© 2012 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page (http://www.checkpoint.com/copyright.html) for a list of our trademarks.

Refer to the Third Party copyright notices (http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.
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=17163
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 September 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
Chapter 1

Introduction to Endpoint Security

In This Chapter

- Getting Started ................................................. 6
- Using the Client .................................................. 8
- Responding to Alerts ........................................... 12
- Uninstalling the Endpoint Security Client ................. 14

Check Point Endpoint Security™ is the first and only client with all essential components for total security on the endpoint: Compliance, Anti-Malware, Media Encryption and Port Protection, Firewall and Application Control, Full Disk Encryption, WebCheck, and Remote Access VPN.

Check Point Endpoint Security protects your computer without having to install and manage multiple agents.

Getting Started

Endpoint Security is managed by an Endpoint Security Management Server that is controlled by an administrator. The administrator creates the Endpoint Security policy that your client uses to protect your computer.

The exact instructions to install the Endpoint Security client depend on your administrator.

Here are some items that are referenced in the instructions below:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Endpoint Security icon in your taskbar notification area.</td>
</tr>
<tr>
<td>192.0.2.10</td>
<td>An example of an IP address that the administrator can ask you to connect to.</td>
</tr>
</tbody>
</table>

Making Sure that the Client is Installed

Your administrator can install the Endpoint Security client for you. If you do not know if you already have the Endpoint Security client installed, check your Endpoint Security status.

To see Endpoint Security status:

1. Right-click the Endpoint Security icon in your taskbar notification area and select Display Overview. The Endpoint Security Main Page opens.

   Note - If you do not see the Endpoint Security client icon in your taskbar notification area, it could be hidden. Configure your taskbar to show the hidden Endpoint Security client icon. If you still do not see the Endpoint Security icon, it is likely that the Endpoint Security client failed to install correctly.

2. Look at your status in the Endpoint Security Main Page.
   - If it shows that you are Connected, your client is properly installed and you do not have to do anything.
   - If you cannot connect successfully, contact your administrator.
**Getting the Endpoint Security Installation**

If an Endpoint Security Installation window opens, do the on-screen instructions to continue the installation ("Installing and Upgrading the Client" on page 7).

If an Endpoint Security Installation window does not open, do this procedure to get the installation. The exact steps depend on the choices made by your administrator.

**Note** - You must have administrator rights on your computer to install the client. For Windows 7 and Vista computers with UAC enabled, you must also run the package using the Run as Administrator option. Consult with your system administrator.

To get the Endpoint Security client installation:

1. Double-click the installation package that your administrator sent you.
   - The Endpoint Security icon appears in your taskbar notification area, if it was not there already.
2. If you are not connected, right-click the taskbar notification area icon, and select Connect.
3. If the window that opens shows Welcome, click Next.
   - In the window shows Server address or Name, enter the IP address or computer name (usually it looks like this: name.domain.com:443)
4. If a window with a fingerprint opens, click Approve.
5. If you are asked to download and install the client package, click the button to do this.
6. Do the on-screen instructions to complete the installation and restart your computer.

**Installing and Upgrading the Client**

**Important** - Do NOT restart the computer during installation. Wait until the upgrade completes.

The client automatically gets updates from the server on a schedule. You can also update manually at any time. To do this, click Update Now from the Endpoint Security Main Page or the icon tray. During updates your computer might be slower than usual.

This update gets policies that changed after the last update. Policies that did not change are not downloaded.

To install or upgrade your Endpoint Security client:

1. When the Endpoint Security Installation window opens, click Install or Postpone.
   - The Postpone option is not always available. If you click Postpone, installation is delayed until the Endpoint Security has resumed installation window opens. You must click OK to continue.
   - If you do not click Install, installation starts automatically at the specified time.
2. Wait for the Endpoint Security Client to install.
3. When the Endpoint Security Client installation is complete message window shows, click Restart to restart the computer immediately.
   - If you do not click Restart, your computer will restart automatically after 90 seconds.
Using the Client

Use the **Endpoint Security Main Page** and the taskbar notification area icon to see all the information related to Endpoint Security.

**Tour of the Endpoint Security Main Page**

The Endpoint Security Main Page provides one-stop access to the security features that keep your computer safe.

To launch the Endpoint Security Main Page, select **Display Overview** from the Endpoint Security system tray menu. You see the Software Blades that your administrator defined for you. (You might not see all of the Software Blades described here.)

- Click a Software Blade to see details and available options.
- The top section shows if everything is compliant and updated, or if you have alerts, status issues, or actions to do.

**Compliance Blade**

Compliance enables Endpoint Security client to protect your enterprise network from Internet threats. Compliance enforces a security policy created by your administrator.

The status shows if you are compliant with the corporate security policy. Status can be:

- **Compliant** - Your computer has the required software and approved versions.
- **Warn** - Your computer is not compliant with the enterprise security requirements. You can access your enterprise network, but you must do the actions shown to become compliant.
- **About to be restricted** - Your computer is not compliant with the enterprise security requirements. Your access to the enterprise network will be restricted if you do not do the actions shown to become compliant within the specified time.
- **Restricted** - Your computer is not compliant with the enterprise security requirements. Your access to the corporate network is restricted. Do the actions shown to become compliant.

Click the **Compliance Blade** to see more about:
• **Policy Details** - A summary of the Compliance policy that is installed on your computer.

• **Current Status** - If your computer has Compliance policy violations. A **Message** tells you about each problem and gives recommended remedies.

You can also run the **Security Analysis Report** from this tab.

**To correct compliance violations:**

• Select a compliance violation message and click **Fix it** to correct the selected violation.

• Click **Try Fix All** to try to correct all listed compliance violations.

If these actions do not resolve the violations, contact your help desk or system administrator.

**Anti-Malware Blade**

Malware includes viruses, spyware, and other malicious software. Anti-Malware scans automatically detect malware on your computer and make them harmless before they can cause damage. The display shows the Anti-Malware policy and if any items are quarantined to protect your computer.

Click **Anti-Malware Blade** to see options:

• **Policy Details** - A summary of the Anti-Malware policy that is installed on your computer.

  Click **Selected** to see the files and paths that are excluded from these scans and explanatory notes.

• **Current Status** - A summary of the Anti-Malware status of your computer. If the status shows that the Anti-Malware signatures are out of date, click **Update Now** under the **Tools** menu.

  • Click **Quarantine** to see files that have been quarantined. In some cases, items detected during an Anti-Malware scan cannot be treated or removed automatically. These items are usually placed into quarantine so that they become harmless but preserved so that they can be treated in the future.

  The **Quarantine** window displays information about each file:

  ▪ **Infection** - Name of the malware
  ▪ **Type** - The type of malware
  ▪ **Risk** - The risk level of the infection
  ▪ **Path** - The original location of the malware on your computer.
  ▪ **Days in Quarantine** - Number of days the file has been in quarantine.

  • See the history of when scans and updates occurred and when they are scheduled to run again.

• **Scan Now** - Click to start an Anti-Malware scan immediately.

**Media Encryption and Port Protection Blade**

The Media Encryption and Port Protection policy determines how you can use external devices that connect to your computer. Media Encryption and Port Protection can scan (for malware), encrypt, and decrypt external devices. The display shows the status of external devices connected to your computer.

Click **Media Encryption and Port Protection Blade** to see options:

• **Policy Details** - A summary of the Media Encryption and Port Protection policy that is installed on your computer.

