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=17164)
To learn more, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the E80.40 home page (http://supportcontent.checkpoint.com/solutions?id=sk82100).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 September 2013</td>
<td>Added Windows 7 in Endpoint Security Management Server Supported Operating Systems (on page 8)</td>
</tr>
<tr>
<td>27 February 2013</td>
<td>Improved clarity in Supported Languages for SmartEndpoint (&quot;Supported Languages&quot; on page 9) and Supported Languages for Endpoint Security Clients (on page 10) Added SmartEndpoint Requirements (on page 9)</td>
</tr>
<tr>
<td>19 December 2012</td>
<td>Added clarification to Supported Security Management Servers (on page 8)</td>
</tr>
<tr>
<td>3 December 2012</td>
<td>Updated Supported Client Operating Systems (on page 10)</td>
</tr>
<tr>
<td>5 November 2012</td>
<td>Improved formatting and layout.</td>
</tr>
<tr>
<td>23 October 2012</td>
<td>Updated Supported Security Management Servers (on page 8).</td>
</tr>
<tr>
<td>15 October 2012</td>
<td>Updated Build Numbers (on page 12).</td>
</tr>
<tr>
<td>11 October 2012</td>
<td>Added Supported Upgrade Paths (on page 11). Improved formatting and layout.</td>
</tr>
<tr>
<td>09 October 2012</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 Release Notes E80.40 ).
Introduction

Thank you for installing Check Point Endpoint Security E80.40 release. This version includes new features, improved management interface, and improved performance and security.

Note - This release continues the Endpoint Security R80 series. From E80.20 and higher, the versions of the series start with the letter E.

What's New

This release includes new features for the server and client.

Security Management Features

- This release supports Smart-1 appliances, Gaia and SecurePlatform.
- Manage Endpoint Security for both Windows and Mac platforms using a unified organizational Security Policy.
- A new Organizational Security Policy provides a full, understandable view of the security policies defined in the organization. You can see all policy rules, assignments and exceptions in a single, unified view.
- A new Security Analysis report shows an improved and easier to use view of enforcement status. You can monitor security violations and automatically receive e-mail notifications at predefined thresholds.

Additional Management Features

- A new WebRH portal gives online remote help for Full Disk Encryption and Media Encryption devices.
- Improved Active Directory Scanner integration and ease of use. Directory scanner now supports Multiple Domains without Trust Relationships.
- You can change details for users and computers that are not included in an Active Directory domain. You can change details, such as name, email address, and phone number.
- The management console shows improved information about client installation. Administrators see more data that makes it easier to understand and troubleshoot client installations.

Endpoint and Network Security Management Features

- Endpoint Security E80.40 is integrated with R75.40 management. You can use the E80.40 SmartConsole to manage the R75.40 network security objects. You can also use the R75.40 SmartConsole to manage non-Endpoint Security Software Blades in E80.40.
- Endpoint Security SmartEvent includes Full Disk Encryption, Media Encryption, Compliance, and Anti Malware analysis.
- Supports SmartLog and SmartEvent.
Client Side Features

**Media Encryption & Port Protection**
- Set granular access to encrypted business data and non-encrypted personal data on corporate computers.
- UserCheck™ engages and educates users to prevent most incidents of unintentional data loss. Upon potential data loss, UserCheck™ educates the user about the organizational security policy, and allows the user to request an immediate exception to the security policy (based on a logged justification).
- Thin client support: Citrix Provisioning Services 5.6 SP2.
- Support for eSATA devices.
- Improved logs in SmartView Tracker and SmartLog.

**Full Disk Encryption**
- Customize graphics in the pre-boot and OneCheck authentication screens.
- Support for hardware accelerated AES encryption, AES-NI.

**Support for Mac Clients**
- Endpoint Security R80.40 management and client support the following software blades on Mac:
  - Firewall for desktop security
  - Security Compliance
  - Full Disk Encryption
  - Remote Access VPN

**Free Endpoint Security Best Practice Analysis:**
This free tool provides immediate visibility of your current Endpoint Security picture and potential risks. It analyzes your security picture and supplies a report that includes 3 categories: Data Loss risks, Intrusion Risks, and Malware Risks.

