Endpoint Security Client

R80.10

User Guide

7 February 2011

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

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=11941

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

Date	Description
2 February 2011	First release of this document

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 Client R80.10 User Guide).

Contents

Chapter 1

Introduction to Endpoint Security

Check Point Endpoint Security™ is the first and only single client that combines all essential components for total security on the endpoint. It includes these Software Blades: Firewall and Application Control, Malware Protection, Full Disk Encryption, Media Encryption and Port Protection, and VPN.

Check Point Endpoint Security protects PCs and eliminates the need to deploy and manage multiple agents.

In This Chapter

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 that you must follow to install the Endpoint Security Client on your machine depend on the administrator's choices.

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

Item	Description
	The Endpoint Security icon that appears in your taskbar notification area.
192.0.2.10	An example of an IP address that you might be told to connect to.

Checking if the Client is Installed

Your administrator might have installed 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 check your Endpoint Security status:

1. From the Endpoint Security icon in your taskbar notification area, right-click and select **Display Overview**.

   The Endpoint Security Main Page opens.

   Note - If you do not see the Endpoint Security icon in your taskbar notification area, expand the taskbar to show hidden icons. If you still do not see the Endpoint Security icon, you do not have the Client installed.

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 not you might need to **Connect** or follow instructions from your administrator.

Installing the Client

To install the Endpoint Security client on your computer:

1. Follow the instructions that your administrator sends you. You might have to install a package and restart at this point.

   The Endpoint Security icon appears in your taskbar notification area if it was not there already.
2. From the taskbar notification area icon, right-click and select **Connect** to connect to the Endpoint Security Management Server, if you are not already connected. You might have to enter an IP address that your administrator provides.
3. If a window with a fingerprint opens, click **Approve**.
4. You might have to download and install the client package at this point.
5. Follow the on-screen instructions to complete the installation and restart.

Using the Client

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

The client automatically connects to a server for updates according to the schedule set by your administrator. You can also update manually at any time by clicking **Update Now** from the Endpoint Security Main Page. During updates your computer might be slower than usual.

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. The Software Blades you see depend on the settings that your administrator defined.

- Click on a Software Blade to see the details.
- The top section shows if everything is compliant and updated or if any component needs attention. All status issues or necessary actions are shown there.
- The status of each component shows next to it.

Compliance Blade

Compliance Enforcement enables Endpoint Security client to protect your enterprise network by enforcing a security policy created by your administrator. In this way, your enterprise can be sure that everyone on the network is protected from Internet threats.

The display shows if you are compliant with the corporate security policy. The states of compliance that you might see are:

- **Compliant** - Computers that are running the correct types and versions of required software are compliant with enterprise security requirements.
- **Warn** - You are warned that your computer is not compliant with the enterprise security requirements. Your ability to access your corporate network does not change. Do the actions shown to become compliant.
- **Restricted** - Your computer is not compliant with the enterprise security requirements. Your ability to access your corporate network might be *restricted* or even *terminated*. Do the actions shown to become compliant.

Click for more information and the **Compliance Detail** pane opens. It includes:

- **Policy Details -** A summary of the Media Encryption and Port Protection policy that is installed on your computer.
- **Current Status** - A **Message** about each problem and a **Remedy** show in the table.

Anti-malware Blade

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

Click Anti-malware and the **Anti-malware Detail** pane opens. This pane includes:

- **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.
- **Current Status -** A summary of the Anti-malware status of your computer.
  - 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 after an update to your virus and spyware signature files.
  - 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. To enforce the Media Encryption and Port Protection, the blade can scan, encrypt, and decrypt the external devices. The display shows the status of external devices connected to your computer. Click and the **Media Encryption and Port Protection Detail** pane opens. This pane includes:

- **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.
  - **Access** - The level of access that you have to the device, either Read Only, Full Access, or No Access.
  - **Authorization Status** - The authorization status of the device based on an Anti-malware scan. If the device has any viruses or suspicious files, it is not authorized. If it is clean it is authorized. You cannot open, encrypt, or decrypt a device that is not authorized. The values can be Waiting for scan, Authorized, or not Authorized.
  - **Encryption Status** - If the device is encrypted or not. Encryption prevents anyone who does not have permissions from viewing files on the device.
- **Scan Device** - Scans the device for Anti-malware. If your Endpoint Security client does not have Anti-malware installed, the scan can run from other Anti-virus programs.
- **Create Encrypted Storage** - Click this to create an encrypted container on a device.
- **Remove Encryption** - Click this to remove encryption from a device.

Depending on the settings set by your administrator you might or might not have permissions to encrypt devices and remove encryption. Settings also determine if you can access encrypted devices on a computer that does not have Endpoint Security with Media Encryption and Port Protection.

For instructions on how to use Media Encryption and Port Protection, see Using Media Encryption and Port Protection (on page 48).

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** and the **Firewall and Application Control Detail** pane opens. This pane includes:

- **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 the Endpoint Security, you must enter a password to start your computer. Until you are authenticated, all information on the computer is encrypted.

Click and the **Full Disk Encryption Detail** pane opens. This pane includes:

- **Policy Details-** A summary of the Full Disk Encryption policy that is installed on your computer.
- **Current Status** - A summary of the Full Disk Encryption status of your computer.
  - **Encryption Status** - Shows the encryption status of components of your computer and devices connected to your computer. It also shows the size and available space for each device.
- **Advanced** - Shows additional 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-virus and firewall functionality, which protect against PC-based threats.

Click WebCheck and the **WebCheck Detail** pane opens. This pane includes:

- **Policy Details** - A summary of the WebCheck policy that is installed on your computer.
- **Current Status** - Shows statistics WebCheck activities including website blocked and threats stopped.
- **Trusted Domains** - Domains or sites that your administrator set as trusted. They are not checked by WebCheck.

VPN Blade

Endpoint Security VPN lets you connect securely to your enterprise network when working remotely. The display shows the state of the VPN (Connected, Disconnected, Connecting, or Disconnecting) and its default site.

Double-click to see more information and the **VPN Detail** pane opens. This pane includes:

- **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 the VPN will try to connect unless you change it.
  - **Gateway IP Address** - The IP address of the VPN site.
  - **Last time connected** - If you are disconnected, see the last time you were connected. This does now show if the VPN is connected.
- **Encryption Details** - How many packets and KB have been 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.
- **Advanced** - Click the links to see more options for connection details, managing settings, and registering to a hotspot. See the VPN section for more information.
  - For the Legacy VPN Client see Legacy VPN Client (on page 15).
  - For Endpoint Connect see Check Point Endpoint Connect VPN Client (on page 30).

Advanced

The **Advanced** page has these options:

- **View component version information** - Shows the versions of the various Endpoint Security Software Blades.
- **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 running in, either Connected or Disconnected.
- **Customize interface** - Lets you select the default action of the Endpoint Security notification area and the options that appear from it and in the Tools menu of the Endpoint Security Main Page.
- **View Logs** - Displays log of your Endpoint Security activity. Your administrator automatically sees this data also.
- **Collect information for technical support -** Collects additional information that Technical Support can use for troubleshooting.

Notification Area

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

Icon	Description
	VPN is connected.
	Security scan, encryption, or change in client settings is in progress.
	Action is necessary (for example: the client is out of compliance with policy, there is an application error, or a reboot is needed).

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.

Option	Description
Display Overview	Shows the Endpoint Security Main Page.
Connect	Connects to the VPN site that is configured.
Connect to	Lets you choose a VPN site to connect to.
Disconnect from VPN	Disconnects your VPN, if you are connected.
Scan Now	Runs the Anti-malware scan immediately.
Update Now	Gets any policy updates from your administrator immediately. This is generally not necessary because the Client automatically updates according to the schedule set by your administrator
Help	Opens the Endpoint Security Online Help.
About	Show the versions of the Endpoint Security components.

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.

Note - Select the **Remember this answer** check box to give permanent permission to programs you trust.

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 are seeing many server applications alerts, you may 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

Compliance alerts occur when there is a change in your computer's compliance with enterprise security requirements. If Endpoint Security determines that a computer is non-compliant, it:

- Shows a Compliance alert.
- Shows you what to do to become compliant.

What happens next depends on your company's security Policies.

- If you do not make your computer compliant in the time allotted by the security policy, your access to the corporate network might be *restricted* or *terminated.*
- If your computer is restricted, you can continue to access some corporate network resources before you perform the steps necessary to make your computer compliant.
- If your computer is terminated, you might only be able to access the instructions of how to make your computer compliant with corporate security requirements.

Full Disk Encryption Alerts

If you have the Full Disk Encryption blade as part of your Endpoint Security, you might see alerts related to Full Disk Encryption.

- When Full Disk Encryption is first installed or your administrator makes certain changes to its policy, you are told to restart you computer.
- If there is a problem with your username, you will not be able to log in to your computer and the computer might restart. In this situation, contact your Endpoint Security technical support.
- If the license for the Full Disk Encryption blade has expired, you see an alert and are not able to log in. In this situation, contact your Endpoint Security technical support.

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.

Chapter 2

VPN

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

In This Chapter

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.