• **Detected Removable Devices** - Shows the status of devices attached to your computer. It includes these details:

  ▪ **Device** - The type of device and the drive it is connected to.
  ▪ **Size** - The amount of storage space on the device.
  ▪ **Authorization Status** - The authorization status of the device based on an Anti-Malware scan.

    ▪ **Authorized** - Clean from malware.
    ▪ **Not Authorized** - Malware or suspicious files were found. You cannot open, encrypt, or decrypt a device that is not authorized.
    ▪ **Waiting for scan** - The device was not scanned.
  ▪ **Encryption Status** - If the device is encrypted or not. Only someone with permissions can view files on an encrypted device.
• **Scan Device** - Scans the device for malware or unauthorized files. If your Endpoint Security client does not have the Anti-Malware Blade installed, the scan can still look for unauthorized files.

• **Create Encrypted Storage** - Click this to create an encrypted storage device.

• **Remove Encryption** - Click this to remove encryption from a device.

If you have the applicable permissions, you can encrypt devices (see "Encrypting Media" on page 19) and access encrypted devices on a computer without Media Encryption and Port Protection ("Accessing Encrypted Storage Device" on page 21).

**Firewall and Application Control Blades**

Firewall and Application Control is your front line of defense against Internet threats. The display shows the status of your firewall and the number of attempted connections and programs that the firewall has blocked.

Click **Firewall and Application Control** to see the options:

• **Policy Details** - A summary of the Firewall and Application Control policies that are installed on your computer.

• **Current Status** - Shows a summary of the firewall and Application Control activity. The List of blocked programs shows details of programs that were blocked.

**Full Disk Encryption Blade**

Full Disk Encryption ensures that only authorized users can access desktops and laptops. If you have the Full Disk Encryption blade installed as part of Endpoint Security, enter a password to start your computer. Until you are authenticated, all information on the computer is encrypted.

Click **Full Disk Encryption Blade** to see options:

• **Policy Details** - Details of the Full Disk Encryption and OneCheck User Settings policies that are installed on your computer.

• **Encryption Status** - Shows the encryption status of components and drives on your computer. It also shows the size, encryption algorithm, and available space for each device.

• **Advanced** - Shows more details for the different parts of your Full Disk Encryption account.

**WebCheck Blade**

WebCheck adds a layer of protection against Web-based threats to the Endpoint Security Anti-Malware and firewall functionality, which protect against PC-based threats.

Click **WebCheck Blade** to see this information:

• **Policy Details** - A summary of the WebCheck policy that is installed on your computer.

• **Trusted Domains** - Domains or sites that your administrator defined as trusted. They are not checked by WebCheck.

• **Current Status** - Shows statistics for WebCheck activities including website blocked and threats stopped.

• **Troubleshooting** - Click **Clear WebCheck Cache** to delete the browser cache of WebCheck visited sites.

**Remote Access VPN Blade**

Endpoint Security VPN (Virtual Private Network) lets you connect securely to your enterprise network when you work from a remote site.

Click **Remote Access VPN Blade** to see options:

• **Connection Status** - The status of the VPN connection:
  • **Duration** - How long it has been connected.
  • **Expiration** - When the authentication expires.

• **Connection Details** - Network details:
- **Site Name** - The site (or VPN gateway) that the client connects to.
- **Gateway IP Address** - The IP address of the VPN site.
- **Last time connected** - If you are not connected to a VPN, the time of your last connection shows. If you are currently connected, this information does not show.
- **Encryption Details** - Shows the quantity of packets and the total KBs that were decrypted and encrypted during the connection.
- **Connect to** - Click to select which VPN to connect to and to enter authentication information.
- **Connect** - Click to connect to the default VPN site.

**Tools**

The **Tools** menu is on the left of the Endpoint Security Main Page.

<table>
<thead>
<tr>
<th>Tools</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Now</td>
<td>Run the Anti-Malware scan.</td>
</tr>
<tr>
<td>Update Now/Upgrade Now</td>
<td>Update the Anti-Malware signatures and client policy (if there is a changed policy on the server for the client to update to). You can also start a postponed deployment.</td>
</tr>
<tr>
<td>Connect</td>
<td>Connect to the default VPN.</td>
</tr>
<tr>
<td>Connect To</td>
<td>Select a VPN to connect to.</td>
</tr>
<tr>
<td>Advanced</td>
<td>See the security policy and configure advanced options.</td>
</tr>
</tbody>
</table>

**Advanced**

The **Advanced** page has these options:

- **View server information** - Shows the IP address of the server you are connected to and the state of the connection.
- **View policies** - Shows the policies that are installed as part of Endpoint Security, the version installed, the date the policy was installed by your administrator, and the mode it is in (Connected or Disconnected).
- **View Logs** - Shows a log of your Endpoint Security activity. Your administrator automatically sees this data also.
- **Collect information for technical support** - Selects which logs are sent to Technical Support to use for troubleshooting. You can specify how much information and the range of dates to include in the compiled logs.
- **Personalization** - Select the default action for the notification area icon.

**Notification Area Icons and Options**

The icons shown in the taskbar notification area let you quickly monitor your security status and Internet activity. You can also access your security settings in just a few clicks. Right-click any of these icons to access a shortcut menu:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![VPN connected icon]</td>
<td>VPN is connected.</td>
</tr>
<tr>
<td>![Security scan icon]</td>
<td>Security scan, encryption, or change in client settings is in progress.</td>
</tr>
</tbody>
</table>
## Introduction to Endpoint Security

When you right-click the Endpoint Security icon, you get several options. The options that are enabled for you depend on the permissions set by your administrator. Similar options are available in the Tools section of the Endpoint Security Main Page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Overview</td>
<td>Show the Endpoint Security Main Page.</td>
</tr>
<tr>
<td>Scan Now</td>
<td>Run the Anti-Malware scan.</td>
</tr>
<tr>
<td>Update Now</td>
<td>Update Anti-Malware signatures.</td>
</tr>
<tr>
<td>Connect</td>
<td>Connect to the VPN site.</td>
</tr>
<tr>
<td>Connect to</td>
<td>Select a VPN site to connect to.</td>
</tr>
<tr>
<td>Register to hotspot</td>
<td>Register for temporary access to a public wireless hotspot. Open a browser immediately and follow the hotspot instructions to register (usually click a button).</td>
</tr>
<tr>
<td>Shut Down Network Protection</td>
<td>Disable Compliance, Firewall, and Anti-Malware.</td>
</tr>
<tr>
<td>Disconnect from VPN</td>
<td>Disconnect your VPN, if you are connected.</td>
</tr>
<tr>
<td>Help</td>
<td>Open the Endpoint Security Online Help.</td>
</tr>
<tr>
<td>About</td>
<td>Show the versions of the Endpoint Security components.</td>
</tr>
</tbody>
</table>

## Responding to Alerts

While you use the Endpoint Security client, you might see alerts. You must respond to some alerts while other alerts are just informative.

### New Application Alerts

The majority of the alerts you see will be New Application alerts. These alerts occur when a program on your computer requests access or server permission to the Internet or your local network. Use the New Application alert to give access permission to applications that need it, such as your browser and e-mail program.

