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=19761
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>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 Management Server E80.40 Installation and Upgrade Guide).
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Getting Started</td>
<td>6</td>
</tr>
<tr>
<td>Planning Endpoint Security Management Server Installation</td>
<td>6</td>
</tr>
<tr>
<td>Installation Prerequisites</td>
<td>7</td>
</tr>
<tr>
<td><strong>Endpoint Security Licenses</strong></td>
<td>8</td>
</tr>
<tr>
<td>Endpoint Security Product Licenses</td>
<td>8</td>
</tr>
<tr>
<td>Demo and Temporary Licenses</td>
<td>9</td>
</tr>
<tr>
<td>License Enforcement</td>
<td>9</td>
</tr>
<tr>
<td>Getting Licenses</td>
<td>9</td>
</tr>
<tr>
<td>Getting and Applying Contracts</td>
<td>10</td>
</tr>
<tr>
<td>Configuring a Proxy for Internet Access</td>
<td>10</td>
</tr>
<tr>
<td><strong>License Status</strong></td>
<td>11</td>
</tr>
<tr>
<td><strong>Installing Endpoint Security</strong></td>
<td>12</td>
</tr>
<tr>
<td>Installing an Endpoint Security Management Server on Windows</td>
<td>12</td>
</tr>
<tr>
<td>Windows</td>
<td>12</td>
</tr>
<tr>
<td>Changing the Endpoint Security Management Server Initial Settings</td>
<td>13</td>
</tr>
<tr>
<td>Installing an Endpoint Security Management Server on Gaia</td>
<td>13</td>
</tr>
<tr>
<td>Installing Gaia</td>
<td>13</td>
</tr>
<tr>
<td>Using the Gaia First Time Configuration Wizard</td>
<td>14</td>
</tr>
<tr>
<td>Installing the E80.40 Endpoint Security Overlay</td>
<td>14</td>
</tr>
<tr>
<td>Installing an Endpoint Security Management Server on SecurePlatform</td>
<td>15</td>
</tr>
<tr>
<td>Installing SecurePlatform</td>
<td>15</td>
</tr>
<tr>
<td>Installing E80.40 SmartConsole</td>
<td>16</td>
</tr>
<tr>
<td>Initial Endpoint Security Management Server Configuration</td>
<td>17</td>
</tr>
<tr>
<td><strong>Installing External Endpoint Policy Servers</strong></td>
<td>19</td>
</tr>
<tr>
<td>Installing on Windows</td>
<td>19</td>
</tr>
<tr>
<td>Installing on Gaia</td>
<td>20</td>
</tr>
<tr>
<td>Installing on SecurePlatform</td>
<td>20</td>
</tr>
<tr>
<td>Configuring an Endpoint Policy Server</td>
<td>20</td>
</tr>
<tr>
<td>Troubleshooting SIC Trust</td>
<td>21</td>
</tr>
<tr>
<td><strong>Installing Endpoint Security Management Servers for High Availability</strong></td>
<td>23</td>
</tr>
<tr>
<td>Installing on Windows</td>
<td>23</td>
</tr>
<tr>
<td>Installing on Gaia</td>
<td>24</td>
</tr>
<tr>
<td>Installing on SecurePlatform</td>
<td>24</td>
</tr>
<tr>
<td>Secondary Server Configuration</td>
<td>24</td>
</tr>
<tr>
<td><strong>Special Installation Scenarios</strong></td>
<td>26</td>
</tr>
<tr>
<td>Configuring the Apache Cache</td>
<td>26</td>
</tr>
<tr>
<td>Viewing Scheduled Tasks</td>
<td>26</td>
</tr>
<tr>
<td>Changing the Clean-up Task Status</td>
<td>26</td>
</tr>
<tr>
<td>Scheduling a New Clean-up</td>
<td>27</td>
</tr>
<tr>
<td>Users Created at Installation</td>
<td>27</td>
</tr>
<tr>
<td><strong>Upgrading the Endpoint Security Management Server</strong></td>
<td>28</td>
</tr>
<tr>
<td>Upgrading on a Windows Endpoint Security Management Server</td>
<td>28</td>
</tr>
<tr>
<td>Upgrading Secondary and Policy Servers</td>
<td>29</td>
</tr>
<tr>
<td>Migrating to a Different Platform</td>
<td>29</td>
</tr>
<tr>
<td>Exporting the Databases and Configuration Files</td>
<td>30</td>
</tr>
<tr>
<td>Importing the Databases and Configuration Files</td>
<td>30</td>
</tr>
<tr>
<td>Migrating the Packages Repository - Manual</td>
<td>31</td>
</tr>
<tr>
<td>Directory Scanner Issues</td>
<td>32</td>
</tr>
<tr>
<td><strong>Upgrading Endpoint Security Clients</strong></td>
<td>33</td>
</tr>
<tr>
<td>Upgrading Clients to E80.40</td>
<td>33</td>
</tr>
<tr>
<td>Notes and Cautions - Windows</td>
<td>33</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Upgrading with Deployment Rules</td>
<td>33</td>
</tr>
<tr>
<td>Upgrading with an Exported Package</td>
<td>34</td>
</tr>
<tr>
<td>Gradual Upgrade</td>
<td>34</td>
</tr>
<tr>
<td>Upgrading Legacy Clients</td>
<td>34</td>
</tr>
<tr>
<td>Offline Upgrades</td>
<td>34</td>
</tr>
<tr>
<td>Online Upgrades</td>
<td>35</td>
</tr>
<tr>
<td>Uninstalling the Endpoint Security Client</td>
<td>36</td>
</tr>
<tr>
<td>Upgrading Media Encryption R73.x Devices and Keys</td>
<td>36</td>
</tr>
</tbody>
</table>
Chapter 1

Getting Started

In This Chapter
Planning Endpoint Security Management Server Installation 6
Installation Prerequisites 7

Planning Endpoint Security Management Server Installation

Before you begin installation, check these items:

- The diagram below shows installation options, where (1) represents the Endpoint Security Management server and (2) represents the Endpoint Policy Server.
  Decide whether to install Endpoint Policy Servers in a distributed architecture (option A); or to use only the Endpoint Policy Server embedded in the Security Management Server (option B).
  It is recommended that remote sites have at least one external Endpoint Policy Server on a dedicated computer for each remote site, and that large sites have multiple Endpoint Policy Servers to ensure good performance.

- Make sure there is connectivity between the Security Management Server and the Endpoint Policy Servers.

- Connectivity between multiple Endpoint Policy Servers is not necessary, but every client must be able to communicate with at least one Endpoint Policy Server.

- Make sure the computers on which the Endpoint Security components (Endpoint Security Management Server, SmartEndpoint, and Endpoint Policy Servers) will be installed are on supported platforms (see the E80.40 Release Note (http://supportcontent.checkpoint.com/documentation_download?ID=17164)

- Make sure that these ports are free to be used by the Endpoint Security Management Server installation:
  80, 81, 443, 1081, 4434, 6666, 8005, 8009, 8080, 8443, 18193, 61616
• When an Endpoint Security client is connected to the Endpoint Security Management Server or Endpoint Policy Server through a proxy, the client’s IP address might be obscured by the proxy’s IP address. To avoid this, configure the proxy to use the X-Forwarded-For HTTP header.

**Installation Prerequisites**

Before installing Endpoint Security Management Server, make sure the required ports are free.

