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=23861
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the E80.41 Endpoint Security Server home page (http://supportcontent.checkpoint.com/solutions?id=sk92101).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 February 2013</td>
<td>First release of this document</td>
</tr>
<tr>
<td>02 April 2013</td>
<td>Updated WebCheck Supported Browsers (on page 8)</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 E80.41 ).
Contents

Important Information .................................................................................................................. 3
Introduction ................................................................................................................................. 5
System Requirements .................................................................................................................. 5
  Endpoint Security Management Server Supported Operating Systems .............. 5
  Endpoint Security Management Server Hardware Requirements .................... 6
  Supported Security Management Servers ............................................................... 6
  Supported SmartConsole Platforms ........................................................................... 6
  Console Requirements ................................................................................................. 6
  Supported Languages ................................................................................................. 7
  Supported Client Operating Systems ................................................................. 7
  Client Languages ..................................................................................................... 7
  Client Hardware Requirements ............................................................................... 8
  WebCheck Supported Browsers ........................................................................... 8
  Media Encryption & Port Protection Support ..................................................... 8
  Legacy Full Disk Encryption Support ................................................................. 8
Installation and Upgrade ......................................................................................................... 8
  Before You Install .................................................................................................... 9
  Installing and Upgrading .................................................................................... 9
  Installing the New SmartConsole ....................................................................... 9
  Upgrading Secondary and Policy Servers ............................................................ 10
Known Limitations ................................................................................................................. 10
Introduction

Thank you for installing Check Point Endpoint Security E80.41 release. This release includes:

- Support for the R75.45 Security Management Server
- Management for E80.41 Endpoint Security clients
- All features from Endpoint Security E80.40
- Improved performance and security

This release is for:

<table>
<thead>
<tr>
<th>Audience</th>
<th>Current Environment</th>
<th>After Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>E80.40 and E80.41 Client Customers managed by E80.40 Endpoint Security Management server</td>
<td>E80.40 Endpoint Security Management server above R75.40</td>
<td>E80.41 Endpoint Security Management server above R75.45</td>
</tr>
<tr>
<td>Network security customers with R75.40 Security Management Server *</td>
<td>R75.40 Security Management Server</td>
<td>R75.45 Security Management Server with E80.41 Endpoint Security Server</td>
</tr>
<tr>
<td>Network security customers with R75.45 Security Management Server *</td>
<td>R75.45 Security Management Server</td>
<td>R75.45 Security Management Server with E80.41 Endpoint Security Server</td>
</tr>
</tbody>
</table>

*Standalone deployments are not supported

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)
  For Windows 2003 SP1, you must install the hotfix specified in Microsoft KB 906469
  ([http://support.microsoft.com/kb/906469](http://support.microsoft.com/kb/906469))
- Windows 7 Enterprise 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

E80.41 Endpoint Security is supported on Check Point Security Management Server R75.45 only. No HFAs or minor versions can be installed on top of the R75.45 Security Management Server.

E80.41 is not supported on top of standalone R75.45 deployments (where the Security Management Server and Security Gateway are on the same computer).

For information on requirements and supported Security Gateways for R75.45, see the R75.45 Release Notes http://supportcontent.checkpoint.com/solutions?id=sk82740.

Supported SmartConsole Platforms

The E80.41 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 8 Enterprise, Professional 32/64-bit
- Microsoft Windows 7 Enterprise, Professional, Ultimate editions 32/64-bit with or without SP1
- Microsoft Windows XP Professional 32-bit, SP3
- Microsoft Windows Vista 32-bit, SP1

Console Requirements

This table shows the minimum hardware requirements for the SmartConsole applications, including the SmartEndpoint.

<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 Endpoint Security Management Console is available in English.
- The SmartEndpoint supports operating systems in other languages, but is in English only. The other supported localized operating systems are:
  - French
  - German
  - Spanish
  - Italian

Supported Client Operating Systems

This release supports the Endpoint Security client on:

- Microsoft Windows 8 Enterprise, Professional 32/64-bit: For new client installations only
- Microsoft Windows 7 Enterprise, Professional, Ultimate editions 32/64-bit with or without SP1
- Microsoft Windows XP Professional 32-bit, SP3
- Microsoft Vista 32/64-bit, SP1
- 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:

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

b) Disable application control in the policy.

c) Install the policy.