Few applications or processes actually require server permission in order to function properly. Some processes, however, are used by Microsoft Windows to carry out legitimate functions. Some of the more common ones you may see in alerts are:

- lsass.exe
- spoolsv.exe
- svchost.exe
- services.exe
- winlogon.exe

If you do not recognize the applications or process that is asking for server permission, search the Microsoft Support Web site (http://support.microsoft.com/) for information on the process to determine what it is and what it is used for. Be aware that many legitimate Windows processes, including those listed above, have
the potential to be used by hackers to disguise worms and viruses, or to provide backdoor access to your system for Trojan horses. If you were not performing a function (such as browsing files, logging onto a network, or downloading files) when the alert appeared, then the safest approach is to deny server permission. If you see many server applications alerts, you might want to run an Anti-Malware scan as an added precaution.

**New Network and VPN Alerts**

Other alerts you might see are the New Network alert and VPN Configuration alerts. These occur when the client detects a network connection or VPN connection. They help you configure your network and program permissions correctly so that you can work securely over your network.

**Compliance Alerts**

The Endpoint Compliance blade makes sure that:

- All required Endpoint Security packages, with version updates, are installed on your computer.
- Required operating systems, with versions, service packs, and updates are installed on your computer.
- Only authorized programs are installed and running on your computer.

Compliance alerts show when your computer does not match the Endpoint Compliance policy. This can occur if there are changes to the Endpoint Compliance rules or to your computer configuration. If Endpoint Security determines that your computer is not compliant, a compliance alert shows with this information:

- One of these Endpoint Compliance states:
  - **Warning** - Your computer is not compliant but you can continue to use network resources. Do the steps to make your computer compliant as quickly as possible.
  - **About to be restricted** - Your computer is not compliant. You must make your computer compliant immediately. If you do not do this, access to network resources from your computer will be restricted.
  - **Restricted** - Your computer is not compliant. Access to network resources from your computer is restricted until you make your computer compliant.
  - Instructions for making your computer compliant with the policy.

**Media Encryption and Port Protection Alerts**

If you have the Media Encryption and Port Protection blade as part of your Endpoint Security, you might see alerts related to device scanning or encryption. Follow the on-screen instructions.
Uninstalling the Endpoint Security Client

To uninstall the Endpoint Security client:

1. If you are using Windows 7 or Vista, disable User Account Control (UAC).
2. Go to the Add/Remove Programs applet in the Windows Control Panel.
3. Make sure that the original EPS.msi and PreUpgrade.exe files are present on the endpoint computer.
4. If the client has Full Disk Encryption installed, run the Add/Remove Programs applet again after the disk completes the decryption.
Chapter 2

Anti-Malware

In This Chapter

Uninstalling other Anti-Virus Software 15
Your Anti-malware Status 15
Updating Anti-Malware 16
Scanning 16

Anti-Malware protects your computer against viruses, spyware, and malicious software. Real-time and scheduled scans detect malicious software and make them harmless before they can damage your computer.

Uninstalling other Anti-Virus Software

Before you install Endpoint Security, uninstall any other Anti-Virus software from your computer, including suite products that include virus protection among their features. If you are using a program that cannot be uninstalled automatically, use Add/Remove Programs from the Windows Control Panel.

Your Anti-malware Status

To view the status of your Anti-Malware Blade, from the Endpoint Security Main Page, click Anti-Malware Blade.

On this page you can:

- See the status of the Anti-Malware Blade. The status can be:
  - On - Anti-Malware has started and is up to date.
  - Off - Anti-Malware is not active.
  - Initializing - Anti-Malware is still starting.
  - Warning - Anti-Malware is not up to date. Update as soon as possible.
  - Alert - Anti-Malware is severely out of date. Update immediately.
  - Error - An error is preventing the Anti-Malware from working. Contact your administrator.
  - Infected - Untreated malware was detected on your computer.
  - Scanning - Anti-malware scan is currently in progress.

- See the dates and times of your last scans and updates.

- Click Scan Now to run a scan.

- See files, paths, and trusted processes that are excluded from scans.

- See items that are quarantined. Quarantined items are deleted and put in a secure storage area. They can be restored from this area if necessary.
Updating Anti-Malware

Every Anti-Malware application contains a definition file, with information to identify and locate malware on the computer. As new malware applications are discovered, the client updates its database with the definition files necessary to detect these new threats.

The Endpoint Security client gets updates regularly. In the Client Status section of the Anti-Malware Detail pane, you can see when the last update occurred and when the next update is scheduled.

To run an update:

- In the Endpoint Security Main Page, under Tools, click Update Now.
- Right-click the endpoint security icon in the taskbar notification area and select Update Now.

If there is an error, you see a message:

- Anti-Malware was unable to update. No connection to the server - Make sure that you are connected to the network. If you continue to see this, contact your administrator.
- An unexpected error occurred - If you continue to see this, contact your administrator.
- Anti-Malware Updater is off.

Scanning

You can start a scan of your computer or a specific file, folder or directory in these ways:

To scan the full computer:

- In the Endpoint Security Main Page, click Tools > Scan Now.
- Right-click the notification area icon and select Scan Now.

To scan a file, folder, or drive:

Right-click a file, folder, or drive on your computer and choose Scan with Check Point Anti-Malware.

Based on the settings configured by your administrator, Anti-Malware scans the entire contents of your computer. It finds malware that might be dormant on all parts of your computer.

Because full-computer scans are very thorough, they require time and computer resources. Therefore, your computer's performance might be slow while a full-computer scan is in progress. To avoid impact on your work, your administrator can schedule scans to run at a time when you are not likely to use your computer.

Note - If you click Pause in the Scan window while a scan runs, only the current scan stops. On-Access scanning is not disabled. Click Resume to continue the scan.

Understanding Scan Results

After the scan is completed, the details of malware detected show in the scan window. The details are:

- Threat - The name of the malware detected.
- Type - The type of threat.
- Action - What actions Endpoint Security took.
- Result - The result of the action.
- Path - Where the infection was found on the computer.
Viewing Quarantined Items

In some cases, items detected during an Anti-Malware scan cannot be treated or removed automatically. These items are usually placed into quarantine so that they become harmless but can be restored and treated in the future after an update to your malware files.

To view and treat Anti-Malware in quarantine:
1. Open Anti-Malware Blade.
2. Click Quarantine.
   The details of the quarantined files shows:
   • Infection - Name of the malware.
   • Type - Type of malware.
   • Risk - The risk level of the infection.
   • Path - The original location of the malware on your computer.
   • Days in Quarantine - Number of days the file has been in quarantine.
3. Select a file and click:
   • Delete - Permanently delete the file.
   • Restore - Takes the file out of quarantine.

Note - Only restore a file if you are sure that the file is not malware.
Chapter 3

Media Encryption and Port Protection

In This Chapter
- Components of Media Encryption and Port Protection
- Using Media Encryption and Port Protection

The Media Encryption and Port Protection blade prevents leakage of sensitive data in these ways:

- The policy defines whether or not to allow access to devices connected to a physical port, such as USB storage devices.
- Based on your permissions, you can optionally encrypt external devices connected to your computer to prevent access without your permission.

The features of Media Encryption and Port Protection are described in the next sections.

Components of Media Encryption and Port Protection

The actions that you can do in Media Encryption and Port Protection depend on the policy set by your administrator. Therefore, all of the features described below might not be available for you.

- Port Protection rules control access to removable devices such as:
  - USB devices
  - CD/DVD Drives
  - PDAs
  - Smartphones
  - Flash memory
  - Floppy disk drives
  - Digital cameras
  - External hard disks (NTFS formatted)

The policy controls device access for all available ports including USB and Firewire. Policy rules define access rights for each type of removable storage device and the ports that they can connect to. Policy rules can also include requirements for malware scanning and data authorization. The policy can also prevent you from connecting unauthorized devices to your computer.