---

**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.
Chapter 2

Endpoint Security Licenses

In This Chapter

| Endpoint Security Product Licenses | 8 |
| Demo and Temporary Licenses | 9 |
| License Enforcement | 9 |
| Getting Licenses | 9 |
| Getting and Applying Contracts | 10 |
| License Status | 11 |

This chapter includes license information for Endpoint Security Servers and Clients. All Endpoint Security licenses are physically installed on the Endpoint Security Management Server.

Endpoint Security Product Licenses

This section describes the required Product licenses for Endpoint Security.

<table>
<thead>
<tr>
<th>License Type</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Container license</td>
<td>One license for each endpoint client (seat). This license is attached to the Endpoint Agent.</td>
</tr>
<tr>
<td>Software Blade licenses</td>
<td>One license for each Endpoint Security Software Blade installed on an endpoint client (seat). The blade licenses include:</td>
</tr>
<tr>
<td></td>
<td>• Full Disk Encryption</td>
</tr>
<tr>
<td></td>
<td>• Media Encryption &amp; Port Protection</td>
</tr>
<tr>
<td></td>
<td>• WebCheck</td>
</tr>
<tr>
<td></td>
<td>• Malware Protection</td>
</tr>
<tr>
<td></td>
<td>• Network Protection - Bundle license that includes Endpoint Security Firewall, Compliance Rules, Application Control, and Access Zones. This license automatically comes with the Container License.</td>
</tr>
<tr>
<td>Management license</td>
<td>A license for each Endpoint Security management server. The management license also includes these management blades:</td>
</tr>
<tr>
<td></td>
<td>• Management</td>
</tr>
<tr>
<td></td>
<td>• Logging &amp; Status</td>
</tr>
<tr>
<td></td>
<td>• User Directory.</td>
</tr>
<tr>
<td>VPN License</td>
<td>A license for the VPN gateway that endpoint users connect to. You Install this license on the Security Management Server that manages VPN gateways. Do NOT install a VPN license on the Endpoint Security Management server.</td>
</tr>
</tbody>
</table>
Demo and Temporary Licenses

These demo and trial Endpoint Security licenses are available:

<table>
<thead>
<tr>
<th>License type</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demo License</td>
<td>A 15 day demo license is automatically installed with Check Point network security products. This license lets you use Security Gateways, the Security Management Server and all SmartConsole applications.</td>
</tr>
<tr>
<td>Trial License</td>
<td>A 30 day trial license is automatically installed when you install Endpoint Security. This license lets you use all Endpoint Security Blades for a limited number of endpoint client seats.</td>
</tr>
<tr>
<td>Evaluation</td>
<td>An evaluation license is available for specified software blades for a specified number of seats.</td>
</tr>
<tr>
<td>Product</td>
<td>You must purchase a Product license for each Endpoint Security Software Blade running on a client. Licenses can be purchased as a Subscription, a contract that is renewed annually, or a one-time purchase.</td>
</tr>
</tbody>
</table>

License Enforcement

License activity conforms to these conditions:

- You can add Endpoint Security licenses as required using one of these methods:
  - SmartUpdate
  - The Gaia or SecurePlatform WebUI.
  - The cplic command
  - The cpconfig command for Windows platforms
- You can remove a client license by resetting the client or deleting the client using SmartEndpoint. These licenses are returned to the license pool.
- Each client gets its Container and Blade licenses from a pool of available licenses.
- You can combine licenses to reach the total number of required clients.
- License validation occurs when the client sends a SYNC or heartbeat messages to the server.
- When there is no container license, software blade registration is blocked.

Getting Licenses

This procedure assumes that you have a user account for the Check Point User Center, and that the necessary licenses and contracts are purchased.

To get the license for your Endpoint Security Management Server:

1. Log in to Check Point User Center (http://usercenter.checkpoint.com).
2. Click Products.
   The page shows the purchased licenses.
   Endpoint Security licenses have these parts in the SKU:
   - CPEP - Check Point Endpoint Security containers.
   - CPSB - Check Point Software Blade. If the macro string includes the -SUBSCR suffix, you must get and apply a contract for this feature ("Getting and Applying Contracts" on page 10).
3. For each license, select License in the drop-down menu at the right of the row.
4. Fill in the form that opens.
   - Make sure that Version is R80 and above.
   - Make sure that the IP Address is the IP address of the Endpoint Security Management Server.
5. Click License.
   A window opens, showing the license data.
6. Save the license file.
7. Add your licenses using one of these methods:
   - SmartUpdate
   - The Gaia or SecurePlatform WebUI.
   - The cplic CLI command
   - The cpconfig command for Windows platforms

**Getting and Applying Contracts**

If the license includes -SUBSCR, you must download the contract file and apply it to the server. If the Endpoint Security Management server has Internet access, it automatically renews contracts. By default, the Endpoint Security Management server looks for new contracts every two hours.

To change the default time interval:
1. Open this file:
   ```shell
   $CPDIR/conf/downloads/dl_prof_CNTCRMGR.xml
   ```
2. Change the <interval> value as necessary.
3. Run cpstop and cpstart.

To apply a contract manually:
1. Log in to Check Point User Center (http://usercenter.checkpoint.com).
2. Click Products.
3. Select Get Contracts File in the drop-down menu at the right of the row.
4. In the window that opens, save the contract file and click Open.
5. Open SmartUpdate. (Start menu > Check Point > SmartUpdate)
7. In the window that opens, browse to where you saved the contract file and click Open.
   The contract is applied to the Endpoint Security Management Server.

If the Endpoint Security Management Server does not have access to the Internet, prepare the contract file download from the User Center differently.

To download a contract to a different computer:
1. In the User Center, click Products > Additional Services.
2. Select the account of the contract.
3. Click Email File or Download Now.
4. When you have the contract file, move it to the Endpoint Security Management Server.

**Configuring a Proxy for Internet Access**

If the Endpoint Security Management server requires a proxy to connect to the internet, you can configure the proxy details in SmartDashboard.

To configure a proxy for the whole environment:
1. In SmartDashboard, select Global Properties > Proxy.
2. Select Use proxy server.
3. Enter the URL and port.
4. Click OK.
5. Select File > Save.
To configure a proxy for the Endpoint Security Management server:
1. In SmartDashboard, open the Endpoint Security Management server object.
2. Select **Topology > Proxy**.
3. Select **Use custom proxy settings for this network object**.
4. Enter the URL and port.
5. Click **OK**.
6. Select **File > Save**.

**License Status**

You can see the status of container and blade licenses in Endpoint Security Management server on the **Reporting** tab > **Licenses Report**. This pane shows the total number of seats and seats in use. If the number of seats exceeds the number of licenses, you must add the number of licenses shown as **Insufficient Seats**.

The lower section of the report shows the details of each license including:

- License Name and status
- Software Blades
- Seats in Use
- Total seats
- Percentage of total licenses in use
- Expiration date
- IP address of license host
Chapter 3

Installing Endpoint Security

In This Chapter
- Installing an Endpoint Security Management Server on Windows • 12
- Installing an Endpoint Security Management Server on Gaia • 13
- Installing an Endpoint Security Management Server on SecurePlatform • 15
- Installing E80.40 SmartConsole • 16
- Initial Endpoint Security Management Server Configuration • 17

Installing an Endpoint Security Management Server on Windows

This section includes instructions for installing an Endpoint Security Management server on a Windows platform.

The procedure for installing an Endpoint Security Management server on a Windows platform includes these steps:

1. Install the E80.40 Endpoint Security Management server ("Windows" on page 12).
2. Install the E80.40 SmartConsole client applications ("Installing E80.40 SmartConsole" on page 16) on your management computers.
3. Run the Express Setup Wizard to do the initial configuration steps ("Initial Endpoint Security Management Server Configuration" on page 17) in SmartEndpoint.