The tool does not contain any active security components and is designed to provide a best practice analysis. It is for Windows based devices that run any security solution.

**VPN**

**Secure Domain Logon (SDL)**
The ability to establish a VPN tunnel prior to user domain logon, and secure the logon process by encrypting the session with the domain controller.

**Secure Client Verification (SCV) – With E80.40 SCV controlled by the EPS server**
Lets the administrator
- Monitor the configuration of remote computers
- Confirm that the configuration complies with the organization’s security policy
- Block connectivity for computers that do not comply.

**Secondary Connect and Multiple Entry Point (MEP).**
Gives access to multiple VPN gateways at the same time, and transparently connect to distributed resources.
- **Connections to Distributed Networks**
  End-users can connect once and get transparent access to resources, regardless of their location. Tunnels are created dynamically as needed, based on the destination of actual traffic.
**What’s New**

- **Enhanced Network Performance**  
  Traffic flows directly from the endpoint user to the gateway, without site-to-site communication.

- **Network Simplification**  
  VPN tunnels and routing parameters are automatically taken from the network topology and destination server IP address.

In an environment with Secondary Connect, the gateway that the client first authenticates to is the Primary gateway. A gateway that the client connects to through a secondary VPN is a Secondary gateway. The Primary gateway must have the Secondary Connect Hotfix installed. See sk65312 (http://supportcontent.checkpoint.com/solutions?id=sk65312).

**RSA Software Token**  
Support for RSA Software Token 4.1

**Intel Smart Connect Technology**  
When Intel Smart connect technology is enabled, the Remote Access client reconnects to the VPN automatically (based on the authentication method and configuration).

**Support for Secure Authentication API (SAA)**  
Allows third party-extensions to the standard authentication schemes. This includes 3-factor and biometrics authentication.

**Office Mode IP address lease auto renewal**  
The remote client automatically asks for an IP address lease renewal after half of the IP lease duration period has elapsed.

**Split DNS**  
Resolves internal names with the SecuRemote DNS Server configuration.

**Third Party SCV Checks**  
This release supports SCV checks created by third party vendors, using the Remote Access Clients E75.20 SCV SDK (http://www.opsec.com/cp_products/90.htm#sdk-e75). After installation, you can use these SCV checks in your SCV policies.

*Note* - Before using the Remote Access Clients SCV SDK, we strongly recommend that you read the Remote Access Clients SCV SDK Documentation.

**Improved Remote Access Clients API based on E75.20 API**  
The Remote Access Clients API is based on the Remote Access Clients E75.20 API (http://www.opsec.com/cp_products/90.htm#sdk-e75). It includes many improvements and backward compatibility support for future releases.

*Note* - Before using the API, read the Readme.txt file inside the zip file.

**Proxy Improvements for Endpoint Security VPN**  
This feature includes these enhancements for Endpoint Security VPN with proxy servers:

- Significantly faster connections from Endpoint Security clients to gateways when using a proxy server.
- Endpoint Security clients can now use a proxy server for outbound encrypted data.

**General improvements and bug fixes**
System Requirements

This section shows supported operating systems, gateways, and hardware requirements.

Endpoint Security Management Server Supported Operating Systems

- Gaia: All releases
- SecurePlatform
- All editions of Microsoft Windows Server 2003 and 2008 (including R2 for 2003 and 2008)
- Windows 7 Professional, Enterprise, Ultimate 32/64-bit
- VMware:
  - VMware vSphere 4.0, 4.1, 5.0
  - VMware ESXi 4.1.0, 5.0

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>4GB</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

E80.40 Endpoint Security is supported on Check Point Security Management Server R75.40 only. No HFAs or minor versions can be installed on top of the R75.40 Security Management Server.

- E80.40 is not supported on top of standalone R75.40 deployments (where the Security Management Server and Security Gateway are on the same computer).
- If E80.40 is installed on an R75.40 Security Management Server, you cannot upgrade the Security Management Server to R75.45.
- Installing E80.40 on top of R75.45 is not supported.