- Media Encryption lets you create encrypted storage on removable storage devices that contains business related data. Once you create the encrypted storage, you will see two drives in Windows Explorer. One drive is encrypted for business data. The other drive is not encrypted and can be used for non-business data.

Your rules can apply different access permissions for business data (encrypted) and non-business data (non-encrypted). Rules can also define which file types are defined as business data and must be stored on encrypted storage.

Using Media Encryption and Port Protection

This section describes the process of encrypting, decrypting and managing removable storage devices. Media Encryption and Port Protection secures a removable storage device by encrypting some or all of the storage device. It then puts the specified files (typically business data) on the encrypted device.
Important - Media Encryption has no way of detecting hardware faults on external drives. For this reason, the encrypted drive might be created on a damaged section of the external drive, resulting in unexpected data loss.

We strongly recommend that you back up all files and data stored on an external device (such as HDD, USB or other flash-based device), before encrypting the device. See sk44844 (http://supportcontent.checkpoint.com/solutions?id=sk44844).

To work with Media Encryption and Port Protection, from the Endpoint Security Main Page, click Media Encryption and Port Protection.

The Media Encryption and Port Protection Details window opens, showing removable storage devices that are attached to your computer.

Encrypted Media

Your organization's policy defines access to business and non-business data. It is possible that your policy allows access only to business data, which is encrypted. Alternatively, your policy can allow access to business and non-business data, but the business data must be encrypted and password protected. In this case, Media Encryption creates two drives on the physical storage device. One encrypted drive for business data and a non-encrypted drive for non-business data.

If you have the required permissions you can:

- Define a password that gives users full access to the encrypted drive.
- Define the percentage of the physical device to be encrypted. For example, if you encrypt 50% of a device, the encrypted (business data) drive will occupy 50% of the physical device. The remainder is assigned to non-encrypted (non-business data) drive. When you import and encrypt files, they are always put on the business data drive.

  Note - If you define a drive that is smaller than the volume of data you want to encrypt, the encryption procedure fails.

Important - We recommend that you do not encrypt non-computer external devices such as: digital cameras, Smartphones, MP3 players, and the like. Do not encrypt removable media that can be inserted in or connected to such devices.

To encrypt a new storage device:

1. Insert a removable storage device (CD, DVD, USB) into your computer.

   Note - You can also start the encryption procedure by dragging a business data file to a storage device in Windows Explorer that has not yet been encrypted. In the Files Must be Encrypted window, click Encrypt. Continue with step 3.

2. From Media Encryption and Port Protection, select a device and click Create Encrypted Storage.

   The Removable Device Encryption window opens. The options shown are set by your administrator. You can also encrypt and decrypt devices

3. In the Removable Device Encryption window, configure the available options. If you do not see an option, that option is not allowed by your policy.
   - Set a password to allow full access to the device while online (connected to your network) and offline.
   - Select a percentage of the storage device to encrypt (not available for CDs or DVDs).

4. Optional (if available): Click Advanced Settings to:
   - Set a password for read-only access to the device.
   - Set an owner for the device (not available for CDs or DVDs). Usually, the administrator sets a policy that only the owner of the device can access the files on the device. Select one of these options:
     - Media owner will be assigned on first use - The first user to insert the storage device into an endpoint computer automatically becomes the owner.
     - Assign media to a user: Assign ownership to the user running the encryption (that is, yourself) or click Browse to select a user from the active domain.

5. Click Encrypt.
6. If you are encrypting a CD or DVD, a window opens where you can add and remove the files that will be copied to the encrypted drive on the disk.
   a) Go up one step in the folder structure.
   b) Add files or add an entire folder copy to the disk.
   c) Select and delete any file or folder that you do not want to copy to the disk.
   d) Click Next. The files are copied to the disk.
   e) A message shows when the procedure completes.
7. A window shows the encryption progress. Based on the type of storage device and the quantity of data, this process may take a long time.
   - **Important** - Do NOT remove the storage device during the encryption process. This will destroy your data and may damage the storage device.
8. When the Finish window opens, click Finish to complete the process.

The encrypted storage device status now appears as **Encrypted** in the Media Encryption and Port Protection window. Non-business data is not changed, deleted or encrypted. It remains on the non-encrypted device.

### Adding Business Data to an Encrypted Device

If you have the required permissions, you can:
- Add new business data files to and from the encrypted storage drive.
- Add non-business data to the unencrypted drive.

**To add business data to an encrypted storage device:**
1. Copy, move, or drag-and-drop files to the applicable device.
2. If you try to copy business data to an unencrypted device or drive, a window opens asking you to encrypt the file. In the Check Point Endpoint Security window, click Encrypt and then click Yes to confirm.
   The business data file is encrypted and copied to the encrypted storage device.

You can also encrypt a device to contain business data from the Media Encryption and Port Protection Details page of the Endpoint Security Main Page.

### Encrypting CDs and DVDs

If allowed by your policy, you can encrypt CDs and DVDs with the following limitations:
- CDs can be encrypted on Windows XP, Windows Vista, and Windows 7.
- DVDs can be encrypted on Windows Vista and Windows 7. To encrypt DVDs on Windows XP, install Microsoft hotfix KB932716.
- Encryption can be done only on RW and blank R/RW disks.
- You cannot add or delete data from a CD or DVD once it is burned. You can only be erased the disk completely.

The process of importing and exporting files to CD/DVDs is similar to that of other removable storage devices described in Encrypting Media (on page 19). Two differences between CD/DVDs and other removable storage devices are that you cannot encrypt only a part of a CD/DVD, and you cannot add or delete files once the disk has been burnt. If you want to remove information on a rewritable disk, you need to use the **Erase** feature to completely erase it.
Encrypting Media In Windows 7

When you insert a new blank CD or DVD in Windows 7 and attempt to write files to it for the first time, two options are available:

- Like a USB flash drive
- With a CD/DVD Player

To successfully encrypt data to the disk, select: With a CD/DVD Player. Media encryption only intercepts requests to burn that use this mode.

Accessing Encrypted Storage Device

As allowed by your policy, you can access business data on an encrypted storage device from a computer protected by Media Encryption and Port Protection. Access permissions can be full (read/write) or read only.

If allowed by your policy, you can also access business data from a computer that is not protected by Media Encryption and Port Protection. In this case you must enter a password to gain access. To do this, Media Encryption copies these files to the physical storage device:

- autorun.inf - Automatically runs the decryption program if auto run is enabled on the device.
- Access to Business Data.exe - The decryption program that lets you access business data on the endpoint client.

**Note** - You must set a password during the encryption process to be able to access the information from computers that do not have Media Encryption and Port Protection installed.

To access data on an encrypted device from a computer without Media Encryption and Port Protection:

1. Insert the encrypted device into the computer.
2. If necessary, open the drive window in Windows Explorer window and double-click Access to Business Data.
3. Enter the applicable password.

A Windows Explorer window shows the contents of the encrypted device. You can work with these files according to your permissions.

- If you have Full access permissions, you can drag-and-drop or copy/paste business data to and from the encrypted device.
- If you have read-only permissions, you can only read the file contents but cannot change the data, copy files, or delete files.

**Note** - If you forget your password or do not have your Smartcard, you can use Remote Help ("If You Do Not Have Your Password" on page 27) for assistance.

Deleting Encrypted Files and Storage Devices

You can delete files from an encrypted storage device or delete the encrypted drive itself. Usually, the Media Encryption and Port Protection policy lets only the device owner or another authorized user remove files or delete an encrypted drive.