Types of Endpoint Security VPNs

Your administrator has configured a VPN type for your client. It may be either:

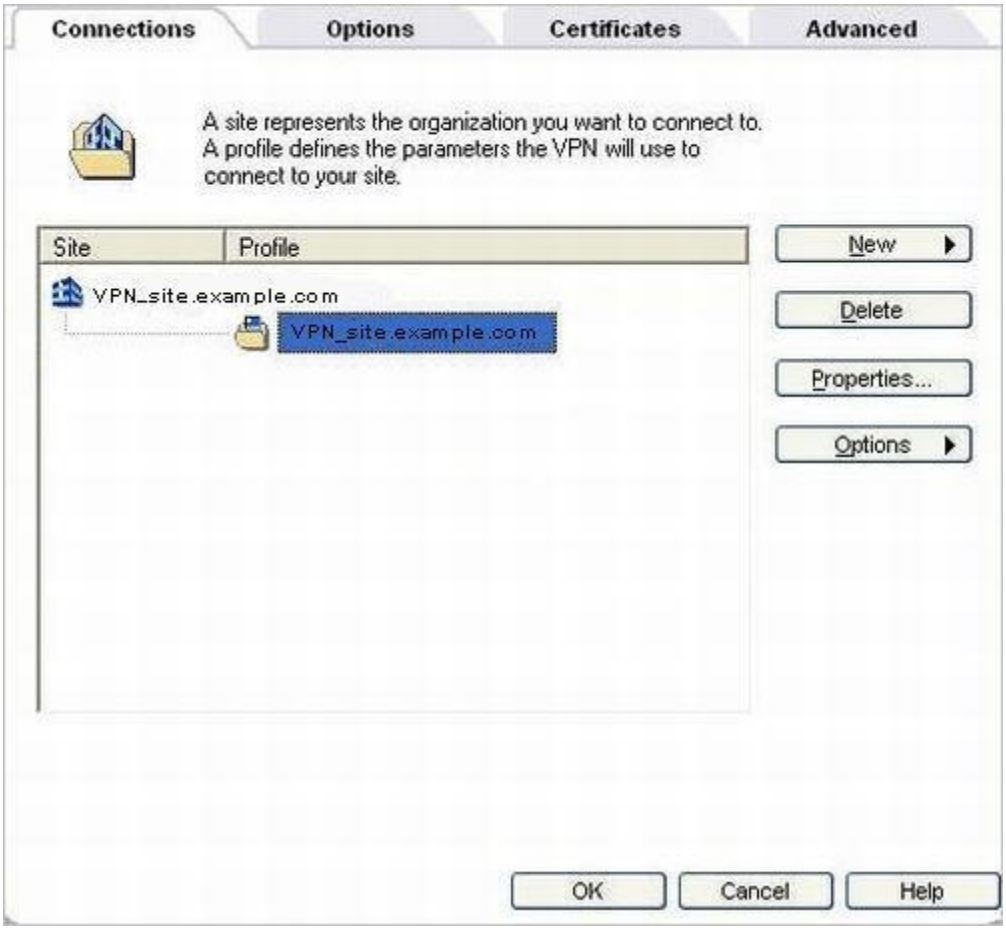
- Check Point Endpoint Connect or
- The Legacy Endpoint Security VPN (SecureClient).

The options that you have to choose from depend on which VPN is provided in your client.

To determine which VPN client you have:

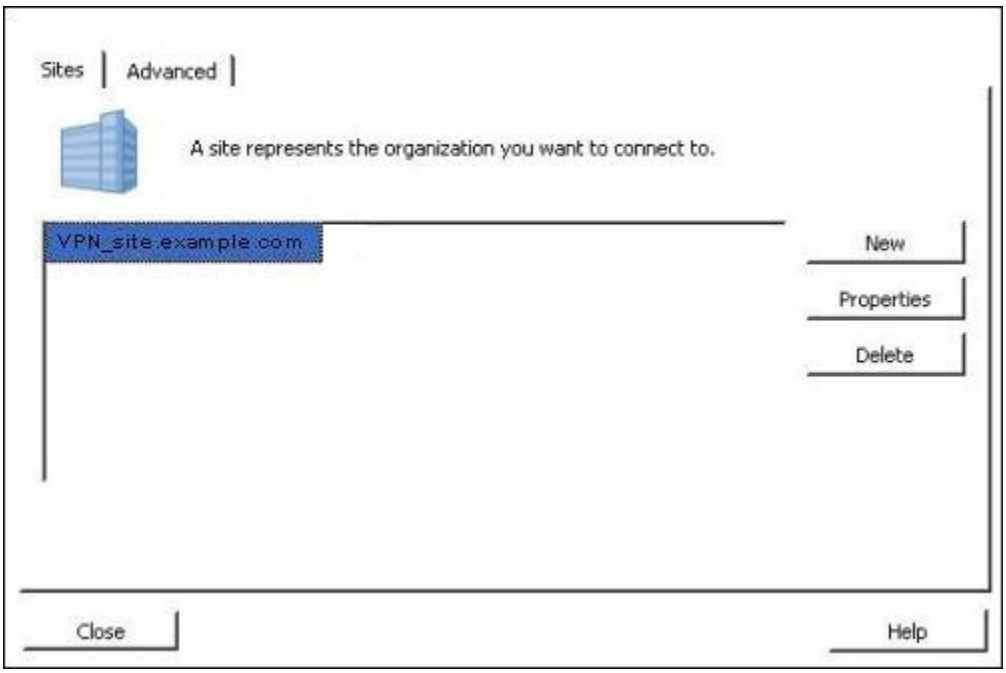
Open the main **VPN Detail** window and click **Manage Settings**.

- If you see four tabs, **Connections**, **Options**, **Certificates**, and **Advanced**, the VPN client is the legacy Check Point client. For managing options in this client, see Legacy VPN Client (on page 15)



- If you see only two tabs, one for **Sites** and one for **Advanced**, the VPN client is Check Point Endpoint Connect. For managing options in this client, see Check Point Endpoint Connect VPN Client (on page 30).

Figure 2-1 Endpoint connect VPN settings



Creating a VPN Site

You can configure multiple VPN sites.

To configure a VPN site:

1. If you do not have a VPN site configured, access the Site Wizard in one of these ways:
   - From the Endpoint Security Main Page, click **VPN**. From the **VPN Detail** page, click **Connect** or **Connect to**.
   - From the notification area icon, right click and select **Connect**.
2. Follow the instructions in the Site Wizard.
3. Enter a server address or name. The wizard might automatically detect a site that your administrator configured. You can leave this site or change it.
4. Select the **Display name** option and enter a name if you want to give the VPN site a description other than the actual server name. For example, you may want to call the site, "Corporate Headquarters".
5. Click **Next** and wait while the new site is created.
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 **VPN**. From the **VPN Detail** page, click **Connect to** or **Connect.**
- From the taskbar notification area icon, right click and select **Connect**.

Legacy VPN Client

This section covers the configuration options available for the legacy VPN Client.

Compact and Extended VPN Interfaces

If your Endpoint Security client is configured with a Legacy VPN, it is deployed with either a compact or an extended version of the VPN interface.

You can change versions yourself when the client is running.

Compact view provides a simplified view of the VPN interface for users who do not need multiple sites or profiles.

Extended view is for more advanced users who need to connect to different VPN sites and who want to manage their VPN configuration in greater detail.

To switch between extended and compact views:

1. If you are switching from extended to compact view, you must first:
   a) Delete all sites (see "Deleting Sites" on page 23).
   b) Disable **Auto Local Logon** (on page 26).
   c) Disable **Secure Domain Logon** (on page 26).
2. From the **VPN Details** page, click **Manage Settings**.
3. Open the **Advanced** tab.
4. In the Product View section, select **Extended View** or **Compact View** and click **OK**.
5. Click **OK** to confirm restart of VPN services.
   The VPN panel shows a message indicating that VPN services are restarting. When the VPN panel is restored it activates the selected view.

Authentication in the Legacy VPN Client

When you connect to a VPN site, and supply identification details, you are authenticating using credentials. There are many authentication methods available.

Contact your system administrator to send you one of the following:

- A registered certificate (on diskette, or a hardware token) and password (for opening the certificate)
- A registration code that allows you to complete the certificate creation process online.
- User name and password
- SecurID card
- SmartCard Response code

Changing Authentication Methods

Your administrator may ask you to change your VPN authentication method. If your laptop acts as a terminal for other users (each user connecting to the site with their own unique certificates), certificates should be switched as needed.

Note - You cannot change authentication methods while connected to a VPN site.

The procedure for changing authentication methods is varies according to the type of VPN that is configured for your client. Choose the instructions relevant to your client, according to the options that are available to you.

To change authentication methods:

1. If you are connected to a VPN site, click **Disconnect**.
2. From the **VPN Details** page, click **Manage Settings**.
3. Click **VPN Settings**.
4. In the **Connections** tab, select a site and click **Properties**.
5. Open the **Authentication** tab.
6. Choose an authentication method from the **Scheme** drop-down list.
7. Provide the information appropriate for your authentication method.
   For example, if you are using a certificate, click **Browse** and choose the certificate.
8. Click **OK**.

The first time that you configure a VPN, the same Scheme configuration option is provided, in the First Time Configuration - Authentication Method window. Select the authentication method from the **Scheme** drop-down list and then click **OK**.