Windows

To install E80.40 Endpoint Security on Windows Server:

1. Log in to Windows using Administrator credentials.
2. Put the installation media in the drive.
   The installation wizard starts automatically.
   Click Next.
3. Accept the License Agreement
   Click Next.
4. Select New installation
5. Click Next.
6. Select Custom and click Next.
8. Clear all other options and then click Next.
9. Click next to accept the default installation path and click Next.
10. Select Primary Security Management and click Next.
11. Click Next to start the installation.
12. After the installation completes, add your licenses and click Next.
   You can use the 15 Trial Period license for initial testing.
13. Enter the SmartConsole administrator name and password and then click Next.
14. Enter the remote client IP addresses that can connect to this Security Management Server and click Next.
   You can enter any to let all remote clients connect.
15. Click **Next** to initialize the Certificate Authority.
16. In the **Fingerprint** window, optionally save the fingerprint and click **Next**.
17. Click **Finish**.

### Changing the Endpoint Security Management Server Initial Settings

After the installation and initial configuration, you can use the Check Point Configuration tool to change the Endpoint Security Management server initial settings.

**To change the Endpoint Security Management server configuration settings:**
1. Run **Start > All Programs > Check Point SmartConsole R75.40 > Check Point Configuration**.
2. In the **Check Point Configuration Tool** window, change these settings as necessary:
   - Licenses and Contracts
   - Administrators
   - GUI Clients
   - Key Hit Session (Regenerate cryptographic seed).
   - Certificate Authority
   - Fingerprint

### Installing an Endpoint Security Management Server on Gaia

The procedure for installing an Endpoint Security Management server on Gaia includes these steps:

1. Install the Gaia operating system (**"Installing Gaia" on page 13**).
2. Use the First Time Configuration Wizard (**"Using the Gaia First Time Configuration Wizard" on page 14**).
3. Install the E80.40 overlay package.
4. Install the E80.40 SmartConsole client applications (**"Installing E80.40 SmartConsole" on page 16**) on your management computers.
5. Run the **Express Setup Wizard** (**"Initial Endpoint Security Management Server Configuration" on page 17**) to do the initial configuration steps in SmartEndpoint.

### Installing Gaia

This procedure explains how to install the Gaia operating system on an open server. Then you configure the Standalone Check Point products.

**To install Gaia on an open server:**

1. Start the computer using the installation DVD.
2. When the first screen shows, select **Install Gaia on the system** and press **Enter**.
3. Select **OK**. You must press **Enter** in 60 seconds, or the computer will try to start from the hard drive. The timer countdown stops when you press **Enter**. There is no time limit for the subsequent steps.
4. Select **OK** to continue with the installation.
5. Select a keyboard language. English US is the default.
6. Make sure the disk space allocation is appropriate for the environment. Select **OK**.
7. Enter and confirm the password for the **admin** account. Select **OK**
8. Select the management interface (default = **eth0**).
9. Configure the management IP address, net mask and default gateway. You can define the DHCP server on this interface. Select **OK**
10. Select **OK** to format your hard drive and start the installation.
11. Select **Reboot** to complete the installation.
Using the Gaia First Time Configuration Wizard

This procedure configures Gaia and installs R75.40.

To configure Gaia for the first time:
1. Using your Web browser, go the WebUI:
   https://<Gaia management IP address>
2. In the Gaia Portal window, log in using the administrator name and password that you defined during the installation procedure.
3. In the First Time Configuration Wizard welcome screen, click Next.
4. Set the date and time (manually, or enter the hostname or IP address of the NTP server) and then click Next.
5. Set the host name, domain name, and DNS servers for IPv4 addresses and then click Next.
6. Set the IPv4 address for the management interface.
7. Optional: Configure the appliance as a DHCP server and click Next.
8. Select Security Management and then click Next.
9. Enter a user name and password for the Security Management server administrator account and then click Next.
10. Define the GUI Clients that can log in to the Security Management server and Endpoint Security Management server and then click Next.
11. Click Finish and then click OK.
12. If the Help Check Point Improve Software Updates window shows, click Yes or No as necessary.
The First Time Wizard completes the process and the Gaia Portal is ready for use.

Installing the E80.40 Endpoint Security Portal Overlay

Before you install the Endpoint Security overlay, we recommend that you save an image of the server. See Image Management in the R75.40 Gaia Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk76540).

2. On the R75.40 server, change the shell to bash ("Defining the Expert Mode to Use the Bash Shell" on page 15).
3. Log in to the Endpoint Security Management server with bash shell permissions.
4. Copy the file that you downloaded to the /var/tmp folder.
   ! Important - Do not save this file to the /var folder itself. This will cause installation failure and problems with SSH communication.
5. Run tar –zxvf Check_Point_E80.40.linux.tgz.
6. Run chmod –R 777 *
7. Run ./UnixInstallScript.
8. Select Endpoint Server Installation.
9. Press y to reboot the computer.
10. Copy /linux/windows/SmartConsole.exe to the Windows computer that manages the Endpoint Security Management server.
11. Run SmartConsole.exe to install the SmartConsole clients.
   ! Important - If you log in to the server platform using the WebUI, you must connect using port 4434. Port 443 will not work for this.
Defining the Expert Mode to Use the Bash Shell

To work in the Gaia expert mode after installing the E80.40 Endpoint Security overlay:

1. Log in to the WebUI using this URL:
2. Select User Management > Users.
3. Click Add to create a new user.
4. In the Add User window:
   a) Create a new user.
   b) Assign the adminRole to this user.
   c) Set the Shell to /bin/bash.

When you log in as this user, you are automatically in the expert mode with the bash shell.

Installing an Endpoint Security Management Server on SecurePlatform

The procedure for installing Endpoint Security Management server on SecurePlatform includes these steps:

1. Install the SecurePlatform operating system and R75.40 Security Management Server ("Installing SecurePlatform" on page 15).
2. Install the E80.40 overlay package.

Installing SecurePlatform

To install an Endpoint Security Management server on SecurePlatform:

1. When the SecurePlatform window opens, press Enter.
   You must press Enter in 90 seconds, or the computer starts from the hard drive.
2. If error messages show during the hardware compatibility scan, correct the problems and then do this procedure again from step 1.
   If you receive a warning message, you can optionally continue the installation.
3. Optional: Click Device List to resolve hardware compatibility issues.
4. Click OK to continue with the installation.
5. Select a keyboard language and then click OK.
6. Select eth0 as the management interface and then click OK.
7. Configure the settings for eth0 and then click OK.
8. Select if you want to allow web based configuration and on which port. Then click OK.
   
   Note - Do not use the default port, 443.

9. Click OK to reformat the hard drive and install SecurePlatform.
10. When the Complete window shows, remove the DVD drive from the computer.
11. Click OK to complete the installation process and reboot the computer.

To configure SecurePlatform using the CLI:

1. Log in using the default login name/password: admin/admin.
2. Enter and confirm a new password for the administrator account.
3. Optional: Enter a new name for the administrator account.
4. Run: sysconfig.
   The first-time system configuration wizard starts. Enter n to continue.
5. Set the host name, domain name, and DNS servers.
6. Configure the settings for the management and other interfaces (network connections).

7. Configure the settings for the routing table and then enter n.

8. Set the date and time and then enter n.

Installing an R75.40 Security Management Server

To install an R75.40 Security Management Server on SecurePlatform:

1. To import a product configuration file from a TFTP server, enter 1 and do the instructions on the screen. Otherwise, enter n to continue.