Make sure that you copy or back up files on the encrypted device before decrypting it. The decryption procedure automatically deletes all data on the encrypted storage device. If your policy does not let you decrypt files or a storage device, you must ask an administrator to do this for you.

To remove files from an encrypted storage device:

1. Connect the encrypted storage device to your computer.
2. If you do not have automatic access to the storage device, enter the password when prompted and click OK.
3. Select the files to delete.
4. Move the files to your local disk or delete them.
To delete an encrypted storage device:
1. Connect the encrypted storage device to your computer.
2. If you do not have automatic access to the storage device, enter the password when prompted and click OK.
3. From the Media Encryption and Port Protection Details page, click Remove Encryption. If there is data on the encrypted drive, a warning message shows saying that all data on the encrypted drive will be deleted. Click Yes to continue.
4. Click Finish to complete the process.

The decryption procedure can take some time, depending on the size and type of device. When the decryption completes, all encrypted data is deleted and the encrypted drive is automatically deleted.

Important - Do NOT remove the storage device during the decryption process. This will destroy your data and may damage the storage device.

Scanning Devices
To start a Media Encryption and Port Protection scan:
In Media Encryption and Port Protection, select a device and click Scan Device. Files are scanned according to the Media Encryption and Port Protection policy.

Note - Clicking Pause in the Scan dialog while a scan is being performed will stop the current scan only. On Access scanning will not be disabled. Click Resume to resume the current scan.

Changing the Encrypted Device Password
To change the removable storage device access password for an encrypted device:
1. Right-click a device in the Media Encryption and Port Protection Details window.
2. Select Advanced > Set Full Access Password or Set Read Only Password.
3. Enter the old password and click OK. You must have Full Access to change a Full Access password or a Read Only password.

Note - The Full Access and Read Only passwords cannot be identical.
4. Enter and confirm the new password.

Note - The password must meet the criteria defined by the administrator.
5. Click OK.
Converting File Encryption Devices to Media Encryption

You can easily convert storage devices that were encrypted with Pointsec File Encryption R73 to Media Encryption E80.40. When you insert a device encrypted with Pointsec File Encryption into an endpoint computer running E80.40, you are prompted to upgrade the device.

To convert a File Encryption device to Media Encryption:

1. Insert the device into a computer that has an Endpoint Security client with the Media Encryption and Port Protection blade active.

2. This message shows:
   To access the device, you need to convert it to Media Encryption format.

3. Click OK.

4. If necessary, enter the File Encryption credentials of the device in the window that opens. These must be the credentials originally to encrypt the storage device. They can be:
   - A corporate user name and password assigned by the administrator
   - A personal user name and password defined for this storage device
   If the device was originally encrypted with a corporate password and Media Encryption and Port Protection can find the password on the computer, this window does not open.

5. Enter and re-enter a new password for the device.

6. Click Continue.

7. Optionally, edit the Media Encryption settings.

8. Click Encrypt.

9. When the encryption is complete, click Finish.
Chapter 4

Firewall & Application Control

In This Chapter

Understanding Firewall Protection 24
Understanding Application Control 24

Firewall and Application Control is your front line of defense against Internet threats.

Understanding Firewall Protection

The firewall guards the "doors" to your computer—that is, the ports through which Internet traffic comes in and goes out. It examines all the network traffic and application traffic arriving at your computer, and asks these questions:

- Where did the traffic come from and what port is it addressed to?
- Do the firewall rules allow traffic through that port?
- Does the traffic violate any global rules?

The answers to these questions determine whether the traffic is allowed or blocked.

The Endpoint Security administrator sets the policies and rules that determine what traffic the firewall allows.

Understanding Application Control

The Application Control blade restricts network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block, or terminate applications and processes. Only applications that try to get network access can be blocked or terminated.

Based on the policy settings, an alert can show which application was blocked or terminated. You can also see which applications are blocked and terminated in the Current Status section of the Firewall and Application Control Blades tab of the Endpoint Security Main Page.
Chapter 5

Full Disk Encryption

In This Chapter

Overview of the Login Screen 25
Authenticating to Full Disk Encryption 26

Full Disk Encryption combines boot protection with Pre-boot authentication, and strong encryption to ensure that only authorized users are granted access to information stored in desktop and laptop PCs.

Overview of the Login Screen

If your administrator enables Full Disk Encryption, when you log in to your computer you will get a Pre-boot login screen where you enter your authentication credentials. If you do not enter the correct credentials, you cannot access your computer at all.

This is important protection for the information stored on your computer and corporate network. For example, if someone steals your computer and tries to access the information in it, the thief will not be able to get past this screen.

You can also use these options in the login screen:

- Remote Help - Click this if you do not know your password. You and the help desk or administrator will exchange information to recover your password.
- SSO Options - Select the SSO Active option to use the same credentials for your Windows login and your Full Disk Encryption login. If you need to log in to Windows with different credentials than the Full Disk Encryption credentials, make sure the SSO Active option is cleared.
- Keyboard Layout - To change the keyboard layout to a different language, click on the shaded area that says your keyboard layout, for example, en-US or sv-SE. You can also press Alt + Shift at this point to switch the keyboard layout to another language you have set in Windows. All keyboard layouts that are loaded in Windows are supported in the Pre-boot environment.
- Options - Click this to:
  - Virtual Keyboard - Open an on-screen keyboard to use in the authentication process.
  - Language - Change the language of the Pre-boot screen.
  - Help - Opens Help for more information.
  - Character Map - Open a set of Latin characters on-screen that you can use in the authentication process.

Using the Virtual Keyboard

From the Pre-boot page, select Options > Virtual Keyboard to open a Virtual Keyboard. You can use the virtual keyboard throughout the authentication.

To close the virtual keyboard, click it again from the Options menu.
Using Special Characters

Your user credentials might contain characters that are not easily available on your keyboard. From the Pre-boot screen, you can select Options > Character Map to enter characters into the login screen.

To insert a character into a field in the Pre-boot login screen:
1. In the Pre-boot login screen, select Options > Character Map.
   A set of Latin characters shows on the screen.
2. Click in a field in the login window, for example User account name.
3. Click a character from the Character Map.
   It shows in the selected field.

To change the set of characters that shows:
1. Click the arrow in the top right corner of the Character Map.
2. Select a set of characters from the list.

Changing the Language

You can set the Pre-boot to recognize a language other than the default language of your computer. After you change the language, it is used as the default the next time you authenticate with Full Disk Encryption.

To set the language for the Pre-boot screen:
1. From the Pre-boot screen, select Options > Language.
   The Language window opens.
2. Select a language and click OK.
   The computer restarts automatically. When it starts again, the Pre-boot screen is in the selected language.

Authenticating to Full Disk Encryption

This section discusses how to authenticate yourself to access your Full Disk Encryption-protected computer.

Being authenticated means being verified by Full Disk Encryption as someone who is authorized to use a specific computer. When you turn on or restart a Full Disk Encryption-protected computer, the Pre-boot login screen opens.

Enter a valid user name and password or insert your Smartcard and enter the PIN. Full Disk Encryption verifies that you are authorized to access the computer and lets Windows start.

Based on the settings for your organization, you might log in to Windows only and not see a Pre-boot login screen.

Note - Depending on the settings configured by your administrator, you might not be able to start Windows in Safe Mode.