Managing Certificates

It is recommended to use digital certificates for authentication when establishing a VPN connection. Certificates are more secure than other methods such as user name and password. When authenticating with certificates, the client and the VPN site each confirm that the other's certificate has been signed by a known and trusted certificate authority, and that it has not expired or been revoked.

You or your administrator must enroll with a certificate authority. You can use any third-party OPSEC (Open Platform for Security) PKI (Public Key Infrastructure) certificate authority that supports the PKCS#12, CAPI, or Entrust standards.

Endpoint Security client lets you create or renew Check Point certificates and manage Entrust certificates.

Managing Entrust Certificates

Endpoint Security client accommodates Entrust certificates. If desired, you can use Entrust Entelligence to create and recover certificates. When you use Entrust for certificate management, the client automatically connects to the Entelligence UI when appropriate.

Before you begin, make sure your administrator has given you a reference number and authorization code, which are required for completing the process.

To use an Entrust certificate for authentication:

First, enable Entrust Entelligence:

1. From the **VPN Details** page, click **Manage Settings**.
2. In the **Certificates** tab, clear the **Don't use Entrust Entelligence** checkbox.

Second, initiate the Entrust certificate:

1. In the **Certificates** tab, click **Select INI file**, browse to the `entrust.ini` file, and click **Open**.
   By default, the `entrust.ini` file is stored in your Windows directory (for example, C:\Windows).
2. Click **Configure INI file**. The Configure Entrust.INI window appears.
3. Provide the following information:
   - The CA manager's host name or IP address and its port number. The default port number is 709.
   - The LDAP Server's host name or IP address and its port number. The default port number is 389.
4. Click **OK**.

Third, create the Entrust certificate:

1. In the **Certificates** tab, Entrust Certificates section, click **Create**. The Create User window appears.
2. Click **Save to File**. Then browse to the directory in which to save the certificate.
3. Provide and confirm a password for your profile. Your password must conform to the following Entrust specifications:
   - At least eight characters long
   - At least one uppercase letter or a numerical digit
   - At least one lowercase letter
   - No long strings of repeating characters
   - No long substrings of the user name
4. Specify your profile parameters by entering the **Reference Number** and **Authorization code** supplied by your system administrator.
5. Click **OK**.
6. In the confirmation window that appears, click **OK** again.

Managing Check Point Certificates

Your system administrator might ask you to create a new Check Point certificate. You can store a Check Point certificate either as a Public-Key Cryptography Standard #12 (PKCS#12) file or as a hardware or software token (CAPI). Confirm with your system administrator how you should store the certificate.

Before you begin, obtain the following information from your administrator:

- the certificate format you should choose
- the certificate registration key
- the IP address (or host name) of the VPN gateway

Creating Check Point Certificate PKCS#12

If your system administrator has asked you to save the certificate in the PKCS#12 format, follow the instructions in this section.

To create a PKCS#12 file:

1. From the **VPN Details** page, click **Manage Settings**.
2. In the **Certificates** tab, click **Create Certificate**.
   The Check Point Certificate window appears.
3. Select **Store as a file (PKCS #12)**. and click **Next**.
4. Provide the connection site IP address or host name and the registration key. Click **Next**.
5. Provide and confirm a password for use with the certificate. Click **Next**.
6. In the confirmation window that appears, click **Finish**.

Creating Check Point Certificate CAPI Token

If your system administrator has asked you to save the certificate as a hardware or software token, follow the instructions in this section.

Before you begin, make sure your administrator has specified which Cryptographic Service Provider (CSP) to use. Some CSPs need special hardware (for example, a token reader/writer), while others do not. Endpoint Security works with the CSPs supported by Windows, and Check Point provides the Internal Certificate Authority (ICA) of the security gateway as a CSP.

To create a hardware or software token:

1. From the **VPN Details** page, click **Manage Settings**.
2. In the **Certificates** tab, click **Create Certificate**.
   The Check Point Certificate window appears.
3. Select **Store on a hardware or software token (CAPI)**. Click **Next**.
4. Select the Cryptographic Service Provider (CSP) for your certificate storage, and then click **Next**.

   Note - Each CSP uses its own unique configuration windows. For specific details, consult your CSP documentation.

5. Provide the connection site IP address or host name and the registration key. Click **Next**.
6. Click **Security Level**, select the level specified by your administrator, and click **Next**.
7. In the window that appears, click **Finish**.
8. Click **Yes**.
9. In the window that appears, click **Finish**.

Storing PKCS#12 in CAPI Store

If you are using the Check Point Internal Certificate Authority (ICA) of the security gateway as a CSP, you can use this procedure to store PKCS#12 files in the CAPI store.

To enter the PKCS#12 file into the CAPI store:

1. Double-click the file with the p12 extension.
   The certificate import wizard opens.
2. Click **Next**.
   The correct path to the file you wish to import is automatically shown:
3. Click **Next**, and enter the password for the private key.
   This is the key you obtained from your system administrator.
   - **Enable strong private key protection**: you will be prompted to enter the password each time the private key is used by the client.
   - **Mark this key exportable**: the key can be backed up or transported at a later time.
4. Click **Next**, and either allow the file to be automatically stored or browse to a specific storage folder.
5. Click **Finish** to complete the certificate import wizard.

Saving the Certificate in Another Location

You, or your administrator, may choose to not save your certificate to the CAPI store.

For example, if you use several desktop workstations and laptops, it is not recommended installing your certificate on all of them.

For this reason, your system administrator may switch from using the certificate stored in the CAPI and to require you to authenticate using a **PKCS#12** certificate directly, stored on a floppy disk or USB drive. If this happens, a message displays when you try to connect to the active site. Browse to the drive where the certificate is stored.

To save the certificate:

1. Save the **PKCS#12** certificate to a floppy or USB disk.
2. Configure the authentication scheme to use certificates (Properties window of site > **Authentication** tab).
3. From the **Certificate** drop-down list, select **From File**.
4. Browse to the certificates stored on a floppy or USB disk.
5. Enter the certificate's password.
6. Click **Connect**.

Renewing Check Point Certificates

Endpoint Security client automatically prompts you to renew your Check Point certificate shortly before it expires. You can also renew the certificate at any time.

To renew a certificate with VPN Settings (Legacy Endpoint Security VPN):

1. From the **VPN Details** page, click **Manage Settings**.
2. In the **Certificates** tab, click **Renew Certificate**.
   The client displays the Renew Check Point Certificate window automatically if your certificate is about to expire.
3. In the **Certificate** field, confirm the location of your current certificate or browse to the new location.
4. In the **Current password** field, provide the password to open the certificate.
5. Click **Next**.
   The Save Certificate window appears.
6. Confirm the certificate file name and location.
7. Provide the new password in the **Password** and **Confirm Password** fields.
   Your password should contain at least six characters, of which four must be unique.
8. Click **Next**.
   The Check Point Certificate window appears.
9. Click **Finish**.
   The client will use this renewed certificate the next time you authenticate to a site.

Creating Profiles and Sites in the Legacy VPN Client

A site represents the organization to which you want to connect. A profile defines the parameters the client will use to connect to your site.

Note - Profiles are supported by Legacy Endpoint Security VPN only.

Before Endpoint Security VPN connects to a site it needs to obtain information regarding the site's structure or Topology, such as the computers and servers available within the organization. The connection wizard gathers this site information. The initial connection, which is different from all subsequent connections, obtains the site's topology. During this process you are requested to authenticate either by supplying a certificate, or through some other means. If you are using certificates to authenticate yourself but have not received one from your system administrator, you will be asked to register. Registering a certificate means that you will complete a certificate creation process which was initiated by your system administrator.

The Settings window displays all your connection profiles, either those you created yourself or profiles created for you by your system administrator. Use this window to define your site and authentication methods.

Managing Connection Profiles

A connection profile defines the parameters the client uses to connect to your site. Most users need only one profile. However, if your network environment changes frequently (for example, if you sometimes connect from hotels or from a partner company's network), you or your system administrator might need to create several different profiles. Each profile connects to the site in a slightly different way, for example using Office mode or Hub mode. Endpoint Security client automatically downloads new profile information when you perform a site update. If you have more than one profile, contact your administrator to find out which one to use.

The functions described in this section are only available in extended view. (For details on compact versus extended view, see Compact and Extended VPN Interfaces (on page 15).)

Creating Profiles

If you are using VPN extended view, your system administrator might require you to create a new connection profile for a particular site. Note that you can only create a new connection profile if you have already defined at least one site.

To create a new connection profile:

1. Do one of the following:
   - From the **VPN Details** page, click **Manage Settings**.
   - Right-click or double-click on the system tray icon, select **Connect to VPN** and then click **Options.**
2. In the Connections tab, click **New** > **Profile**.
   The Profile Properties window opens.
3. Provide a profile name and description.
4. Select a site from the **Site** drop-down list.
5. Select a gateway from the **Gateway** drop-down list.
6. Open the **Advanced** tab, and select any configuration options specified by your administrator.
7. Click **OK** to close the Profile Properties window and then click **OK** to close the VPN Settings window.

Exporting and Importing Profiles

You can export (save) and import existing profiles. For example, your administrator can create a profile and you can import it.

To export a profile:

1. From the **VPN Details** page, click **Manage Settings**.
2. In the **Connections** tab, do one of the following:
   - Select the desired profile and then click **Options** > **Export Profile**.
   - Right-click the desired profile and select **Export Profile**.
   The profile is saved as a file with **srp** extension.