2. In the Welcome window, press n to continue.

3. Enter y to accept the End User License agreement.

4. Select New Installation and then press n.

5. Select only Check Point management to install, and then press n.


7. Press n to confirm.

8. Enter n to enter your licenses later (recommended) using SmartUpdate or the WebUI.

9. Do the on-screen instructions to add administrators and GUI clients.

10. Press y to start the installed products.

11. Restart the computer.

Installing the E80.40 Endpoint Security Overlay

Before you install the Endpoint Security overlay, we recommend that you save an image of the server. See Image Management in the R75.40 Gaia Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk76540).


2. On the R75.40 server, change the shell to bash ("Defining the Expert Mode to Use the Bash Shell" on page 15).

3. Log in to the Endpoint Security Management server with bash shell permissions.

4. Copy the file that you downloaded to the /var/tmp folder.

   **Important** - Do not save this file to the /var folder itself. This will cause installation failure and problems with SSH communication.

5. Run tar –zxvf Check_Point_E80.40.linux.tgz.

6. Run chmod -R 777 *

7. Run ./UnixInstallScript.

8. Select Endpoint Server Installation.

9. Press y to reboot the computer.

10. Copy /linux/windows/SmartConsole.exe to the Windows computer that manages the Endpoint Security Management server.

11. Run SmartConsole.exe to install the SmartConsole clients.

   **Important** - If you log in to the server platform using the WebUI, you must connect using port 4434. Port 443 will not work for this.

Installing E80.40 SmartConsole

The SmartConsole clients install automatically on a Windows Endpoint Security Management server. You must install the SmartConsole clients manually on each GUI client that connects to the SmartConsole or SmartEndpoint.

Before you install the SmartConsole, you must install .Net Framework 3.5 SP1.
To install E80.40 SmartConsole from the installation media:
1. Make sure that .Net Framework 3.5 SP1 is installed on the computer.
2. Run the setup.exe in the \Windows\CPclnt\ folder on the distribution media.
3. From the Welcome screen, click Next.
4. Accept the Software License agreement.
5. Click Next to accept the default location or select a different installation folder.
6. Make sure that all relevant SmartConsole applications are selected for installation and click Next.
7. Click Finish.
   You can clear the option to automatically start SmartDashboard.

To run SmartEndpoint:
Run Start > All Programs > Check Point SmartConsole E80.40 > SmartEndpoint.

Initial Endpoint Security Management Server Configuration
You can use the Endpoint Security Express Setup Wizard to do these initial configuration steps after a new installation:

- Enable or disable each Software Blade as necessary
- Configure default actions and rules for each Software Blade
- Configure the default deployment rules for each Software Blade
- Make sure that the administrator doing the initial configuration has Read Only AD permissions and can read deleted containers.
- Run the Directory Scanner to import Active Directory objects to the Endpoint Security Management server
- Configure passwords for upgrading legacy R73 Secure Access and Full Disk Encryption to the current version.
- Export Software Blade packages to your SmartEndpoint computer for distribution to endpoint clients.

To run the Express Setup Wizard:
1. Run SmartEndpoint.
2. In the Overview, click the Getting Started link.
3. In the Express Setup Wizard window, click Next.
4. On the Policy Configuration page:
   - Enable and disable Software Blades as necessary.
   - Configure the default security rule for each Software Blade. In many cases you can use the default settings right out of the box. To learn more, see the Software Blade chapters in the E80.40 Endpoint Security Management Server Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk82100).
7. On the Deployment page:
   - Select Support R73 Client Upgrade and enter the legacy R73 Secure Access and Full Disk Encryption passwords. Do this only if you are upgrading from these releases.
   - Select the Select Virtual Group option to automatically add endpoint clients to virtual groups when the installation packages are deployed. Click New to create a new group.
• Click **Export Package** to export the Software Blade packages to your SmartEndpoint client. Select the endpoint type (Desktop or Laptop) and Windows edition (32-bit or 64-bit). Enter the path to the location on your SmartEndpoint client.

8. Click **Finish**.

Your Endpoint Security Management server is now ready for use.
Chapter 4

Installing External Endpoint Policy Servers

In This Chapter

- Installing on Windows 19
- Installing on Gaia 20
- Installing on SecurePlatform 20
- Configuring an Endpoint Policy Server 20
- Troubleshooting SIC Trust 21

We recommend that you use a distributed deployment that contains external Endpoint Policy Servers on dedicated computers.

- Install at least one Endpoint Policy Server for each remote site.
- For larger sites, install many Endpoint Policy Servers to improve performance.

⚠️ Important - When you add an Endpoint Policy Server to a High Availability deployment, you must install the database in SmartDashboard on all Endpoint Security Management servers and Endpoint Policy Servers. To do this, select Policy > Install Database.

Installing on Windows

Do these procedures to install an Endpoint Policy Server on a Windows computer.

To install an Endpoint Policy Server:
1. Log in to Windows using Administrator credentials.
2. Put the installation media in the drive.
   - The installation wizard starts automatically.
   - Click Next.
3. Accept the License Agreement
   - Click Next.
4. Select New installation
5. Click Next.
6. Select Custom and click Next.
7. Select Endpoint Security and click Next.
8. Optional: In the Destination Folder page, click Browse to select a different folder for the installation
9. Click Next.
10. In the Security Management Type page, select Policy Server and click Next.
    - The products that will install show on the screen.
11. Click Next to start the installation.

When the installation is complete, the wizard continues with initial configuration.
To continue the installation wizard:
1. In the Licenses and Contract page, select an option and click Next.
   - Use Trial Period license - You can use the 15 Trial Period license for initial testing.
   - Add a new license
2. In the Add Administrator page, enter the SmartConsole Administrator Name and Password and then click Next.
3. In the GUI Clients page, enter the IP addresses of remote computers that can connect to this server and click Next. You can enter any to let all remote clients connect.
4. In the Secure Internal Communication page, enter and confirm a Secure Internal Communication (SIC) Activation Key and click Next.
5. Click Finish.
6. Click OK to restart the computer.

Installing on Gaia

Do these procedures to install an Endpoint Policy Server on a Gaia computer.

To install an Endpoint Policy Server on Gaia:
1. Install Gaia ("Installing Gaia" on page 13).
2. Do the procedure in Using the Gaia First Time Configuration Wizard (on page 14) with this change: In the step where you select Security Management, you must also select Log Server or SmartEvent Server.
3. Do the procedure in Installing the E80.40 Endpoint Security Overlay (on page 14) with this change: After you run ./UnixInstallScript, select Policy Server Installation.

Installing on SecurePlatform

Do these procedures to install an Endpoint Policy Server on a SecurePlatform computer.

To install an Endpoint Policy Server on SecurePlatform:
1. Install SecurePlatform ("Installing SecurePlatform" on page 15).
2. Do the procedure in Installing an R75.40 Security Management Server (on page 16) with this change: Select Log Server and NOT Primary Security Management.
   In the Secure Internal Communication page, enter and confirm a Secure Internal Communication (SIC) Activation Key
3. Do the procedure in Installing the E80.40 Endpoint Security Overlay (on page 14) with this change: After you run ./UnixInstallScript, select Policy Server Installation.

Configuring an Endpoint Policy Server

In SmartEndpoint, you add the Endpoint Policy Server to the list of servers and create SIC trust between the Endpoint Policy Server and Endpoint Security Management server. This also creates an object for the Endpoint Policy Server in SmartDashboard.