Ensuring That No One Tampered with Your Computer

If you did not personally start the machine yourself, you should always press CTRL+ALT+DEL to restart your computer before authenticating yourself. This ensures that your computer has not been tampered with and that your user account name and password cannot be hijacked.
Authenticating for the First Time with Fixed Password

Usually you use your Windows credentials to log in to your Full Disk Encryption-protected computer as a new user. Sometimes an administrator will give you a user account name and a password.

To authenticate for the first time with your fixed password:
2. Enter your User account name and Password. The password is obscured with asterisks (*) when entered.
3. Click OK.
4. Click Continue to close the window.
Full Disk Encryption lets Windows start.

Authenticating with a Smartcard or USB Token

Smartcards and USB tokens contain certificates protected by PIN codes. To be authenticated by Full Disk Encryption, you must connect the card or token to the computer and enter a valid card or token PIN.

Your administrator will supply you with your Smartcard or USB token and the information that you need to use it.

Make sure that your Smartcard or USB token is connected to your computer before you start to authenticate.

To authenticate with a Smartcard or USB token:
1. Connect your smart card/USB token to your Full Disk Encryption-protected computer.
2. Start your computer or press Ctrl+Alt+Delete. The User Account Identification window opens.
3. When the PIN field shows, enter your PIN.
4. Click OK.
Full Disk Encryption lets Windows start.

If You Do Not Have Your Password

If you forget your password or do not have your Smartcard, use Remote Help for assistance.

There are two types of Full Disk Encryption Remote Help:

- One Time Login - Allows access as an assumed identity for one session, without resetting the password.
- Remote password change - Use this option if you use a fixed password and forgot it.

To use Remote Help to log in:
1. Enter your User account name and click in the next field.
3. Select either Password Change or One-Time Logon.
4. Call your administrator or helpdesk to guide you through the process.
Chapter 6

WebCheck

In This Chapter
- WebCheck Protection 28
- Suspicious Site Warnings 28

WebCheck provides comprehensive protection against various Internet threats for your computer and your corporate network.

WebCheck Protection

Your administrator determines which WebCheck settings are deployed to protect your computer against Web-based threats. The following list explains the WebCheck features.

- **Trusted Mode**: Your browser opens in Trusted mode automatically when you go to your corporate Web site or Internet Web sites your administrator deems trustworthy. WebCheck features are inactive because these Web sites do not pose the same risk as the Internet at large. Your administrator configures which sites are safe to open in Trusted mode.

- **Virtualization**: WebCheck traps malware and other uninvited programs that are downloaded to your computer without your permission or knowledge in a virtual file system and blocks them so that they never get to your hard disks.

- **Anti-phishing**: WebCheck tracks the most recently discovered phishing and spy sites. WebCheck also looks for certain known characteristics of fraudulent sites, to detect phishing sites that were created even seconds before you encountered them.

  If you go to one of these sites, WebCheck interrupts your browsing with a warning so you can leave the site immediately.

**Switching between the Trusted and Virtualization modes**

Due to limitations of the virtual engine, WebCheck uses different browser windows for each mode. Links to trusted and untrusted sites open in their respective windows. Sometimes sites contain automatic redirections that can cause the opening extra browser windows.

Suspicious Site Warnings

When WebCheck detects a security problem with a Web site you are visiting, it warns you immediately about the imminent danger so you can leave before anything happens.
**Yellow Caution Banner**

If you reach a Web site that does not have adequate security credentials, a yellow caution message opens at the top of the page.

This site may not necessarily be malicious. It may be that it is new or has limited funding and therefore has not yet obtained a strong security certification (SSL certificate). Nevertheless, the lack of security at the site means that data could be intercepted, so avoid entering sensitive data.

<table>
<thead>
<tr>
<th>Yellow Caution Banner</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk level of Web site</td>
<td>MEDIUM for entering data or downloading files from this site.</td>
</tr>
<tr>
<td>Recommendation</td>
<td>With WebCheck active, viewing the site should be safe, but do not enter any sensitive data or download files at this site.</td>
</tr>
<tr>
<td>Why is the site questionable?</td>
<td>Click the <strong>Read more</strong> link in the warning dialog box to get security related information about the site.</td>
</tr>
</tbody>
</table>

**"May Be Unsafe" Messages**

If you reach a Web site where the heuristic detection of WebCheck finds characteristics associated with phishing, your browsing is interrupted by a blue "may be a unsafe" message.

Although the site has characteristics common to phishing, it has not been officially reported as a phishing site. It could be a new, not-yet-discovered phishing site. On the other hand it could be safe.

Consider these recommendations to help you decide whether to trust this site.

<table>
<thead>
<tr>
<th>Blue Warning - May Be Unsafe</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk level of Web site</td>
<td>MEDIUM to HIGH for entering data or downloading files from this site.</td>
</tr>
<tr>
<td>Recommendations</td>
<td>The site may not be a phishing site, but we recommend you click <strong>Avoid this Site</strong> if any of the following are true:</td>
</tr>
<tr>
<td></td>
<td>• Did you get to this site by clicking a link in an e-mail?</td>
</tr>
<tr>
<td></td>
<td>• Does the address start with http instead of https? (Sites that ask for private data should be secured by extra encryption and authentication, indicated by https.)</td>
</tr>
<tr>
<td></td>
<td>• Is there a misspelling in the site address, such as &quot;yahooo&quot; instead of &quot;yahoo&quot;?</td>
</tr>
<tr>
<td></td>
<td>• Was the site created very recently?</td>
</tr>
<tr>
<td></td>
<td>• Is the site hosted in a country you weren't expecting?</td>
</tr>
<tr>
<td>Why is the site questionable?</td>
<td>Heuristic detection has found some characteristics common to phishing, but the site is not officially reported as a phishing site at his time.</td>
</tr>
</tbody>
</table>

If you believe that the site is safe to access, you can click the **Stay on Site** button. If you do not want any more warning messages from this site, click the **Click here** link and you will not get a warning message the next time you access the site.
Dangerous Site Messages

If you browse to a site that is known to be dangerous, WebCheck interrupts your browsing with a blue message that says: **Warning- This site is dangerous.**

<table>
<thead>
<tr>
<th>Dangerous Site Warning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk level of Web site</td>
<td>VERY HIGH</td>
</tr>
</tbody>
</table>

Recommendation

If you are not very sure that this site is legitimate, you should leave this site immediately to protect your computer and network.

Click **Avoid this Site** in the message to get out safely.

If you are sure that the site is safe to access, you can click the **Stay on Site** button. If you do not want any more warning messages from this site, click the **Click here** link and you will not get a warning message the next time you access the site.
Chapter 7

VPN

In This Chapter

VPN Basics 31
Secure Domain Logon 32
Configuring VPN 32
Changing the Site Authentication Scheme 33
Collecting Logs 36

Endpoint Security lets you easily set up a secure VPN to connect to your corporate resources.

VPN Basics

Endpoint Security VPN lets you connect securely to your enterprise network when working remotely. You can then access private files over the Internet knowing that unauthorized persons cannot view or alter them. The VPN connection can be made directly to the server or through an Internet Service Provider (ISP). Remote users can connect to the organization using any network adapter (including wireless adapters) or modem dialup.

The Endpoint Security VPN authenticates the parties and encrypts the data that passes between them. The VPN feature uses standard Internet protocols for strong encryption and authentication. Encryption ensures that only the authenticated parties can read the data passed between them. In addition, the integrity of the data is maintained, which means the data cannot be altered during transit.