To import a profile:

Click **New** > **Import Profile**.

Cloning Profiles

You can clone profiles and then modify and save them as new profiles.

To clone a profile:

1. From the **VPN Details** page, click **Manage Settings**.
2. In the **Connections** tab, do one of the following:
   - Select the desired profile and then click **New** > **Clone Profile**.
   - Right-click the desired profile and select **Clone Profile**.
   The Profile Properties window appears.
3. Modify the profile properties as desired. For example, change the name, the description, or the gateway.
4. Click **OK**.

Changing Profiles

If you are using VPN extended view and if you have configured more than one profile, you can change the profile with which you connect.

Note - You cannot change profiles while connected a VPN site.

To switch profiles:

1. If you are connected to a VPN site, disconnect by doing one of the following:
   - Right-click the Endpoint Security system tray icon and select **Disconnect from VPN**.
   - Open **VPN** and click **Disconnect**.
2. Open the VPN Connection window by doing one of the following:
   - Right-click the Endpoint Security system tray icon and select **Connect to VPN**.
   - Open **VPN** and click **Connect**.
   The VPN Connection window opens.
3. In the Location Profile drop-down list, choose the desired profile.
4. Provide your password and click **Connect**.

The selected profile is now default.

Creating Profile Desktop Shortcut

You can create a desktop shortcut that brings up the VPN Connection window, configured to use your chosen profile. This works only for profiles that specify a particular gateway (as opposed to profiles that use the default, "Any Gateway").

To create a profile shortcut:

1. From the **VPN Details** page, click **Manage Settings**.
2. In the **Connections** tab, do one of the following:
   - Select the desired profile and then click **Options** → **Create Shortcut**.
   - Right-click the desired profile and select **Create Shortcut**.

   You can now double-click the shortcut on your desktop to initiate a VPN connection.

Viewing Profile Properties

The client displays profile properties in the Profile Properties window. This same window also appears when you start to clone a profile or create a new profile.

To view profile properties:

1. From the **VPN Details** page, click **Manage Settings**.
2. In the **Connections** tab, right-click the profile and choose **Properties**.

   The Profile Properties window appears.
3. Click a tab:
   - **General**: Shows the site name, site description, and gateway.
   - **Advanced**: Set Office Mode, connectivity enhancements, Visitor Mode, and Hub Mode.

Deleting Profiles

If you use VPN extended view, you can delete profiles when they are no longer useful.

Note - You can only delete a profile that you created; you cannot delete a profile provided by your network administrator.

To delete profiles

1. From the **VPN Details** page, click **Manage Settings**.
2. In the **Connections** tab, do one of the following:
   - Select a profile and then click **Delete**.
   - Right-click a profile and select **Delete Profile**.
3. In the confirmation window, click **Yes**.

Managing VPN Sites

Before you establish a VPN connection, you must define a site (a VPN server or device) to which the client connects. A site definition tells the client how to connect to the VPN site. During the initial connection, you must authenticate by supplying a certificate or authenticate through some other means. The client then obtains the site's structure (or topology). After the site is defined, VPN connections can be opened.

Defining Sites

If you have configured the client to display the extended version of the VPN interface, you can define additional sites as needed. Using the instructions in this section, follow the **Site Wizard** to define a new site.

Before defining a site, make sure your administrator gives you:

- Information about your method of authentication (user name and password, certificate, or similar). If you are planning to use a certificate for authentication, you should already have the certificate or received one from your administrator. See Managing Certificates (on page 16).
- The name or IP address of the security gateway that provides remote access to the corporate network.

Preparing:

If you are using Endpoint Security VPN functionality for the first time, and have not defined a site:

1. From the **VPN Details** page, **Connect**.
2. In the window that opens, click **Yes**.

If you have already defined a VPN destination site, and now want to define another:

1. From the **VPN Details** page, click **Manage Settings**.
2. Open the **Sites** tab.
3. Do one of the following:
   - If you are in extended view, click **New > Site**.
   - If you are in compact view, click **Define Server**.
   - If you are in the **Sites** tab, click **New**.

The Site Wizard opens.

To define a site:

1. Provide the VPN site IP address or host name.
2. Select **Display Name** and provide a display name.
3. Click **Next**.

   The client takes a moment to identify the site.
4. Select the method of authentication. The choices and subsequent actions are:
   - **User name and Password**: Click **Next** to advance to the User Details window. Enter your user name and password, and click **Next**.
   - **Certificate**: Click **Next** to advance to the Certificate Authentication window. Browse and select your certificate and then provide the certificate password. Click **Next**.
   - **SecurID**: Click **Next** to advance to the SecurID Authentication window. Choose **Use Key FOB hard token**, **Use PinPad card**, or **Use SecurID Software token**. Click **Next**. Provide the necessary information for your authentication type. Click **Next**.
   - **Challenge Response**: Click **Next** to advance to the Challenge Response window. Provide your user name and click **Next**.
5. If prompted, choose the desired connectivity setting (Standard or Advanced) and click **Next**.

   After a short wait, the Please Validate Site window displays your certificate's fingerprint and distinguished names (DN).

   If your administrator gave you the site's fingerprint and DN, compare them to those in the window. If they match, click **Next**.

   The Site Created Successfully window opens.
6. Click **Finish**.

Updating Sites

When you update a site, you download any new client settings and any updated information about the site and its associated profiles, including any new profiles your administrator has configured. To update a site, you must first be connected to the site. If you are not connected when you attempt to update, the client prompts you to connect.

To update a site:

1. From the **VPN Details** page, click **Manage Settings**.
2. In the **Connections** tab or **Sites** tab, select a site and click **Options** → **Update Site**.

   If you are already connected to the site, a progress window indicates when the update is complete.

   If you are not connected, the client prompts you to connect. You must do so to complete the update.

Viewing Site Properties

The client lets you view site properties, such as the site IP address and the authentication method. Information in the Site Properties window is divided into the following categories:

- **General**: Shows the site name, site IP address, and the last site update time.

- **Authentication:** View or modify the authentication method (see "Changing Authentication Methods" on page 16).
- **Advanced**: Enable the NAT-T protocol (see "NAT Traversal" on page 28).

To view site properties:

1. From the **VPN Details** page, click **Manage Settings**.
2. In the **Connections** tab or **Sites** tab, right-click the desired site (not the profile, but the site that holds the profile) and choose **Properties**.

   The Site Properties window appears.
3. Open **General**, **Authentication**, or **Advanced** tab.

Disabling Sites

You can disable a site, and then enable it later. Note that by disabling a site, you also disable all associated profiles.

To disable a site:

1. From the **VPN Details** page, click **Manage Settings**.
2. In the **Connections** tab, disconnect your VPN connection.
3. Do one of the following:
   - Select the desired site and then click **Options** → **Disable Site**.
   - Right-click the desired site and select **Disable Site**.

   A red "x" appears on the icons for the site and associated profiles indicating they are disabled.

To re-enable a site:

- Select the site and then click **Options > Enable Site**.
- Right-click the site and select **Enable Site**.

Deleting Sites

You can delete sites when they are no longer useful.

Important - If you delete a site, you also delete all associated profiles.

To delete sites:

1. From the **VPN Details** page, click **Manage Settings > Connections** tab.
2. Disconnect your VPN connection.
3. Do one of the following:
   - Select the site and then click **Delete**.
   - Right-click the site and select **Delete Site**.
4. In the confirmation window that appears, click **Yes**.

Connecting and Disconnecting Using the Legacy Client

This section explains how to connect to and then disconnect from a VPN site. The instructions assume you have already defined at least one site.

To connect to an existing site:

1. Right-click the Endpoint Security icon in the system tray and select **Connect**. Or in Endpoint Security go to the **VPN Detail page** and click **Connect**.

   The VPN Connection window opens. Depending on your authentication method, the window displays different fields. For example, if you authenticate using certificates, the certificate path is displayed and you are prompted to provide your password.
2. Provide the appropriate information and click **Connect**.

   Endpoint Security displays a window showing progress and whether the connection is successful.

To disconnect:

1. Do one of the following:

- Right-click the Endpoint Security icon in the system tray and select **Disconnect from VPN**.
- In Endpoint Security, open **VPN** → **Disconnect**.

A confirmation window appears.

2. Click **Yes**.

Connection Status

You can view different types of connection status information.

To view connection status information:

- Open **VPN**: View current connection status, active profile name, connection duration, and remaining time before re-authentication.
- Open **VPN > Activity**: View details about the compression and decompression of IP packets.
- Open **VPN** and click the **Connection Details link**: View connection details.

Understanding Connection Details - Legacy VPN

SecureClient (Legacy Check Point VPN) shows these categories of information about the current connection.