To create the Endpoint Policy Server in SmartEndpoint:
1. Log into SmartEndpoint using the IP address and credentials for the Primary Endpoint Security Management server.
2. Select Manage > General Properties.
3. In the Endpoint Policy Server pane, click New.
4. In the Select New Object Type window, select Host and click OK.
   The Host Properties window for the server opens.
5. Enter a Name for the Endpoint Policy Server and its IP address.
6. Click Communication to create SIC communication with the Endpoint Security Management server.
7. In the Communication window:
a) Enter and confirm the SIC Activation Key that you entered in the Check Point Configuration Tool.
b) Click Initialize to create a state of trust between the Endpoint Policy Server and the Endpoint Security Management server.
c) If the trust is not created, click Test SIC Status to see what you must do to create the trust successfully.
d) If you have to reset the SIC, click Reset, reset the SIC on the Secondary or Policy Server (“Troubleshooting SIC Trust” on page 21) and then click Initialize.
e) Click Close.

8. Click OK.
9. If prompted, click Save. Otherwise, select File > Install Policies.

To complete the Endpoint Policy Server configuration in SmartEndpoint:
1. In SmartEndpoint, select Manage > General Properties.
2. Double-click the Endpoint Security Management server object.
3. In the object properties window, click Install Database. This establishes communication with the Endpoint Policy Server.
4. After the installation process completes click Close in the Install Database window.
5. Click OK.
6. If a High Availability Secondary server exists, perform step 1-4 on the Secondary server object also.
7. Open the Endpoint Policy Server object created with the previous procedure.
8. In the object properties window, click Install Database.
   This step establishes communication with the Endpoint Security Management server and lets the Endpoint Policy Server collect logs.
9. After the installation process completes click Close in the Install Database window.
10. Click OK.
11. Click OK.
12. Click Save.
13. If you see an Enforce Changes message that prompts you to save the changes, click Save & Install.
14. If you did not click Save & Install, select File > Install Policies.

The Endpoint Policy Server synchronizes with the Endpoint Security Management server after the policy and databases are installed. This can take a long time based on the quantity of policies and installation packages.

Troubleshooting SIC Trust

If you cannot successfully create SIC trust on a server, it might be necessary to reset SIC on a peer server.

To reset SIC on an Endpoint Policy Server:
1. In the CLI of the server, run cpconfig.
   The Check Point Configuration Tool opens.
2. Select the Secure Internal Communication tab.
3. Click Reset.
4. Click Yes.
5. Enter an Activation key and confirm it.

If you cannot create a state of trust between the Endpoint Security Management server and Endpoint Policy Server and get this message:

SIC Status for CP: Unknown
Could not establish TCP connection with <Policy Server IP address>
- Make sure that the CPD process is running on the Endpoint Policy Server and that TCP connectivity is allowed from the Security Management Server to the IP address of the Endpoint Policy Server on port 18191.
- Make sure that the Windows Server firewall on the Endpoint Security Management server does not drop Check Point communication.
Chapter 5

Installing Endpoint Security Management Servers for High Availability

In This Chapter
- Installing on Windows 23
- Installing on Gaia 24
- Installing on SecurePlatform 24
- Secondary Server Configuration 24

You can install one or more additional Endpoint Security Management servers for High Availability. Servers used for High Availability must have the same Operating System version and the same system architecture (either 32-bit or 64-bit).

If you have a primary Endpoint Security Management server that was originally installed with R80, R80.10, or E80.20 EA, before you install a secondary server you must Uninstall the Edge Compatibility package from the primary Endpoint Security Management server.

Installing on Windows

To install more Endpoint Security Management servers for High Availability on Windows:

1. Log in to Windows using Administrator credentials.
2. Put the installation media in the drive.
   - The installation wizard starts automatically.
   - Click Next.
3. Accept the License Agreement
   - Click Next.
4. Select New installation
5. Click Next.
6. Select Custom and click Next.
7. Select Endpoint Security and click Next.
8. Optional: In the Destination Folder page, click Browse to select a different folder for the installation
9. Click Next.
    - The products that will install show on the screen.
11. Click Next to start the installation.
    - When the installation is complete, the wizard continues with initial configuration.
To continue the installation wizard:
1. In the Licenses and Contract page, click Next to use the Trial Period license. A new license is not necessary.
2. In the Secure Internal Communication page, enter and confirm a Secure Internal Communication (SIC) Activation Key and click Next.
3. Click Finish.
4. Click OK to restart the computer.

Note - You can connect to a Secondary Endpoint Security Management server, but only in the Read Only mode.

Installing on Gaia

To install more Endpoint Security Management servers for High Availability on Gaia:
1. Install Gaia ("Installing Gaia" on page 13).
2. Do the procedure in Using the Gaia First Time Configuration Wizard (on page 14) with this change:
   In the step where you select Security Management, you must also select Secondary.
   - Enter and confirm the SIC information when prompted.
   - Do not define administrators, client IP addresses, certificate authority or save the fingerprint. This information is automatically imported from the primary Endpoint Security Management server.
3. Do the procedure in Installing the E80.40 Endpoint Security Overlay (on page 14).

Note - You can connect to a Secondary Endpoint Security Management server, but only in the Read Only mode.

Installing on SecurePlatform

To install more Endpoint Security Management servers for High Availability on SecurePlatform:
1. Install SecurePlatform ("Installing SecurePlatform" on page 15).
2. Do the procedure in Installing an R75.40 Security Management Server (on page 16) with this change:
   - Enter and confirm the SIC information when prompted.
   - Do not define administrators, client IP addresses, certificate authority or save the fingerprint. This information is automatically imported from the primary Endpoint Security Management server.
3. Do the procedure in Installing the E80.40 Endpoint Security Overlay (on page 14).

Note - You can connect to a Secondary Endpoint Security Management server, but only in the Read Only mode.

Secondary Server Configuration

In the SmartDashboard connected to the Primary server, you create a network object to represent the Secondary Security Management Server. You then synchronize the Primary and Secondary Security Management Servers.

To configure the secondary server in SmartDashboard:
1. Open SmartDashboard.
2. In the Network Objects tree, right-click Check Point and select Host.
3. In the Check Point Host window, enter a unique name and IP address for the server.
4. In the Software Blades section, select the Management tab.
   This automatically selects the Secondary Server, Logging and Status, and Provisioning options.
   a) Enter and confirm the SIC Activation Key that you entered in the Check Point Configuration Tool.
   b) Click Initialize to create a state of trust between the Endpoint Policy Server and the Endpoint Security Management server.
   c) If the trust is not created, click Test SIC Status to see what you must do to create the trust successfully.
   d) If you have to reset the SIC, click Reset, reset the SIC on the Secondary or Policy Server ("Troubleshooting SIC Trust" on page 21) and then click Initialize.
   e) Click Close.
7. Click OK.
8. Select File > Save.

To do the first synchronization:
2. Manually copy new MSI files from the Active Endpoint Security Management server to the Standby Endpoint Security Management server:
   a) On the Active Endpoint Security Management server, copy these folders:
      On Windows Platforms: %fwdir%\conf\SMC_Files\uepm\MSI
      On SecurePlatform or Gaia: $FWDIR/conf/SMC_Files/uepm/msi
   b) On the Standby Endpoint Security Management server, replace these folders with the folders that you copied from the Active Endpoint Security Management server:
      On Windows Platforms: %fwdir%\conf\SMC_Files\uepm\MSI
      On SecurePlatform or Gaia: $FWDIR/conf/SMC_Files/uepm/msi
   c) On Linux machines, run:
      (i) cd $FWDIR/conf/SMC_Files/uepm
      (ii) chmod -R u+rw,x,g+rw,x,o-rwx msi/ -
      (iii) find msi/ -type d -exec chmod g+s {} \;
3. Open SmartEndpoint that is connected to the Primary Security Management Server and select File > Install Policies.
4. Select the General Properties policy and click Install.
   The servers automatically synchronize again according to the settings configured in SmartDashboard, including the sync schedule. If you configured the manual synchronization settings in SmartDashboard, you must synchronize manually.

