a management-only computer or appliance. Standalone (Security Gateway + Management) deployment is not supported.

R77.30.01 is not supported with the R77.30 Jumbo Hotfix. All existing security fixes are integrated into R77.30.01.

### 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 R77.30.01 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.
UDM Hardware and Software Requirements

The minimum recommended hardware requirements for the UDM machine:

<table>
<thead>
<tr>
<th>Component</th>
<th>All Supported Operating Systems</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>Disk Space</td>
<td>10GB</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

Suspicious Account Activity Monitoring is supported on:
- Capsule Workspace
- Mobile Access Portal
- Windows 8.1 Check Point VPN Plug-in for PC

Capsule Docs Requirements

See the Capsule Docs Chapter of the Endpoint Security Administration Guide

Capsule Docs Integration with DLP Requirements

Content-aware file protection requires the DLP Software Blade enabled on an R77.30 gateway with these requirements:

<table>
<thead>
<tr>
<th>Open Server Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Cores</td>
<td>2</td>
</tr>
<tr>
<td>Memory</td>
<td>4GB</td>
</tr>
<tr>
<td>Disk Space (for installation)</td>
<td>250GB</td>
</tr>
<tr>
<td>Operating System</td>
<td>Gaia</td>
</tr>
</tbody>
</table>
Supported Check Point Appliances: 2000, 4000, 12000, 21000, and 61000 Appliances
Supported VMware: ESXi 4.0, 4.1, 5.1, and 5.5

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 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>10*</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 Professional</td>
<td>32/64-bit</td>
<td>SP1 (optional)</td>
<td>All</td>
</tr>
</tbody>
</table>

*Supported builds of Windows 10: 10240, 10586
For Windows 8, XP, or Vista contact Check Point Support.

**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, Capsule Docs</td>
</tr>
<tr>
<td>2012 R2</td>
<td>All</td>
<td>64-bit</td>
<td></td>
<td>Compliance, Anti-Malware, Firewall, Capsule Docs</td>
</tr>
<tr>
<td>2008</td>
<td>All</td>
<td>32/64-bit</td>
<td>SP1 or SP2</td>
<td>Compliance, Anti-Malware, Firewall, Capsule Docs</td>
</tr>
</tbody>
</table>
**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
- Polish

---

**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.

---

**Important**

- Application Control is not supported on all versions of Windows Server
- URL Filtering is not supported on all editions of Windows XP

Do not deploy these Software Blades on clients that run operating system that are not supported. You can also disable these Software Blades in the policy.

**To disable Software Blades on operating systems that are not supported:**

1. Configure the rules for these clients:
   - Windows Servers - Disable Application Control
   - Windows XP - Disable URL Filtering
2. Install the policy on all clients.

---

For supported Mac OS versions, see the [E80.62 Endpoint Security Client for Mac Release Notes](http://supportcontent.checkpoint.com/documentation_download?ID=47284).

---

<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>2008 R2</td>
<td>All</td>
<td>32/64-bit</td>
<td></td>
<td>Compliance, Anti-Malware, Firewall, Capsule Docs</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>
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 10 32/64-bit
- Windows 8.1 32/64-bit
- Windows 8 32/64-bit
- Windows 8 logo certified hardware with UEFI version 2.3.1 or higher
- 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 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.
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

Check Point has tested the SED support with the drives listed in the table below. Note that this is not an exhaustive list of supported drives. The list contains drives explicitly tested by Check Point and known to satisfy the above requirements for a Self Encrypting Drive.

<table>
<thead>
<tr>
<th>Hard Disk Drive Name</th>
<th>Opal Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seagate 250 GB Momentus Thin</td>
<td>1</td>
</tr>
<tr>
<td>Hitachi Travelstar ZK7320</td>
<td>1</td>
</tr>
<tr>
<td>Crucial M500 120 GB</td>
<td>2</td>
</tr>
<tr>
<td>Seagate 500 GB Momentus Thin</td>
<td>2</td>
</tr>
<tr>
<td>Seagate 500 GB Momentus Thin (FIPS 140-2)</td>
<td>2</td>
</tr>
<tr>
<td>SanDisk X300s 256 GB</td>
<td>2</td>
</tr>
<tr>
<td>Samsung 850 EVO 120GB</td>
<td>2</td>
</tr>
<tr>
<td>Intel SSD Pro 2500 180GB</td>
<td>2</td>
</tr>
<tr>
<td>Intel SSD 535 Series 360GB</td>
<td>2</td>
</tr>
<tr>
<td>SK hynix SC305 128GB</td>
<td>2</td>
</tr>
<tr>
<td>SK hynix SC300 256GB</td>
<td>2</td>
</tr>
<tr>
<td>SK hynix SC300 512GB</td>
<td>2</td>
</tr>
</tbody>
</table>


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 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 8 - 11
- Adobe Acrobat Pro 8 and 9
Supported SmartConsole Platforms

The R77.30.01 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>

**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>
<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 Windows versions:
SmartEndpoint supports all platforms listed in Supported SmartConsole Platforms (on page 17) with this additional requirement:

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.

Supported Upgrade Paths

Supported Upgrades for Endpoint Security Management
These Endpoint Security Management Server upgrades are supported:

• In-place Upgrade from R77.30 to R77.30.01 with the R77.30.01 Hotfix.
  If you use Full Disk Encryption with Pre-boot customization, see sk108957 http://supportcontent.checkpoint.com/solutions?id=sk108957.