Information Type	Description
Status Summary	Client connection status, gateway IP address, current computer's IP address.
Connections	Name, IP address, site name, and tunnel properties of each available gateway. The active gateway is designated "(Primary)".
Gateway information	More Gateway information.
UDP Encapsulation	Enables Endpoint Security client to overcome problems created by a Hide NAT device.
Visitor Mode	Enables Endpoint Security client to connect through a gateway that limits connections to port 80 or 443.
Office Mode	Prevents IP address conflicts on remote networks by ensuring that the client receives a unique IP address from the gateway.
Tunnel Active	Indicates whether the VPN tunnel is open.
IP Compression	Indicates whether data is compressed for slow links, such as dialup.
IKE Over TCP	Indicates whether IKE negotiation is over TCP or not (if not, it is over UDP). Enable for complex IKE.
Tunnel MTU Properties	Current Maximum Transmission Unit (MTU). When the client is communicating across multiple routers with a site, it is the smallest MTU of all the routers that is important.
Computer	Current computer's connection status and other connection information.
Active Connection Settings	Summary of current profile, including: site to connect to, gateway hostname, protocol specifications.
Name	Name of the connection profile, as it appears in the VPN Connection window. It might be an IP Address.
Description	Descriptive name for the profile, showing additional information.
Site	Name of the site to connect to.

Information Type	Description
Profile Gateway	Name of the gateway specified in the connection profile.
Selected Gateway	Actual gateway chosen for the connection; may differ from the gateway defined in the connection profile.
Gateway defined in the connection profile	Name of the defined gateway.
Support Office mode	Indicates whether Office Mode is supported.
Support IKE over TCP	Indicates whether the tunnel negotiation is taking place over TCP instead of UDP to avoid packet fragmentation.
Force UDP Encapsulation	Indicates whether UDP encapsulation is being used to overcome problems created by hide NAT devices that do not support packet fragmentation.
Visitor Mode	Indicates whether Visitor Mode is active.
Route all traffic through gateway (Hub mode)	Indicates whether Hub Mode is active.
Tunnel MTU Discovery	Indicates whether the process that discovers the MTU from Endpoint Security to the gateway is active.

Enabling Logging

For trouble-shooting purposes, your system administrator may ask you to create a report log. The report log contains site-specific information and should be treated as strictly confidential. Send the report only to your system administrator or other authorized authority.

To enable logging:

1. From the **VPN Details** page, click **VPN Settings.**
2. In the **Advanced** tab, select **Enable Logging**.

To send logs:

1. In the **Advanced** tab, click **Save Logs**
   If a message appears (`Send this report only to your system administrator.`) click **OK**.
2. Wait while the logs are connected. A confirmation message will appear; click **OK**.
   The folder, where the logs are saved, opens.
3. Send the CAB or TGZ file to the administrator.

Configuring Connection Options

This section describes various connection and login options available to the legacy VPN Client.

Note - Auto-Connect, Secure Domain Logon, and Auto Local Logon are not available in the compact version of the VPN interface.

Auto-Connect

This option is available in Legacy Endpoint Security VPN only.

Auto-connect prompts you to establish a VPN connection when you first try to access a private network, such as the company intranet. This saves you the time of navigating through Endpoint Security and initiating the connection yourself.

In Auto-Connect mode, the client prompts you to establish a VPN connection every time it detects traffic destined for your corporate network or intranet site.

- If you choose to connect, the client encrypts traffic to the site.

- If you do not connect, the client prompts you to indicate how long to wait before reminding you again to connect. During this time, traffic to the site is sent unencrypted. However, if your site is configured to drop all unencrypted traffic, you will not be able to communicate with servers behind the site's gateway.
- If Office Mode is also enabled, you must re-initiate the connection after the Auto-Connect connection has succeeded.

To activate Auto-Connect:

1. Open **VPN** → **Main** and click **VPN Settings**.
2. In the **Options** tab, select the **Enable Auto-Connect** checkbox and click **OK**.
   The Enable Auto Connect window appears.
3. Select a re-launch option.
4. Click **OK**.

Secure Domain Logon

This option is available in Legacy Endpoint Security VPN only.

In a Windows environment, your account may belong to a domain controlled by a domain controller (a computer that provides Microsoft Active Directory service to network users and computers). Secure Domain Login (SDL) is useful when the domain controller lies behind your site's firewall.

When you try to establish a VPN connection to a Windows domain, the client sends your login credentials to the domain controller for verification. When you enable SDL, the client establishes the VPN connection *before* communicating with the domain controller.

To enable Secure Domain Logon:

1. Open **VPN** → **Main** and click **VPN Settings**.
2. In the **Options** tab, select **Enable Secure Domain Logon** and click **OK**.

Auto Local Logon

This option is available in Legacy Endpoint Security VPN only.

If you log in to the VPN site with a user name and password (as opposed to logging on with a certificate), you can enable Auto Local Logon to automate your login.

If you enable both Auto Local Logon and Auto-Connect, the client automatically establishes a VPN connection when you first try to access a site that requires encrypted communication (that is, traffic whose destination is the VPN site). This is useful for unattended computers that serve many end users as a terminal.

To enable Auto Local Logon:

1. Open **VPN > Main** and click **VPN Settings**.
2. In the **Options** tab, select **Enable Auto Local Logon** and click **Auto Local Logon Options**.
   The Auto Local Logon window appears.
3. Provide your Windows user name and password, and VPN user name and password and then click **OK**.
   A message displays stating that your change will be applied after the next reboot.
4. When the window closes, click **OK** to close the VPN Settings window.

Connecting Through a Hotspot

Your enterprise or disconnected policy may not automatically allow access to your network through a wireless hot-spot provided by a hotel or other public place. Your policy may allow you to partially override this restriction to register a hot-spot. This override is temporary, and has the following limitations:

- Only ports 80, 8080, and 443 are opened. These ports are commonly used for hot-spot registration.
- No more than five IP addresses are allowed while registering the hot-spot.
- Ports 80, 8080, and 443 are closed if any of these events occur:
  - The client successfully connects to the network
  - Ten minutes pass
  - Three connection attempts result in failure

To enable hot-spot registration:

1. Do one of the following:
   - Right-click the system tray icon and select **Register to Hotspot/Hotel**.
   - Open the Connect window and click **Options**, then select **Register to Hot Spot/Hotel**.

   A message appears, indicating the time period allowed for registration.
2. Connect to the Internet.

If the **Register to Hotspot/Hotel** option is not available, this feature has been disabled by your network administrator.

Enabling Office Mode

Office Mode causes the gateway to assign your computer a temporary IP address that does not to conflict with any other IP address at the site. The assignment is made after authentication and remains valid as long as you are connected. This feature overcomes certain connectivity issues.

Office Mode can be enabled through a profile that your administrator deploys to your client, or you can enable it manually.

To enable Office mode:

1. Open **VPN > Main** and click **VPN Settings**.
2. In the **Connections** tab, right-click the profile and choose **Properties**.

   The Profile Properties window appears.
3. Click the **Advanced** tab, select **Office Mode**, and click **OK**.

VPN Tunneling (Hub Mode)

Hub Mode enables Endpoint Security VPN to use the site's gateway as a router, thus making all the client's traffic available for content inspection, and introducing an extra layer of security. If your system administrator decides to use Hub Mode, you might be instructed to enable it manually.

To enable Hub mode:

1. Open **VPN > Main**.
2. If you see **VPN Settings** button:
   a) Click **VPN Settings**.
   b) In the **Connections** tab, select a profile and click **Properties**.
   c) Open the **Advanced** tab.
   d) Select **Route all traffic through gateway** and click **OK**.

Proxy Settings (Visitor Mode)

If you connect to the organization from a remote location such as hotel or the offices of a customer, Internet connectivity may be limited to web browsing using the standard ports designated for HTTP, typically port 80 for HTTP and port 443 for HTTPS. The remote client needs to perform an IKE negotiation on port 500 or send IPSec packets (instead of the usual TCP packets); therefore, a VPN tunnel cannot be established in the usual way. This issue is resolved using Visitor Mode (also known as *TCP Tunneling*), through a proxy server.

Before you configure proxy settings, contact your system administrator for a valid user name and password to use to access the proxy. You may also need the proxy server IP address and port number.

To configure proxy settings:

1. From the **VPN Details** page, click **VPN Settings**
2. On the **Options** tab, click **Configure Proxy Settings**.
3. Configure proxy settings.
   - **No proxy / transparent proxy**: Default.
   - **Detect proxy from Internet Explorer settings**: Client takes proxy settings from Microsoft Internet Explorer. Before selecting this setting, make sure the settings are defined manually: in Microsoft Internet Explorer, Tools > Internet options > Connections tab > LAN Settings, select "Use a proxy server for this connection". If the "Automatically detect settings" option or the "Use automatic

configuration script" option is selected, the client will not be able to detect the proxy settings from Microsoft Internet Explorer.

- **Manually define proxy**: If the proxy's settings cannot be automatically detected, you may be required to configure the Microsoft Internet Explorer settings according to the instructions, IP address, and port number provided by your system administrator.

4. In the Proxy Authentication section, provide the user name and password for proxy authentication.
5. Click **OK**.

Dial Up Support

The option to configure and use dialup connections through Endpoint Security is available if you have the Endpoint Connect VPN client.

If no network is available when you try to connect to a site, and no dialup connection has been configured, the Endpoint Connect client displays a message:

```
Connection Failed
No network detected
Click here to activate dialup
```

- Click the link to open the New Connection Wizard and configure a dialup connection.
- If a single dialup connection is already defined, click the link to dial and connect.
- If multiple dialup connections are defined, a list is displayed. Choose a connection and Endpoint Connect dials it.
- If Transparent Network and Interface Roaming is enabled, and the VPN is in the Reconnecting state, Endpoint Connect displays a `Reconnecting` message with the link to activate dialup.