The VPN Detail page displays information about any current VPN connection (if any) and about the status of your remote connection to a VPN enabled security gateway. From the VPN page, you can click Manage Settings > New to launch the Site Wizard to create a VPN site, connect to or disconnect from a VPN site, or open the VPN Settings window to configure profiles and sites, configure any special connection options, or manage certificates.

Creating a VPN Site

You can configure multiple VPN sites. If you are in a hotspot environment, connect to the hotspot before you connect to the VPN site.

To configure a VPN site:

1. If you do not have a VPN site configured, open the Site Wizard: right-click the notification area icon and select Connect.
2. When the wizard opens, click Next.
3. Enter a server address or name.
   The wizard can detect a site that your administrator configured. You can leave this site or change it.
4. Optional: Select the Display name option and enter a name, if you want to see a name of the site that is meaningful for you. For example, you can call the site "Corporate Headquarters".
5. Click Next and wait while the new site is created.
   If you see the message about the site’s certificate, contact your system administrator.
6. Click Finish to complete the Wizard.
Connecting to the VPN

To connect to a VPN site you can:

- From the Endpoint Security Main Page, click **Remote Access VPN Blade > Connect to** or **Connect**.
- From the taskbar notification area icon, right-click and select **Connect**.

Secure Domain Logon

If the system administrator says that you must use SDL, enable Secure Domain Logon (SDL).

**To enable SDL on a client:**
1. Right-click the Client icon and select **VPN Options**.
2. In **Options > Advanced**, select **Enable Secure Domain Logon (SDL)**.
3. Click **OK**.
4. Restart the computer and log in.

Configuring VPN

You might have the option to go through the VPN for all your Internet traffic. This is more secure.

**To configure VPN Tunneling:**
1. Right-click the Client icon and select **VPN Options**.
   - The **Options** window opens.
2. On the **Sites** tab, select the site to which you want to connect, and click **Properties**.
   - The **Properties** window for the site opens.
3. Open the **Settings** tab.
4. **In VPN tunneling**, click **Encrypt all traffic and route to gateway**.
   - **Note** - In SecuRemote, this option is disabled. If this option is disabled in Endpoint Security VPN or Check Point Mobile for Windows, consult your system administrator.
5. Click **OK**.
Changing the Site Authentication Scheme

If you have the option from your system administrator, you can change the method that you use to authenticate to the VPN.

To change the client authentication method for a specific site:
1. Right-click the Client icon and select VPN Options. The Options window opens.
2. On the Site tab, select the site and click Properties. The Properties window for the site opens.
   On the Settings tab, select an option from the Authentication Scheme drop-down menu.
   - Username and password
   - Certificate - CAPI
   - Certificate - P12
   - SecurID - KeyFob
   - SecurID - PinPad
   - SecurID Software Token
   - Challenge Response
   - SAA - Username and Password
   - SAA - Challenge Response

Certificate Enrollment and Renewal

A. To enroll a certificate:
1. Right-click the client icon in the system tray, and select VPN Options. The site Properties window opens.
2. On the Sites tab, select the site from which you will enroll a certificate and click Properties.
3. Select the Settings tab.
4. Choose the setting type you want, CAPI or P12, and click Enroll. The CAPI or P12 window opens.
5. For CAPI, choose the provider to which you will enroll the certificate.
6. For P12, choose a new password for the certificate and confirm it.
7. Enter the Registration Key that your administrator sent you.
8. Click Enroll. The certificate is enrolled and ready for use.

B. To renew a certificate:
1. Right-click the client icon in the system tray, and select VPN Options. The site Properties window opens.
2. On the Sites tab, select the site from which you will renew a certificate and click Properties. The authentication method you chose is set and the certificate will be renewed accordingly.
3. Select the Settings tab.
4. Click the Renew button. The CAPI or P12 window opens.
5. For CAPI, choose the certificate you want to renew from the drop-down list. For P12, choose a P12 file and enter its password.
6. Click Renew. The certificate is renewed and ready for use.
Importing a Certificate into the CAPI Store

Before you can use the certificate to authenticate your computer, you must get:

- The certificate file.
- The password for the file.
- The name of the site (each certificate is valid for one site).

If the system administrator instructed you to save the certificate on the computer, import it to the CAPI store. If not, the administrator will give you the certificate file on a USB or other removable media. Make sure you get the password.

To import a certificate file to the CAPI store:
1. Right-click the client tray icon, and select VPN Options.
2. On the Sites tab, select the site and click Properties.
3. Open the Settings tab.
4. Make sure that Certificate - CAPI is selected in the Method list.
5. Click Import.
7. Enter the certificate password and click Import.

Authenticating with PKCS#12 Certificate File

For security reasons, your system administrator might require you to authenticate directly with the PKCS#12 certificate and not from the certificate stored in the CAPI. For example, if you use several desktop workstations and laptops, you might not want to leave your certificate on different computers. If the PKCS#12 certificate is in the CAPI store and someone steals your laptop, they can use the client to connect to the site. For increased security, your administrator might instruct you to save the PKCS#12 certificate to a USB stick or other storage device.

To authenticate with a PKC#12 certificate file:
2. Connect to the site.
   The Connect window opens.
3. In the Certificate File area, browse to the certificates stored on the floppy or USB disk.
4. In the Password field, enter the certificate password.
5. Click Connect.

Note - If you selected the Always-Connect option, whenever communication between the site and client is closed, the user will be prompted to enter the certificate password.

SecurID

The RSA SecurID authentication mechanism consists of either hardware (FOB, USB token) or software (softID) that generates an authentication code at fixed intervals (usually one minute), with a built-in clock and encoded random key.

The most common form of SecurID Token is the hand-held device. The device is usually a key FOB or slim card. The token can have a PIN pad, onto which a user enters a personal identification number (PIN) to generate a passcode. When the token does not have a PIN pad, a tokencode is displayed. A tokencode is the changing number displayed on the key FOB.

The Endpoint Connect site wizard supports both methods, as well as softID. Endpoint Connect uses both the PIN and tokencode, or just the passcode, to authenticate to the gateway.
**Challenge-Response**

Challenge-response is an authentication protocol in which one party provides the first string (the challenge), and the other party verifies it with the next string (the response). For authentication to take place, the response is validated.

**Secure Authentication API (SAA)**

Secure Authentication API (SAA) lets you use third-party authentication technologies with your E80.40. To work, it requires a DLL file that is installed on your client.

If your administrator instructs you to select Secure Authentication API (SAA) as the authentication method when you create a site, you need this information:

- The type of SAA authentication that you must select - one of these:
  - **Username and Password** - Users enter a username and password.
  - **Challenge Response** - Users enter a response to a challenge.

- You might need a DLL file. If your administrator already configured this, then you do not need it.

  **Note** - Only users with administrator permissions can replace the DLL.

If you select SAA as the authentication in the site wizard, a new page opens where you select the type of SAA authentication and a DLL file, if required.

![Secure Authentication API (SAA)]

Select the type of third party authentication that you use.

- **Username and Password**
  Click if your system administrator provided you with account name and a password.

- **Challenge Response**
  Click if you are required to provide different responses to a challenge.

**Use a Secure Authentication API File:**

![Select a SAA DLL file] Browse...

Select the Secure Authentication API DLL file supplied by your administrator. If you do not have this, contact your administrator.

---

**Replacing the SAA DLL File**

Your administrator might instruct you to replace the DLL file on your client.