   Note - While the synchronization takes place, SmartDashboard shows Not Responding.

You can use the SmartDashboard and SmartEndpoint on the secondary server in Read Only mode.
In This Chapter

Configuring the Apache Cache ........................................... 26
Users Created at Installation ............................................. 27

Configuring the Apache Cache

By default, the size of the apache cache is set to 5GB. After installing the Endpoint Security Management Server, it can be necessary to adjust the cache to a size more applicable to your hardware.

For cleaning and controlling the size of the cache directory, Apache supplies the executable tool: htcacheclean. Endpoint Security Management Server uses cpd (the Check Point daemon) to schedule htcacheclean to run at specified intervals. When running, htcacheclean:

- Checks the cache directories at regular intervals for removable content
- Controls the cache size.

Using the cpd scheduler configuration tool you can:

- View Scheduled tasks
- Change the task status
- Schedule new tasks

Viewing Scheduled Tasks

The default disk clean-up task scheduled during installation of the Endpoint Security Management Server is called ApacheCacheClean. To see the task and its parameters, run:

```
# cpd_sched_config print
```

The same data is available in the Windows registry under:

HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\CPShared\<version_number>\reserved\CPD_Scheduler\ApacheCacheClean

Changing the Clean-up Task Status

1. To stop the cache clean-up, run:

```
# cpd_sched_config deactivate ApacheCacheClean -r
```

2. To start the cache clean-up, run:

```
# cpd_sched_config activate ApacheCacheClean -r
```

**Note** - The activate and deactivate commands refer to the scheduler's timer. Deactivate suspends the timer. Activate restarts the timer. Restarting the timer does not immediately invoke htcacheclean. The scheduler runs htcacheclean only after the specified time interval.

3. To delete the clean-up task, run:

```
# cpd_sched_config delete ApacheCacheClean -r
```

**Note** - The -r flag applies the update immediately.
**Scheduling a New Clean-up**

To schedule a new clean-up task, use the `add` flag.

For example, if disk cache clean-up must occur each hour (3600 seconds) and the cache directory size stay below 100MB, run:

```bash
# cpd_sched_config add NewApacheCacheClean -c "C:\Program Files\CheckPoint\CPuem\E80.40\apache22\bin\htcacheclean.exe" -v -nt -p "C:\Program Files\CheckPoint\CPuem\E80.40\apache22\cache" -l100M -e 3600 -r
```

After one hour, the cpd scheduler runs the new task.

*Note* - Make sure to wrap the paths with double quotes exactly as shown in the example.

**Users Created at Installation**

During the server installation, a local user account (CPEP$USER) is created automatically. The account has:

- Special privileges to run Endpoint Security Management Server services.
- A predefined password that you cannot change.
- The Endpoint Security $user is not authorized to log into the system.
Chapter 7

Upgrading the Endpoint Security Management Server

In This Chapter

Upgrading on a Windows Endpoint Security Management Server 28
Upgrading Secondary and Policy Servers 29
Migrating to a Different Platform 29
Directory Scanner Issues 32

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 E80.3X. See the E80.3X 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.

When you upgrade to E80.40, you must first upgrade your Endpoint Security Management servers and Endpoint Policy Servers. Then you can upgrade your existing clients and add new clients.

Note - New Endpoint Security client packages and logs are automatically installed in the server repository during the upgrade procedure.

Upgrade workflow:
2. Upgrade the E80.3X Endpoint Security Management server to E80.40 ("Upgrading on a Windows Endpoint Security Management Server" on page 28)
3. Optional: Migrate ("Migrating to a Different Platform" on page 29) to the Endpoint Security Management server to a Gaia or SecurePlatform platform.
4. Install the E80.40 SmartConsole applications ("Installing E80.40 SmartConsole" on page 16).

Upgrading on a Windows Endpoint Security Management Server

To upgrade an E80.3X Endpoint Security Management server to E80.40:
3. Run UepmPolicyExport.msi on the E80.3x Endpoint Security Management server. This utility exports the policy database from E80.3X.
   
   Important - If installing from a CD, do not let auto run start the E80.40 installation program.

4. The utility installs itself and runs automatically.
5. Log in and do the instructions on the screen.
6. Run Setup.exe from the E80.40 distribution media.
7. When prompted, reboot the computer.
Upgrading the Endpoint Security Management Server

8. On the Endpoint Security Management server, go to the installation folder of the SmartEndpoint. By default this is C:\Program Files (x86 on 64 bit computers)\CheckPoint\SmartConsole\E80.40\PROGRAM\.
9. Run EPUpgradeImportTool.exe.
10. Log in and do the instructions on the screen.

Upgrading Secondary and Policy Servers

The basic procedure for upgrading Secondary or Endpoint Policy Servers is the same as for the Primary (Active) server, except that import and export are not necessary.

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 R75.40. 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.

Migrating to a Different Platform

The current Endpoint Security Management server release includes migration tools that support cross-platform migration between Windows, Gaia, and SecurePlatform. You can also migrate to a different computer with the same operating system. The migration tools let you export the Endpoint Security databases and configuration files from the source computer and import them to the destination computer.

Important - The source and destination computers must have the same IP address. See sk65451 http://supportcontent.checkpoint.com/solutions?id=sk65451 for how to change the server's IP.

You can migrate between computers with different operating systems and also between 32 bit and 64 bit computers.

In this case, The migration tool imports copies of the two files to the apache22/conf folder with the .migrateBkp extension. Manually change the contents of the existing files on the destination computer as necessary.

To migrate an Endpoint Security Management server to a different platform:
2. Export (“Exporting the Databases and Configuration Files” on page 30) the Endpoint Security Management server databases and configuration files from the source computer.
3. Import (“Importing the Databases and Configuration Files” on page 30) the Endpoint Security Management server databases and configuration files to the destination computer.
Exporting the Databases and Configuration Files

To export the databases and configuration files:
1. Run cpstop.
2. Go to the location on the source computer:
   - Windows - %fwdir%\bin\upgrade_tool
   - Gaia or SecurePlatform - $FWDIR/bin/upgrade_tools
3. Run the command for the source computer operating system:
   - Windows - migrate export --include-uepm-msi-files <path>
   - Gaia or SecurePlatform ./migrate export --include-uepm-msi-files <path> <path>
   The --include-uepm-msi-files argument adds the client installation Packages Repository (.msi files) to the exported TGZ file.
   <path> is the path and file name of the export TGZ file.
4. Run the command to get the PAT version:
   - Windows - uepm patver get
   - Gaia or SecurePlatform - ./uepm patver get
   Save the PAT version information shown by this command for use during the import procedure.
   Note - Exporting and importing the client installation Packages Repository can take a long time for a large organization and generate a large export file. A faster, but more complex, alternative, is to manually copy the Packages Repository ("Migrating the Packages Repository - Manual" on page 31) from the source to the target computer.
   If you use the manual procedure, do not use the --include-uepm-msi-files argument in step 4.