For information on requirements and supported Security Gateways for R75.40, see the R75.40 Release Notes (http://downloads.checkpoint.com/dc/download.htm?ID=13079).
Supported SmartConsole Platforms

The E80.40 SmartConsole is supported on these platforms:

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

**Notes**

- You can use the E80.40 SmartConsole clients to manage R75.40 Security Gateways and other objects.
- You can use the R75.40 SmartConsole to manage non-Endpoint Security Software Blades in E80.40.

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>2048MB</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 operating systems are:

- French
- German
- Spanish
- Italian

The Endpoint Security Management Server is supported only in English.
Supported Client Operating Systems

This release supports the Endpoint Security client on:

- Microsoft Windows 7 Enterprise, Professional, Ultimate editions 32/64-bit
- Microsoft Windows 7 Enterprise, Professional, Ultimate editions 32/64-bit SP1
- Microsoft Windows XP Professional 32-bit, SP3
- Microsoft Vista 32/64-bit, SP1
- Microsoft Windows Server 2003 32 bit (Supported blades: Compliance and Anti-Malware)
- Mac OS X 10.6 Snow Leopard
- Mac OS X 10.7 Lion
- Mac OS X 10.8 Mountain Lion

This release also supports these Blades on Windows servers:

<table>
<thead>
<tr>
<th>Windows Server</th>
<th>Supported Blades</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003 32-bit</td>
<td>Anti-Malware and Compliance</td>
</tr>
<tr>
<td>2008 32/64-bit</td>
<td>Anti-Malware, Compliance, and Firewall</td>
</tr>
<tr>
<td>2008 R2</td>
<td>Anti-Malware, Compliance, and Firewall</td>
</tr>
</tbody>
</table>

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:

1. Assign the server group or members to a new application control policy.
2. Disable application control in the policy.
3. Install the policy.

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
WebCheck Supported Browsers
WebCheck supports these browsers:
• Internet Explorer, versions 6, 7, 8, 9
• Mozilla Firefox, version 15

Media Encryption & Port Protection Support
Storage Devices
• Standard USB 2.0 and 3.0 devices
• eSATA devices
• CD/DVD devices
• SD cards
Supported Thin Clients
• Citrix Provisioning Services 5.6 SP2

Legacy Full Disk Encryption Support
You can upgrade to Full Disk Encryption in E80.40 from:
• FDE EW 6.3.1
• R73 and higher

Supported Upgrade Paths
Server Upgrade
The only supported upgrade path for E80.40 is from E80.3X on Windows platforms only. To upgrade to E80.40 from earlier versions, you must first upgrade your Endpoint Security Management Servers to E80.30. See the E80.30 Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk65921) for detailed procedures.

After you upgrade your Endpoint Security Management Server to E80.40, you can then migrate to a SecurePlatform or Gaia platform.

Client Upgrade
You can upgrade to E80.40 from earlier versions of R80.x and E80.x clients with these requirements:
• You must upgrade both the Initial Client and the Software Blade Package at the same time. You cannot upgrade the Initial Client by itself.
• During the upgrade you cannot remove the Full Disk Encryption or WebCheck blades.
• You can change all other Software Blades and all Software Blade configuration settings.
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>8.2.498</td>
</tr>
<tr>
<td>Compliance</td>
<td>8.14.0.4034</td>
</tr>
<tr>
<td>Media Encryption &amp; Port Protection</td>
<td>8.14.0.4061</td>
</tr>
<tr>
<td>Anti-Malware</td>
<td>8.2.10.93</td>
</tr>
<tr>
<td>Firewall &amp; Application Control</td>
<td>8.1.000.032</td>
</tr>
<tr>
<td>Remote Access VPN</td>
<td>836004025</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>80.1.30.59</td>
</tr>
<tr>
<td>WebCheck</td>
<td>1.6.616.0</td>
</tr>
<tr>
<td>Windows Client</td>
<td>814004498</td>
</tr>
<tr>
<td>Mac Client</td>
<td>811000151</td>
</tr>
</tbody>
</table>

Known Limitations

The E80.40 Known Limitations are available from the Support Center (http://supportcontent.checkpoint.com/solutions?id=sk82101).

Some R75.40 Known Limitations might also apply to Endpoint Security E80.40. We suggest that you read this document, which is also available from the Support Center (http://supportcontent.checkpoint.com/solutions?id=sk67582).