Advanced Configuration Options in the Legacy Client

If you are using the extended version of the VPN interface, the client provides the advanced configuration options.

Suspending Popup Messages

When Endpoint Security VPN is disconnected from the site, and Auto-Connect is enabled, every time Endpoint Security VPN detects traffic destined for the site, a popup message prompts you to connect. Clicking inside this message displays the **Suspend Popup** message. Clicking **Cancel** will display an option suspending pop-up messages.

If you choose to suspend popup messages, for example for sixty minutes, then during those sixty minutes all traffic to the site is either dropped or sent unencrypted. When the sixty minutes expires, you are once again prompted to connect each time Endpoint Security VPN detects traffic destined for the site.

NAT Traversal

To use NAT (Network Address Translation) with VPN, you need to configure your VPN client to support NAT-T. You must do this in cooperation with the administrator of the firewall gateway, as NAT-T ports and options must be configured in both your client and the gateway to support each other.

To enable Connectivity Enhancements

1. Open **VPN** → **Main** and click **VPN Settings**.
2. In the **Connections** tab, right-click the profile and choose **Properties**.

   The Profile Properties window appears.
3. On the **Advanced** tab, select **Use NAT-T Traversal Tunneling** and configure:
   - **IKE over TCP**: Solves the problem of large UDP packets created during IKE phase I, by using TCP packets. This option is relevant if the VPN uses IKE protocols. The administrator must enable support of IKE over TCP.
   - **Force UDP Encapsulation**: Solves the problem of large UDP packets by wrapping them in IPSec headers. The administrator must enable port 2746 for source and destination.
4. Click **OK**.

To use NAT (Network Address Translation) with VPN, you need to configure your VPN client to support NAT-T. Do this with your system administrator. NAT-T ports and options must be configured in both your client and the gateway to support each other.

To enable NAT-T:

1. Open **VPN** → **Main** and click **VPN Settings**.
2. Select the **Site** and click **Properties**.
3. On the **Advanced** tab, select **Enable NAT-T** protocol.

   Note - Enable NAT-T should be the default option.

4. Click **OK**.

Switching to Endpoint Connect

There may be occasions when your site administrator requests you to switch from the Legacy VPN client to Endpoint Connect. The administrator will provide the command line tool called: `changeVPN.exe`.

1. Copy `changeVPN.exe` to a folder on your local machine.
2. Open a command prompt:

   Start > Run > enter `cmd`
3. Change directory to the folder where you saved `changeVPN.exe`
4. Run:

   ```
   ChangeVPN EPC
   ```

   Executing this command terminates existing VPN connections, and prevents additional connections until the client machine is rebooted.
5. Reboot the client machine.

Command Line Options

Command	Explanation
SCC	VPN commands executed on SecureClient are used to generate status information, stop and start services, or connect to defined sites using specific user profiles.
scc connect	Connects to the site using the specified profile, and waits for the connection to be established. In other words, the OS does not put this command into the background and executes the next command in the queue.
scc connectnowait	Connects asynchronously to the site using the specified profile. This means, the OS moves onto the next command in the queue and this command is run in the background.
scc disconnect	Disconnects from the site using a specific profile.
scc erasecreds	Unsets authorization credentials.
scc listprofiles	Lists all profiles.
scc numprofiles	Displays the number of profiles.
scc restartsc	Restarts SecureClient services.
scc passcert	Sets the user's authentication credentials when authentication is performed using certificates.
scc setmode <mode>	Switches the SecuRemote/SecureClient mode.

Command	Explanation
scc setpolicy	Enables or disables the current default security policy.
scc sp	Displays the current default security policy.
scc startsc	Starts SecureClient services.
scc status	Displays the connection status.
scc stopsc	Stops SecureClient services.
scc suppressdialogs	Enables or suppresses dialog popups. By default, suppress dialogs is off.
scc userpass	Sets the user's authentication credentials -- username, and password.
scc ver	Displays the current SecureClient version.
scc icacertenroll	Enrolls a certificate with the internal CA, and currently receives 4 parameters - site, registration key, filename and password. Currently the command only supports the creation of p12 files.
scc sethotspotreg	Enables HotSpot/Hotel registration support.

Check Point Endpoint Connect VPN Client

This section covers the configuration options available for Check Point Endpoint Connect.

Authentication in Endpoint Connect

This section covers authentication and credential management in the Check Point Endpoint Connect VPN client.

User Name and Password

User name and password is the simplest form of authentication. Together with your system administrator, decide on an appropriate user name and password. Strong passwords:

- Are lengthy

  A 15-character password composed of random letters and numbers is much more secure than an 8-character password composed of characters taken from the entire keyboard. Each character that you add to the password increases the protection that the password provides.
- Combine letters, numbers, and symbols

  A mixture of upper and lower case letters, numbers, and symbols (including punctuation marks not on the upper row of the keyboard).
- Avoid sequences or repeated characters

  For example 12345, or aaaaa.
- Avoid look-alike substitutions of numbers or characters

  For example replacing the letter "i" with the number "1", or zero with the letter "o".
- Avoid your login name
- Avoid dictionary words in any language

These authentication credentials are stored either in the security server database, on an LDAP or RADIUS server.

Understanding Certificates

A certificate is the digital equivalent of an ID card issued by a trusted third party known as a Certification Authority (CA). While there are well known external CAs such as *VeriSign* and *Entrust*, Endpoint Connect typically uses the digital certificates issued by the site's security gateway, which has its own Internal Certificate Authority (ICA). The digital certificate used by Endpoint Connect contains:

- Your name
- A serial number
- Expiration dates
- A copy of the certificate holder's public key (used for encrypting messages and digital signatures)
- The digital signature of the certificate-issuing authority, in this instance the ICA, so that the security gateway can verify that the certificate is real and (if real) still valid.
- A certificate is a file in the PKCS#12 format with the **.p12** extension.

Certificates can be supplied by your system administrator, or you can get them through the enrollment and renewal process ("Certificate Enrollment and Renewal" on page 33).

Certificates can be imported to the CAPI store or saved to a folder.

Storing a Certificate in the CAPI Store

By means of a Windows software library that implements the Microsoft Cryptographic Application Programming Interface (CAPI), Check Point certificates for Endpoint Connect are stored as either hardware or software tokens. A token is a complex string of numbers used for authentication and encryption. CAPI enables Windows-based applications such as Endpoint Connect to perform secure, cryptographic operations.

Controlled by the Windows operating system, the CAPI *store* is a repository of digital certificates associated with a given Cryptographic Service Provider (CSP). CAPI oversees the certificates, while each CSP controls the cryptographic keys belonging to the certificates. For Endpoint Connect, the CPS is the Internal Certificate Authority (ICA) of the security gateway.

If you are using certificates for authentication, your system administrator will supply (out of band) a file with a P12 extension. This is a **PKCS#12** file, a format commonly used to store private encryption keys. The PKCS#12 file is password protected. The password will have been set by your system administrator. Once you have this password from your system administrator, you can enter your certificate into the CAPI store.

To enter the PKCS#12 file into the CAPI store:

1. Double-click the file with the p12 extension.
   The certificate import wizard opens.
2. Click **Next**.
   The correct path to the file you wish to import is automatically shown:
3. Click **Next**, and enter the password for the private key.
   This is the key you obtained from your system administrator. If you:
   - **Enable strong private key protection** you will be prompted to enter the password each time the private key is used by the client.
   - **Mark this key exportable**, the key can be backed up or transported at a later time.
4. Click **Next**, and either allow the file to be automatically stored or browse to a specific storage folder.
5. Click **Finish** to complete the certificate import wizard.

Saving the Certificate to a Folder of Your Choice

If you do not wish to save your certificate to the CAPI store, for example you use several desktop workstations and laptops and for security reasons do not wish to leave your certificate on different machines, then save the **PKCS#12** certificate to a floppy or USB disk. Then:

1. Configure the client to use certificates for authentication ("Changing Authentication Schemes" on page 33).
2. From the drop-down **Certificate** box, select **From File**.
3. In the **From File** area, browse to the certificates stored on a floppy or USB disk.
4. Enter the certificate's password.

5. Click **Connect**.

Note - If you have the **Always-Connect** option configured, then each time the client loses communication with the site, you will be prompted to enter the certificate's password.

Another advantage of not having the **PKCS#12** certificate in the CAPI store is that, if someone steals your laptop, they will not be able to use the client to connect to the site without knowing the password—even if they have the **PKCS#12**. For this reason, your system administrator may switch from using the certificate stored in the CAPI and to require you to authenticate using the **PKCS#12** certificate directly. If this happens, a message displays when you try to connect to the active site. Browse to the folder where the certificate is stored.

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) using a built-in clock and an encoded random key.

The most typical 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 has *no* 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 (on page 32).

Endpoint Connect uses both the PIN and tokencode or just the passcode to authenticate to the security gateway.

SecurID Authentication Devices

Several versions of SecurID devices are available. The older format is a small device that displays a numeric code (*tokencode*) and time bars. The token code changes every sixty seconds, and provides the basis for authentication. To authenticate, the user must add to the beginning of the tokencode a special PIN (Personal Identification Number). The time bar indicates how much time is left before the next tokencode is generated. The remote user is requested to enter both the PIN number and tokencode into the Client's main connection window.