Importing the Databases and Configuration Files

To import the databases and configuration files:
1. Copy the exported TGZ file to the destination computer.
2. Go to this location on the destination computer:
   - Windows - %fwdir%\bin\upgrade_tools
   - SecurePlatform or Gaia - $FWDIR/bin/upgrade_tools
3. Run the command for the destination computer operating system.
   - Windows - migrate import --include-uepm-msi-files <path>
   - SecurePlatform or Gaia - ./migrate import--include-uepm-msi-files <path>
   The --include-uepm-msi-files argument imports the client installation Packages Repository (.msi files) from the exported TGZ file.
   <path> is the path and file name of the exported TGZ file.
   Note - If you used manual MSI copy procedure, do not use the --include-uepm-msi-files argument in step 3.
4. If you have manually customized ssl.conf and/or httpd.conf files and
   - The source and target computers have different operating systems
   Or
   - The $FWDIR path or $UEPMDIR path are different on the source and target computers
Do these steps:

a) Go to \$UEPMDIR/apache22/conf (\%UEPMDIR\%\apache22\conf on windows).

b) Manually merge the ssl.conf.migrateBkp and httpd.conf.migrateBkp files from the source computer with those on the destination computer.

This step lets you keep your manual customizations after the upgrade and migration.

To restore the source computer PAT version:
1. Go to \$UEPMDIR/bin (\%UEPMDIR\%\bin in windows).
2. Run these commands as applicable for your operation system.
   - **Linux:** /opt/uepm patver set <Source PAT + 10>
   - **Windows:** uepm patver set <Source PAT + 10>
   
   <Source PAT + 10>: This argument is the source PAT version saved from the export procedure ("Exporting the Databases and Configuration Files" on page 30) + 10.
   
   For example, if the source PAT version is 5, use the value 15 in step 2.
3. Run cprestart on the destination computer.

Migrating the Packages Repository - Manual

You can use this procedure to manually copy the client installation Packages Repository from the source to the target computer. This procedure requires less free disk space on the source and target machines. We recommend this procedure because it is faster for large organizations with many installation packages in the repository.

To manually copy the Packages Repository to a Windows destination computer:
1. Go to \%FWDIR\%conf\SMC_Files\uepm (\%FWDIR\%conf\SMC_Files\uepm on a SecurePlatform or Gaia computer).
2. Rename the msi folder to msiOLD.
3. Copy the msi folder from the source computer to \%FWDIR\%conf\SMC_Files\uepm on the destination computer.

To manually copy the Packages Repository to a SecurePlatform or Gaia destination computer:
1. Go to $FWDIR/conf/SRC_Addr/uepm ($FWDIR/conf/SRC_Addr/uepm on SecurePlatform or Gaia).
2. Rename the msi folder to msiOLD.
3. Copy the MSI folder from the source computer:
   - $FWDIR/conf/SRC_Addr/uepm from SecurePlatform or Gaia.
   - $FWDIR/conf/SRC_Addr/uepm when the source machine is a Windows computer to $FWDIR/conf/SRC_Addr/uepm on the destination computer.
4. Run these commands on the destination computer:
   - cd $FWDIR/conf/SRC_Addr/uepm
   - chmod -R u+rw,g+rw,o=rwx msi/
   - find msi/ -type d -exec chmod g+s {} \;

To automatically copy the Packages Repository:

Add this argument to the migrate export and migrate import commands:

--include-uepm-msi-files backup.tgz

For example:
migrate export --include-uepm-msi-files backup.tgz
migrate import --include-uepm-msi-files backup.tgz
Directory Scanner Issues

This section includes some issues that have an effect on Directory Scanner instances. When you upgrade to E80.40, the previous version Directory Scanner instances are copied to the E80.40 database with necessary changes. The Directory Scanner instance is automatically disabled and the Request for rescan option is set to True.

When you use the Directory Scanner for the first time after the upgrade, you are prompted to define the credentials for each instance. After you enable your instances, it does a full scan (rescan) of the AD instead of scanning for incremental changes. This can take a long time depending on the AD population size.
Chapter 8

Upgrading Endpoint Security Clients

In This Chapter

- Upgrading Clients to E80.40
- Upgrading Legacy Clients
- Uninstalling the Endpoint Security Client

Upgrading Clients to E80.40

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.

**Client Upgrade workflow:**

1. For E80.20 and earlier Endpoint Security Clients with legacy (pre R80) VPN clients, remove all Firewall related blades. Do this before the upgrade.
2. Make sure that the clients are connected to an E80.40 Endpoint Security Management server.
3. Deploy the Software Blade Packages to clients with Software Deployment Rules or by exporting packages.

**Notes and Cautions - Windows**

When upgrading to a Windows computer, be aware of these limitations:

- All packages are installed on the C drive.
- The required space on drive C is:
  
  Log files size (%fwdir%\log) + Conf files size (%fwdir\conf) + 4 GB

  - %fwdir%\log contains server and client logs.
    Log file size varies for different environments.
  - %fwdir%\conf contains server configuration and client packages.
    Client .msi files are very large.

**Upgrading with Deployment Rules**

The Common Client Settings Policy controls if users can postpone an upgrade installation or if the upgrade is installed on clients immediately. You can configure the settings in the Client Settings Policy. Edit the Default installation and upgrade settings.

To upgrade clients with Software Deployment Assignments:

1. In the Deployment tab, select a rule and change its Endpoint Client Version in the Client Version column.
   All computers are assigned to that Policy rule will be upgraded.
2. Optional: Change who the rule applies to in the Applies To column.
3. Select File > Save or click the Save icon.
4. Select File > Install Policies or click the Install Policies icon.
5. The Endpoint Agent on each assigned client downloads the new package. The client installation starts based on the settings in the Common Client Settings policy rule. You can configure:
   - If the Common Client Settings policy forces installation and automatically restarts without user notification.
   - If the Endpoint Agent sends a message to the user that an installation is ready and gives the user a chance to postpone the installation or save work and install immediately.
6. The Endpoint Agent installs the new client.
   If the user does not click Install now, installation starts automatically after a timeout.
7. After installation, the Endpoint Agent reboots the computer.

**Upgrading with an Exported Package**

Upgrade a client to a new package that includes the same blades as it has now. Add and remove blades after the upgraded package is installed.

To upgrade clients with an exported package:
1. In the Deployment tab, select Packages for Export from the tree.
2. Click Add to add a new package or select a package from the list.
3. Edit the Version and Blades to make them correct for your environment.
4. Select File > Save.
5. Click Export Package.
   The Export Package window opens.
6. In the Export Package window:
   a) Select the platform versions (32/64 bit) to export for laptops and desktops.
   b) Enter or browse to a destination folder.
7. Click OK.
   The package EPS.msi and/or PreUpgrade.exe files are downloaded to the specified path. A different folder is automatically created for each option selected in step 3a.
8. Send the EPS.msi and PreUpgrade.exe files to endpoint users. Endpoint users manually install the packages. They must use Administrator privileges.
   You can also use third party deployment software, a shared network path, email, or some other method.

**Gradual Upgrade**

To upgrade more gradually, you can create a new rule and distribute it only to specified computers.

Note - For an exported package, save the new package in a different location than the previous package.

When you are prepared to upgrade all clients, upgrade all rules.

**Upgrading Legacy Clients**

See the Endpoint Security Release Notes (http://supportcontent.checkpoint.com/solutions?id=sk82100) for the supported upgrade paths for this version. Legacy clients are those earlier than version R80. You must enter password information to upgrade legacy Secure Access and Full Disk Encryption.

**Offline Upgrades**

During an offline upgrade, the endpoint has no connection with the Endpoint Security Management server. For this reason, the Preupgrade.exe package delivered to the client must contain:

- All the passwords necessary to successfully uninstall legacy products
- The new E80.40 client with the necessary blades and policies
Offline upgrades use the `Preupgrade.exe` file, which is automatically created in the same directory as the MSI package.