Client Languages

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 17

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 E80.41 from:

- FDE EW 6.3.1
- R73 and higher

Installation and Upgrade

You can install E80.41 Endpoint Security Management server on top of:

- E80.40
- R75.40
- R75.45 without Endpoint Security

If you upgrade from E80.40 management and want to use E80.41 clients, get E80.41 clients from sk91181 (http://supportcontent.checkpoint.com/solutions?id=sk91181) and upload them to the Package Repository manually.

Note - You cannot upgrade from R75.45VS to this version.

Get all files from sk92101 (http://supportcontent.checkpoint.com/solutions?id=sk92101).
Before You Install

**Windows 7** - Turn off User Account Control (UAC) before you install on Windows 7. Reboot after the installation.


Installing and Upgrading

Run all installations from the command line. Do not double-click to install the package on Windows.

Download the .tgz file for your platform from sk92101 (http://supportcontent.checkpoint.com/solutions?id=sk92101).

You can safely delete the .tgz file after you extract the package.

**To install E80.41 with the CLI:**

1. Log on to the target machine.
   
   On SecurePlatform only:
   
   a) Run idle 120 to make sure that the installation is not stopped by the automatic logon timeout.
   
   b) Run expert to enter the expert mode.

2. Make sure the target computer or appliance has sufficient free disk space.

3. Create a temporary directory in the /var/tmp partition on non-Windows platforms, or in the c:\ partition on Windows platforms.

4. Copy the upgrade package for your platform to the temporary directory using SFTP, SCP, or other secure utility.

5. Go to the temporary directory and extract the .tgz package.
   
   - On non-Windows platforms, run: gtar -zxvf <file name>
   
   - On Windows platforms, use an archive utility, with administrator privileges.

6. Start installation:
   
   - On non-Windows platforms, from the temporary directory created in /var/tmp, run: ./UnixInstallScript.
     
     You must run this command from the temporary directory created in /var/tmp.
   
   - On Windows platforms, run: Setup.exe

7. Do the instructions on the screen to install the components.
   
   When the installation is completed, each successfully installed component shows in a list as Succeeded.

8. When prompted, reboot the computer.
   
   In a cluster environment, make sure to upgrade all the cluster members.

For procedures not included here, see the E80.40 Installation and Upgrade Guide (http://supportcontent.checkpoint.com/solutions?id=sk82100).

Installing the New SmartConsole

Download the SmartConsole for Endpoint Security E80.41 (http://supportcontent.checkpoint.com/solutions?id=sk92101) to your GUI client computer and install the file.

If you have an older version of SmartConsole, uninstall it before you install the new SmartConsole.
Upgrading Secondary and Policy Servers

The basic procedure for upgrading Secondary or Endpoint Policy Servers is the same as for the Primary (Active) server.

**To upgrade a High Availability environment:**

1. Upgrade the Active Endpoint Security Management server.
   a) Before you restart the Active Endpoint Security Management server, run `cpstop` on all Standby Endpoint Security Management servers.
   b) Restart the Active Endpoint Security Management server.


3. Do these steps for each Standby and Endpoint Policy Server:
   a) In the SmartDashboard Firewall tab, double click the network object for each Endpoint Security Management server and Endpoint Policy Server.
   b) On the General Properties pane, make sure that the Version is set to R75.45. Change if necessary.
   c) Click **OK** and save your changes.
   d) Install the database.

4. Manually synchronize the Active server to the Standby servers.
   This causes the Active database to overwrite the Standby database.

**Note** - An Endpoint Policy Server with a version lower than the Endpoint Security Management Server continues to communicate with clients, but will not synchronize with the newer Endpoint Security Management Server.

Known Limitations

The E80.41 Known Limitations are in sk92102 (http://supportcontent.checkpoint.com/solutions?id=sk92102).

Known limitations for E80.40 (http://supportcontent.checkpoint.com/solutions?id=sk82101) also apply to this release.

Some R75.45 Known Limitations http://supportcontent.checkpoint.com/solutions?id=sk82740 apply to Endpoint Security E80.41.