• Advanced Upgrade from R77.20.01 to R77.30.01.

For other versions you must upgrade to R77.30 and then install the R77.30.01 Hotfix.

To upgrade to R77.30.01 from R77.20.01 with an Advanced Upgrade:
2. Extract the files to a temporary folder.
3. Run:
   • On Windows - migrate export <filename>.tgz
   • On Gaia - ./migrate export <filename>.tgz
4. Copy the TGZ file to a fresh R77.30.01 computer and use the local migrate tools ($FWDIR/bin/upgrade_tools) to run:
   • On Windows - migrate import <filename>.tgz
   • On Gaia - ./migrate import <filename>.tgz
5. Copy the MSI and Drivers folders from the original computer to the new computer.

You can only install a hotfix on R77.30.01 if the hotfix explicitly supports an upgrade from R77.30.01.

Supported Upgrades for Endpoint Security Client

Upgrade to E80.62 Endpoint Security client is available for versions E80.50 and higher.
For earlier versions, contact Check Point Support.
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 to Windows 10

- The E80.62 client supports:
  - Upgrades to Windows 10 from earlier versions of Windows.
  - Upgrades from earlier builds of Windows 10 to supported later builds of Windows 10. See Supported Client Operating Systems (on page 12).
- Upgrade to Windows 10 with an earlier version of the Endpoint Security client, is blocked by Microsoft.
- On Windows 10, install Microsoft KB3074683 before you install E80.62.
- For upgrades with Full Disk Encryption installed:
  - Make sure you have valid Windows 10 licenses.
  - See sk106433 http://supportcontent.checkpoint.com/solutions?id=sk106433
- After a Windows 10 upgrade with Media Encryption & Port Protection or Anti-Malware installed, an additional reboot is required to make Media Encryption & Port Protection and Anti-Malware fully operational. A reboot message is shown after the upgrade that says that the client has been repaired and a reboot is necessary.

Legacy Full Disk Encryption Support

You can upgrade to Full Disk Encryption in E80.62 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 an 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 E80.62 clients work with the R77.30.01 server.

For installation and upgrade instructions, use the procedures in the R77 Installation and Upgrade Guides to install or upgrade to R77.30. Then install the R77.30.01 Hotfix http://supportcontent.checkpoint.com/solutions?id=sk108375.

You can also install the R77.30.01 Hotfix on an existing R77.30 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 Hotfix

To install R77.30.01 on a Windows Security Management Server:

1. Back up your R77.30 Security Management Server.
2. Download the R77.30.01 installation file: R77.30.01.Windows.tgz and save it on the Security Management Server.
3. Extract the file.
4. Open the CLI as an administrator.
5. Run: Setup.exe
6. Reboot.

To install R77.30.01 on a Gaia Security Management Server:

1. Back up your R77.30 Security Management Server.
2. Create a temporary directory.
3. Download the R77.30.01 installation file: R77.30.01.Gaia.tgz
4. Save the file to a temporary directory.
5. Connect to the management server with SSH.
6. Run these commands in expert mode:
   - tar -zxvf R77.30.01.Gaia.tgz
   - ./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 R77.30.01 SmartConsole:

Download the SmartConsole from the sk home page

Note - If you have another version of SmartConsole installed on your computer, you must first uninstall it, then install the R77.30.01 SmartConsole.

Java Upgrades

By default, Endpoint Security Server installed on Gaia OS runs Java 32-bit. Endpoint Security Server also supports Java 64-bit, which provides better performance for systems with RAM size equal to or larger than 4GB.

To use an Endpoint Security Server in 64-bit mode, you must configure Gaia OS to automatically boot to the 64-bit kernel edition and upgrade Java to 64-bit.

To use an Endpoint Security Server in 64-bit mode:

1. Connect to command line on Gaia OS.
2. Log in to clish.
   Run: `set edition 64-bit`
4. Save the Gaia Database.
   Run: `save config`
5. Reboot the computer.
6. Make sure that the Gaia OS booted with the 64-bit kernel edition.
   Run: `show version all`

To upgrade Java to 64-bit:

Run: `$UEPMDIR/system/utils/replace_ibm_jre_to_64_bit`

To revert Java to 32-bit:

Run: `$UEPMDIR/system/utils/replace_ibm_jre_to_64_bit uninstall`
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>8.7.534</td>
</tr>
<tr>
<td>Anti-Bot</td>
<td>8.60.1.866</td>
</tr>
<tr>
<td>Anti-Malware</td>
<td>8.6.0.86</td>
</tr>
<tr>
<td>Compliance</td>
<td>8.60.1.850</td>
</tr>
<tr>
<td>Capsule Docs</td>
<td>91.1.1271</td>
</tr>
<tr>
<td>Forensics</td>
<td>8.60.1.601</td>
</tr>
<tr>
<td>Media Encryption &amp; Port Protection</td>
<td>8.60.0.963</td>
</tr>
<tr>
<td>Firewall &amp; Application Control</td>
<td>8.60.910</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>86.0.109.5</td>
</tr>
<tr>
<td>Remote Access VPN</td>
<td>986000452</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>86.0.21.824</td>
</tr>
</tbody>
</table>

Known Limitations

All limitations from earlier E80.x releases apply unless they are listed as resolved.

Known limitations for this release are in sk108376