**To create an offline upgrade package:**
1. On **Deployment** tab, select **Packages for Export** from the tree.
2. Click **Add**.
   A new package shows in the list.
3. Optional: Change the package **Name** and **Version**.
4. In the **Settings** column, select **Support client preinstall upgrade**.
5. Under **Support client preinstall upgrade**, make these selections as necessary:
   a) **Silent Mode** - Choose if silent mode is active. When active, the procedure tool runs silently without user intervention. If silent mode is not active, users can see the GUI of the Upgrade tool. If silent mode is active, select what happens after the upgrade:
      ▪ Force restart after upgrade.
      ▪ Prompt user to restart after upgrade.
   b) **Secure Access upgrade** - To enable a Secure Access upgrade you must enter the uninstallation password. Click on **Legacy Secure Access upgrade not supported** and select **Configure Upgrade Password**.
      In the **Legacy Secure Access Upgrade** window, select **Support Legacy upgrade** and enter and confirm the uninstallation password.
   c) **Legacy Full Disk Encryption upgrade** - To enable an upgrade from legacy Full Disk Encryption EW, you must enter the uninstallation password. Click on **Legacy Full Disk Encryption EW upgrade not supported** and select **Configure Upgrade Password**.
      In the **Legacy Full Disk Encryption EW** window, select **Support Legacy upgrade** and enter and confirm the uninstallation password.
6. Make sure the blades in the **Desktop Blades** and **Laptop Blades** columns are correct.
7. Optional: In the **Settings** column, add a Virtual Groups destination for the package. Click **Do not export to Virtual Groups** and select **New**.
8. Select **File > Save**.
9. Select the package and click **Export Package**.
10. In the **Export Package** window:
    a) Select the platform versions (32/64 bit) to export for laptops and desktops.
    b) Enter or browse to a destination folder.
11. Click **OK**.
    The `PreUpgrade.exe` files are downloaded to the specified path.
12. Send the `PreUpgrade.exe` files to endpoint users. Endpoint users manually install the packages. They must use Administrator privileges.
    You can also use third party deployment software, a shared network path, email, or some other method.

**To install the offline upgrade, users must:**
1. Double-click `Preupgrade.exe`.
2. Follow the on-screen instructions to install the package.

**Online Upgrades**

During an online upgrade the endpoint has a connection to the server. When the initial client is installed, it connects to the server. The initial client uses the **Common Client Settings** that contains uninstall passwords for legacy products.

**To create a package for an Online upgrade:**
1. In the **Policy** tab > **Client Settings** section, and right-click **Default installation and upgrade settings**.
2. Click **Edit Properties**.
   The **Installation** window opens.
3. Click **Legacy Client Uninstall Password**.
4. Enter uninstall passwords for:
   • Legacy Secure Access
   • Legacy FDE EW
5. Click OK.
7. Click Add.
8. Add a package with Initial Client Only, with the version you require.
9. Click Export Package.
10. In the Export Package window:
    a) Select the platform versions (32/64 bit) to export for laptops and desktops.
    b) Enter or browse to a destination folder.
11. Click OK.
    The package EPS.msi files are downloaded to the specified path.
12. Send the EPS.msi to endpoint users. Endpoint users manually install the packages. They must use Administrator privileges.
    You can also use third party deployment software, a shared network path, email, or some other method.
After the EPS.msi is installed, you can add a package with Endpoint Security Software Blades. See Upgrading with Deployment Rules (on page 33).

Uninstalling the Endpoint Security Client

To uninstall the Endpoint Security client:
1. Make sure that the original EPS.msi and PreUpgrade.exe files are present on the endpoint computer.
2. If you are using Windows 7 or Vista, disable User Account Control (UAC).
3. Go to Control Panel > Programs and Features > Uninstall or change a program.
5. If the client has Full Disk Encryption installed, run the Uninstall or change a program applet again after the disk completes the decryption.

Upgrading Media Encryption R73.x Devices and Keys

This version includes a wizard that lets you export Media Encryption devices from the R73.x database and import them into an E80.40 Endpoint Security Management server. When upgrading from Media Encryption R73 to the current version:
• We recommend that you add the UUID of the R73 server to the trusted list.
• You can access devices that were encrypted on the R73 Media Encryption server automatically, if you export the devices and keys from the R73 database and import them in to the Endpoint Security Management Server.

Important: Encryption keys associated with Active Directory users that were not added to the Media Encryption (Protector) server manually or through group synchronization, will not be migrated.

Media Encryption (Protector) Encryption Keys and Devices are stored in the MS-SQL database. The Protector Server connects to MS-SQL through named pipelines. To migrate Media Encryption keys and devices, you must configure MS-SQL to accept requests over TCP connections. You must create a login profile that has the permissions required to access the Disknet database.
• If the Protector Server is installed with default settings, use the instructions here.
• If the MS-SQL is installed on an external machine, or MS-SQL management tools are installed, consult with your DBA, and skip to the Running Migration Tools section.

To configure the MS-SQL server to accept requests over TCP connections:
1. In the regedit tool, find the "SuperSocketNetLib" key.
   The path to this key can be different according to the platform and installed tools.
2. Right-click the "SuperSocketNetLib" entry and export it for backup.
3. Create a reg file to customize the server:
   If the path to the SuperSocketNetLib entry is the same in the Media Encryption (Protector) server and in this article:
   a) Copy this registry fragment to a separate file.
   b) Save it with the "reg" extension, and run it.
   If the path is different, edit the new reg file so that it fits the path on the machine.

   Windows Registry Editor Version 5.00
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\MSSQLServer]
   "LoginMode"=dword:00000002
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\SuperSocketNetLib]
   "ProtocolList"=hex(7):74,00,63,00,70,00,00,00,6e,00,70,00,00,00,00,00
   "TcpPort"="1433"
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\SuperSocketNetLib\Tcp]
   "TcpHideFlag"=dword:00000000
   "TcpDynamicPorts"=""
   "TcpPort"="1433"
   "Enabled"=dword:00000001

4. When the registry edit is done, open the regedit utility.
5. Make sure that the "reg" script ran successfully and that the values in the registry were changed according to the script.
6. Restart the "MSSQLSERVER" process.

To add a new login profile to the MS-SQL server:
1. Run the osql tool from the command line: osql -E
2. Run these commands in the osql command line:
   EXEC sp_addlogin 'ep','ep'
   GO
   EXEC sp_grantdbaccess 'ep', 'Disknet'
   GO
   EXEC sp_addsrvrolemember 'ep', 'sysadmin'
   GO

To run the Migration Wizard:
1. Make sure that Media Encryption & Port Protection and the Endpoint Security server are up and running.
   **Important**! This is required to complete the key migration successfully.
3. Open the SmartEndpoint console.
4. Click **Tools** menu > **Devices and Keys Migration Tool**.
5. Enter the details of the Media Encryption R73 Database: IP address or server name, Database Username, Database Password, Database Name.
6. Click **Next**.
7. Select **Import Devices** or **Import Keys** or both.
8. Click **Next**.
See the import results. When import is done, users can access the media from computers with Endpoint Security client installed.

**Important!** Users must access the media at least once to enable Remote Help Key Recovery.

More details can be found in `deviceMigrtor.log` file, which is located in the same folder as the `SmartEndpoint.exe` executable. To go to this folder, right-click the **SmartEndpoint** icon and select **Properties > Open File Location.**