**Note** - Only users with administrator permissions can replace the DLL.

**To replace the local DLL file:**

1. Right-click the client icon and select **Options**.
2. In the **Advanced** tab, next to **Use a Secure Authentication API File**, browse to select the new DLL file.
   This file is used for SAA authentication.
Connecting to a Site with SAA

Usually, when you connect to a site, a login window opens and you enter your authentication information directly in that window. If SAA is the authentication method for the site, there are no fields for authentication information in the login window. You must click the **Connect** button in the window and a new window opens for authentication information.

![Login Window with SAA Authentication Method](image)

Collecting Logs

If your system administrator or help desk asks for logs to resolve issues, you can collect the logs from your client.

**To collect logs:**
1. Right-click the Client icon and select **VPN Options**.
2. Open the **Advanced** tab.
3. Click **Enable Logging**.
4. Reproduce the problem.
5. Click **Collect Logs**.

**Note** - The logs are saved to `%TEMP%\trac\trlogs_timestamp.cab`. It opens after the logs are collected.

This folder is sometimes hidden. If you need to locate this folder, in **Control panel > Folder Options > View**, select **Show hidden files and folders**.
Chapter 8

Troubleshooting

In This Chapter

Technical Difficulties 37
Using Logs 37
Collecting Information for Technical Support 38

Technical Difficulties

The policies and setting of your Endpoint Security are set by your Endpoint Security administrator. The administrator can solve many issues by making slight changes to your settings. Therefore, if you have technical difficulties, contact your administrator.

Using Logs

Endpoint Security activity is recorded in logs. Your administrator might use information from the logs for various reasons that include:

- To identify the cause of technical problems.
- To monitor Anti-Malware or VPN traffic more closely.
- To see if there is proper communication between your client and other machines that it needs to communicate with.
- To make sure that all features function as they should

To see the logs go to Endpoint Security Main Page > Advanced > View Logs.

What Can I do with Logs

The table below lists actions that you can do in the Log page.

<table>
<thead>
<tr>
<th>What You Want to Do</th>
<th>Required Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>See details of a log entry</td>
<td>Double-click the log entry</td>
</tr>
<tr>
<td>Export logs to a file</td>
<td>Select File &gt; Export to file</td>
</tr>
<tr>
<td>See logs of a specific type</td>
<td>Select View &gt; Event Filter</td>
</tr>
<tr>
<td>See logs from a specific date</td>
<td>Select View &gt; Event Filter</td>
</tr>
<tr>
<td>Sort logs According to a specific column</td>
<td>Click the column heading</td>
</tr>
<tr>
<td>Update the displayed logs one time</td>
<td>Select File &gt; Refresh or click the Refresh icon</td>
</tr>
<tr>
<td>Update the displayed logs every 5 seconds</td>
<td>Select File &gt; Auto Refresh or click the Auto Refresh icon</td>
</tr>
<tr>
<td>Copy log entries to the clipboard</td>
<td>Select the entries and click Control +C</td>
</tr>
</tbody>
</table>
Using the Event Filter
The Event Filter lets you filter the logs to see the information that is relevant to you.

You can filter by:
- **Event types** - Select or clear the checkboxes that relate to the different Endpoint Security features. Only logs of events from the selected features are included in the results.
- **Time period** - Select a Start date and time and End date and time. Clear either the Start or End options if you want to keep them blank.
- **Number of events** - Select the maximum number of events that will show in results.
  - **Show Newest or Oldest first** - Select which logs should be at the top of the list.

To use the Event Filter:
1. Open the Event Filter pane:
   - Click the View Event Filter window icon.
   - Select View > Event Filter.
2. Click the black arrows to open and close the sections of the Events Filter pane.
3. Make selections to filter the log results.
4. Click Filter.
   The results of the filter show in the Log Viewer.

Exporting Logs
You might need to export the logs to a file to send to your administrator.

To export the logs:
1. From the Log Viewer window:
   - Click the Export icon.
   - Select Edit > Export to File.
   The Save As window opens.
2. In the Save As window, select the location where you want the file to be saved, enter a File name, and click Save.
   The logs are saved in a text file.

You can email this file to your administrator.

Collecting Information for Technical Support
Your administrator might tell you Collect information for technical support. This tool collects information from your system that technical support can use to resolve issues.

To use the Collect information for technical support tool:
1. From the Endpoint Security Main Page select Advanced and click Collect information from technical support.
   A command line window opens.
2. Press Enter to run the tool.
3. Wait while the tool runs.
4. When it finishes, it says that a cab file was created and opens the window where the cab file is located.
5. You can email this file to an address that you are given.
Index

A
Accessing Encrypted Storage Device • 21
Adding Business Data to an Encrypted Device • 20
Advanced • 11
Anti-Malware • 15
Anti-Malware Blade • 9
Authenticating for the First Time with Fixed Password • 27
Authenticating to Full Disk Encryption • 26
Authenticating with a Smartcard or USB Token • 27
Authenticating with PKCS#12 Certificate File • 34

C
Certificate Enrollment and Renewal • 33
Challenge-Response • 35
Changing the Encrypted Device Password • 22
Changing the Language • 26
Changing the Site Authentication Scheme • 33
Collecting Information for Technical Support • 38
Collecting Logs • 36
Compliance Alerts • 13
Compliance Blade • 8
Components of Media Encryption and Port Protection • 18
Configuring VPN • 32
Connecting to a Site with SAA • 36
Connecting to the VPN • 32
Converting File Encryption Devices to Media Encryption • 23
Creating a VPN Site • 31

D
Dangerous Site Messages • 30
Deleting Encrypted Files and Storage Devices • 21

E
Encrypting CDs and DVDs • 20
Encrypting Media • 19
Encrypting Media In Windows 7 • 21
Ensuring That No One Tampered with Your Computer • 26
Exporting Logs • 38

F
Firewall & Application Control • 24
Firewall and Application Control Blades • 10
Full Disk Encryption • 25
Full Disk Encryption Blade • 10

G
Getting Started • 6
Getting the Endpoint Security Installation • 7

I
If You Do Not Have Your Password • 27
Important Information • 3
Importing a Certificate into the CAPI Store • 34
Installing and Upgrading the Client • 7
Introduction to Endpoint Security • 6

M
Making Sure that the Client is Installed • 6
Media Encryption and Port Protection • 18
Media Encryption and Port Protection Alerts • 13
Media Encryption and Port Protection Blade • 9

N
New Application Alerts • 12
New Network and VPN Alerts • 13
Notification Area Icons and Options • 11

O
Overview of the Login Screen • 25

R
Remote Access VPN Blade • 10
Replacing the SAA DLL File • 35
Responding to Alerts • 12

S
Scanning • 16
Scanning Devices • 22
Secure Authentication API (SAA) • 35
Secure Domain Logon • 32
SecurID • 34
Suspicious Site Warnings • 28

T
Technical Difficulties • 37
Tools • 11
Tour of the Endpoint Security Main Page • 8
Troubleshooting • 37

U
Understanding Application Control • 24
Understanding Firewall Protection • 24
Understanding Scan Results • 16
Uninstalling other Anti-Virus Software • 15
Uninstalling the Endpoint Security Client • 14
Updating Anti-Malware • 16
Using Logs • 37
Using Media Encryption and Port Protection • 18
Using Special Characters • 26
Using the Client • 8
Using the Event Filter • 38
Using the Virtual Keyboard • 25

V
Viewing Quarantined Items • 17
VPN • 31
VPN Basics • 31
W
WebCheck • 28
WebCheck Blade • 10
WebCheck Protection • 28
What Can I do with Logs • 37

Y
Yellow Caution Banner • 29
Your Anti-malware Status • 15