The newer format resembles a credit card, and displays the tokencode, time bars and a numeric pad for typing in the PIN number. These type of devices mix the tokencode with the entered PIN number to create a *Passcode*. SecureClient requests only the passcode.

SoftID

SoftID operates the same as a passcode device but consists only of software that sits on the desktop.

The **Advanced** view displays the tokencode and passcode with COPY buttons, allowing the user to cut and paste between softID and the VPN client.

Key Fobs

A small hardware device with built-in authentication mechanisms that control access to network services and information is known as a *key fob*. While a password can be stolen without the owner's knowledge, a missing key fob is immediately apparent. Key fobs provide the same two-factor authentication as other SecurID devices: the user has a personal identification number (PIN), which authenticates them as the device's owner; after the user correctly enters their PIN, the device displays a number which allows them to log on to the network. The SecurID SID700 Key Fob is a typical example of such a device:

When the Endpoint connect window opens for a user that has identified securID as the preferred method of authentication, a field for the PIN opens.

Challenge Response

Challenge-response is an authentication protocol in which one party presents a question (the challenge) and another party provides an answer (the response). For authentication to take place, a valid answer must be provided to the question. Security systems that rely on smart cards are based on challenge-response.

Changing Authentication Schemes

To change the authentication scheme used by the client for a specific site:

1. In the **VPN** window, click **VPN Settings**.
   The **Options** window opens
2. On the **Site** tab, select the relevant site and click **Properties**.
   The **Properties** window for that site opens.
   On the **Settings** tab, use the drop-down **Authentication Method** box to either:
   a) Username and password
   b) Certificate - CAPI
   c) Certificate - P12
   d) SecurID - Keyfob
   e) SecurID - PinPad
   f) SecurID - Software token (SoftID)
   g) Challenge Response

Certificate Enrollment and Renewal

Enrollment refers to the process of applying for and receiving a certificate from a recognized Certificate Authority (CA), in this case Check Point's Internal CA. In the enrollment process, your system administrator creates a certificate and sends you the certificate's registration key. The client sends this key to gateway, and in return receives the certificate, either CAPI or PCKS#12, which is saved or stored ("Storing a Certificate in the CAPI Store" on page 31).

You can enroll either when creating a site or after a site is created.

Enrolling During Site Creation

To enroll for a certificate while creating a site:

1. Open the **VPN** panel > open **VPN Settings**
2. On the **Sites** tab, click **New**.
   The Site wizard opens.
   Follow the wizard until you reach the Certificate Authentication window
3. Select **Check this if you don't have a certificate yet (only works with ICA certificates)**.
4. Click **Next**.
   When the **Site Created Successfully Message** appears, click **Finish**.
5. When asked if you would like to create a certificate now, click **Yes**.
   The client's enrollment window opens, either for CAPI or PCKS#12.
6. Enter the required authentication details, such as the registration key, and click **Enroll**.
   - If you have a PCKS#12 certificate, the **SAVE AS** window opens. Save the certificate to an appropriate directory.
     (i) You are asked if you want to connect. Click **Yes**.
     (ii) When the main connection window opens, browse to the location of your PCKS#12 certificate.
   - CAPI certificates are automatically entered into the CAPI store.
     (i) The RSA window opens.
     (ii) Click **OK**.

   The certificate will be a protected item. Each time the client uses the certificate, you will be required to manually grant permission.
7. The **Enrollment** window opens.
8. When prompted, add the certificate to the root store.
9. After the Enrollment succeeded message, the connection window opens with the certificate selected.
10. Click **Connect**.

Automatic Certificate Renewal

When using certificates for authentication, each time you connect to the site, the client checks to see how close the certificate is to its expiration date. If necessary, and simultaneously with the connect process, the certificate is renewed. A message balloon appears in the system tray: **Certificate renewal in progress**.

Certificate Renewal

A certificate can be renewed at any time.

To renew a certificate:

1. In the VPN window, click **VPN Settings.**
2. Select the site and click **Properties.**
3. Click **Renew**.

   The authentication window opens.
4. Using the drop-down box, select your certificate.
5. When prompted, grant access to the protected item (your certificate).
6. Wait while the certificate is renewed.

A **Renewal Succeeded** message appears, followed by the connection window.

Creating Sites in Endpoint Connect

To create a site:

1. From your system administrator, obtain the name or IP address of the security gateway that provides remote access to the corporate network.
2. Right-click the client icon in the system tray, and select **Settings**.
3. In the VPN window, click **VPN Settings**

   The **Options** window opens:
4. On the **Sites** tab, click **New**.

   The Site Wizard opens:
5. Enter the name or IP address of the security gateway, and click **Next**.

   The **Authentication Method** window opens.
6. Select an authentication method, and click **Next**.

   If **Certificate** is your preferred method of authentication, when you click **Next** the **Certificate authentication** window opens.

   Select whether to use a **PKCS#12** certificate stored in a folder, or a **PKCS#12** that has been entered into the CAPI store.
   - See Understanding Certificates (on page 31) for more information.
   - See Certificate Enrollment and Renewal (on page 33) if you do not have a certificate and wish to obtain one.
7. Click **Next**.

   The digital fingerprint, a way for the site to authenticate itself to the client, appears.

   This digital fingerprint is kept in the Windows registry and not displayed again — even if the client is upgraded.
8. Click **Yes**, and wait until the **Site created successfully** message appears.
9. Click **Finish**.
10. When asked if you would like to connect, click **yes**.

    The main connection window opens.
11. Enter your authentication credentials, and click **Connect**.

    The client connection window opens. If your system Administrator has configured Endpoint Security on Demand (ESOD):
    - A compliance check runs to determine whether your desktop is secured by anti virus software, the presence of a firewall, recommended and relevant software updates.
    - If your desktop or laptop fails the initial compliance check, a report is displayed that contains links to online remediation sources. Follow the links to correct the problems discovered by the endpoint security check, then try to connect again through the main connection window.

12. The connection status window opens.
    When the "connection succeeded" message displays, click **Hide**. The client is now connected.

Connecting and Disconnecting Using Endpoint Connect

Connecting to a Site

To connect to a newly created or existing site:

1. Right-click the client icon in the system tray, and select **Settings**.
2. In the **VPN** window, click **Quick Connect** or **Connect**
   The Connection window opens:
3. Enter your authentication credentials.
   If you are using a certificate, the last certificate is automatically selected.
4. Click **Connect**.
   The Connection Status window displays:
   During this time:
   - You are authenticated using your chosen method
   - Network topology information is downloaded from the gateway to your local client
   - Virtual network adapters are loaded

If configured by the site administrator, an Endpoint Compliance check is run.

Alternative Ways of Connecting

Endpoint Connect offers two alternative ways of connecting.

- Right-click the client icon in the system tray, and select **Quick Connect**
  - Endpoint Connect connects directly to the last active site.
  - A tool tip appears when the connection is established.
- Right-click the client icon in the system tray, select **Connect**.

Understanding Connection Settings - Endpoint Connect VPN

Settings Tab	Description
Always Connect	If you client is configured to allow you to change this option, select **Enable Always Connect** to automatically connect to the active VPN whenever possible.
VPN Tunneling	If you client is configured to allow you to change this option, select **Encrypt all traffic and route to gateway** to use the VPN tunneling functionality for all traffic going from this client.
Authentication	Select the authentication method from the drop-down list.

Disconnecting from a Site

To disconnect from a site:

1. Right-click the client icon in the system tray.
2. Click **Disconnect from VPN.**
   A tooltip appears above the system tray informing you that the client is disconnected.

Password Caching for Single Sign On

Providing that your site administrator has enabled password caching, then Endpoint client remembers any password you entered during the last authenticated/successful connect operation. For example if you use username/password as your authentication scheme, or enter the password to your p12 certificate.

- This password is held only in memory and deleted once you explicitly disconnect from a site.
- If, for example, location awareness is enabled, then as the client automatically reconnects to the site, the password is supplied transparently from cache.
- If you see the password field already populated when you attempt to connect to a site, this means that the cached credentials will be used. If necessary, you can override them and enter new credentials.

Note - If the Full Disk Encryption blade is installed on your client with OneCheck enabled, then the password caching functions differently.

Configuring Connection Options

This section describes various connection and login options available for Check Point Endpoint Connect.

Staying Connected all the Time

To ensure that you remain connected to the active site:

1. Right-click the client icon in the system tray and select **Settings**.
2. From the **VPN Details** page, select **VPN Settings**.
   The **Options** window opens.
3. On the **Sites** tab, select the site to which you wish to remain connected, and click **Properties**.
   The **Properties** window for the site opens.
4. In the **Always-Connect** area of the window, select **Enable Always-Connect**.

Location Aware Connectivity

Endpoint Connect intelligently detects whether it is inside or outside of the VPN domain (Enterprise LAN), and automatically connects or disconnects as required. When the client is detected within the internal network, the VPN connection is terminated. If the client is in **Always-Connect** mode, the VPN connection is established again when the client exits.

Connecting Through a Hotspot

Hotspot Detection

For wireless connections, Endpoint Connect might automatically detect the presence of a hotspot if this is configured by your administrator. When connecting for the first time through the hotspot server:

1. The connection naturally fails because no registration details have been presented.
2. The client automatically opens its internal browser window showing the hotspot registration form.
3. Enter the relevant authentication and payment credentials.
   The client automatically detects when the form is submitted and immediately connects to the site.

Proxy Settings

From time to time you may need to change your proxy server settings.

To change the proxy settings for Endpoint Connect:

1. Right-click the client icon in the system tray and select **Settings**.
2. In the **VPN** window, select **VPN Settings**.
   The **Options** window opens.
3. Click the **Advanced** tab and select **Proxy Settings**.
   The **Proxy Settings** window opens.
4. Configure your **Proxy Definition** and **Proxy Authentication** credentials according to the new settings.
   - **No proxy/transparent proxy**: No proxy is defined.
   - **Detect proxy from Internet Explorer settings**: This is the default setting. The client takes proxy settings from Microsoft Internet Explorer. Before selecting this setting, verify that the proxy settings are defined manually:
     - In Microsoft Internet Explorer, open **Tools > Internet Options > Connections tab > LAN Settings**, then select **Use a proxy server for this connection**.
   - **Manually define proxy**: You may be required to configure the proxy settings manually. In Microsoft Internet Explorer, open **Tools > Internet Options > Connections tab > LAN Settings**, then select

Use a proxy server for this connection. Your administrator can provide the IP address and port number.

5. In the **Proxy Authentication** section, provide the user name and password for proxy authentication.

VPN Tunneling (Hub Mode)

A VPN tunnel is an encrypted channel that provides secure access to the active site. To configure VPN Tunnel settings:

1. Right-click the client icon in the system tray and select **Settings**.
2. In the **VPN** window, select **VPN Settings**.
   The **Options** window opens.
3. On the **Sites** tab, select the site to which you wish to remain connected, and click **Properties**.
   The **Properties** window for the site opens.
4. In the **VPN tunneling** area of the window, select **Encrypt all traffic and route to gateway**.
   - If you select **Encrypt all traffic and route to gateway**, all outbound traffic on the client is encrypted and sent to the security gateway but only traffic directed at site resources passes through the gateway. All other traffic is dropped.
   - If you do *not* select **Encrypt all traffic and route to gateway**, only traffic directed at site resources is encrypted and sent to the gateway. All other outbound client traffic passes in the clear.

Dial Up Support

Endpoint Connect supports dialup connections for a number of scenarios:

- If no network is available when you try to connect to a site, and no dialup connection has been configured, the client displays a connection failed message:

  ```
  Connection Failed
  No network detected
  Click here to activate dialup
  ```

  - Click the link to configure a dialup connection.
  - The link opens the New Connection Wizard. Complete the wizard to configure a dialup connection.
- If a single dialup connection is already defined, then clicking the **activate dialup** link instructs the client to dial it.
- If more than a single dialup connection is configured, then choose which connection to choose from the displayed list.
- If *Transparent Network and Interface Roaming* is enabled, and the client is in a state of "reconnecting", the option to configure a dialup connection is displayed.

Smart Card Removal

If you are authenticating using a Smart Card, and the smart card or smart reader is removed from the USB port, the client detects that the certificate is no longer available and disconnects from the site. A **VPN tunnel has disconnected. Smart card was removed** message is displayed.

Tunnel Idleness

If you see a **VPN tunnel has disconnected. Tunnel inactivity timeout reached** message, this means that no traffic has passed between you and the site during a period set in minutes by your system administrator.

Your organization may have specific security requirements, such that an open VPN tunnel should be transporting work-related traffic to the site at all times. An idle or inactive tunnel should be shut down.

A mail program such as OUTLOOK performing a send-receive operation every five minutes would be considered work-related, and the tunnel kept open.

Advanced Configuration Options in Endpoint Connect

Command Line Options

The Endpoint Connect can also be run from the command line. The client has a number of command line options of the type: `command_line <command>[<args>].`

To use the command line:

1. Open a command prompt.
   Start > Run >enter: `cmd`
2. Browse to the Endpoint Connect directory:
   `C:\Program Files\CheckPoint\TRAC`
3. Enter `command_line <command> [<args>]`:
   Where <`command`> is one of the following:

Command	Function
Start	Starts the Endpoint Connect service
Stop	Stops the Endpoint Connect service
Status	Prints status information and lists current connections
info [-s <site name>]	Lists all connections or prints site name information
connect -s <sitename> [-u <username> -p <password> | -d <dn> | -f <p12> | -pin <PIN> -sn <serial>]	Connects using the given connection. • <sitename> parameter is optional. If no site is defined, the client connects to the active site. If no active site is defined, an error message appears. • Optional credentials can be supplied.
disconnect	Disconnects the current connection
create -s <sitename> [-a <authentication method>]	Creates a new connection, and defines an authentication method. Valid authentication values are: • username-password • certificate • p12-certificate • challenge-response • securIDKeyFob • securIDPinPad • SoftID **Note -** An administrator can specify a particular authentication method. If the wrong method is entered, you will be prompted to enter an alternative.
delete -s <site name>	Deletes the given connection
help / h	Shows how to use the command
list	Lists user Domain Names stored in the CAPI
ver	Prints the version
log	Prints log messages
enroll_p12 -s <sitename> -f <filename> -p <password> -r <registrationkey> [-l <keylength>]	Enroll a p12 certificate
renew_p12 -s <sitename> -f <filename> -p <password> [-l <keylength>]	Renews a p12 certificate

Command	Function
enroll_capi -s <sitename> -r <registrationkey> [-i <providerindex> -l <keylength> -sp <strongkeyprotection>]	Enroll a capi certificate
renew_capi -s <sitename> -d <dn> [-l <keylength> -sp <strongkeyprotection>]	Renew a capi certificate
change_p12_pwd -f <filename> [-o <oldpassword> -n <newpassword>]	Change p12 password

Collecting and Sending Log files

To troubleshoot unforeseen issues with the Endpoint Connect, your system administrator may ask you to send log files. Before you can collect and send log files, logging must be enabled.

To enable Logging:

1. Right-click the client icon in the system tray and select **Settings**.
2. In the **VPN** window, select **VPN Settings**.
   The **Options** window opens.
3. On the **Advanced** tab, select **Enable logging**.

To send log files:

1. Right-click the client icon in the system tray and select **Settings**.
2. In the **VPN** window, select **VPN Settings**.
   The **Options** window opens.
3. On the **Advanced** tab, click **Collect Logs**.
   - If your system administrator has preconfigured an email address for the logs, your default email program opens with the address already entered and the logs attached as a single compressed file.
   - If no email address has been configured, the log files are gathered into a single compressed file which you can save.
4. Send the contents of the compressed file to your site administrator.

Switching to the Legacy VPN client

There may be occasions when your site administrator requests you to switch from Endpoint Connect to the Legacy VPN client. For example to take advantage of legacy client features such as:

- Link Selection
- Secondary Connect
- Multiple Entry Points (MEP)
- SAA Authentication

The administrator will provide the command line tool called: **changeVPN.exe**.

1. Copy **changeVPN.exe** to a folder on your local machine.
2. Open a command prompt
   Start > Run > cmd
3. Change directory to the folder where you saved **changeVPN.exe**
4. Run:
   ```
   ChangeVPN SC
   ```
   Executing this command terminates existing VPN connections, and prevents additional connections until the client machine is rebooted.
5. Reboot the client machine.

Chapter 3

Full Disk Encryption

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

In This Chapter

Overview of the Login Page

If your administrator enables Full Disk Encryption, when you log in to your computer you will get a Preboot 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 page.

You can also use these options:

- **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 Preboot environment.
- Click **Options** to:
  - Open a **Virtual Keyboard** to use in the authentication process.
  - Set the **Language**.
  - Open **Help** for more information.

Authenticating to Full Disk Encryption

This section discusses how to use a fixed password 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 switch on or restart a Full Disk Encryption-protected computer, the **User Account Identification** window opens.

Enter a valid user name and password. Full Disk Encryption verifies that you are authorized to access the computer and starts the computer.

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

The following sections explain how to access your Full Disk Encryption-protected computer as a new user. The administrator will give you your personal user account and a password.

To authenticate for the first time with your fixed password:

1. Start your Full Disk Encryption-protected computer.
   The User Account Identification window opens.
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.

If You Do Not Have Your Password

If you forget your password, 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.
2. Click **Remote Help**.
   The Remote Help Logon window opens.
3. Select either **Password Change** or **One-Time Logon.**
4. Call your administrator or helpdesk to guide you through the process.

Windows Integrated Logon

If your administrator selected the Windows Integrated Logon (WIL) feature, you are usually logged on to Windows without entering your Full Disk Encryption credentials.

You might need to authenticate yourself to Full Disk Encryption if you:

- Remove your WIL-enabled computer from the network
- Add hardware devices to your WIL-enabled computer or in any way changed the hard drive
- Move the hard drive to another computer
- Exceed the allowed number of failed attempts to log on to Windows.

If the system detects any indications of these issues, WIL can be disabled automatically. The computer then restarts, and you must authenticate yourself to Full Disk Encryption before the operating system starts.

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

Note - The **Max Failed Windows Logon Attempts** feature is not supported in Windows Vista and Windows 7.

Using the Virtual Keyboard

From the Preboot page, select **Options > Virtual Keyboard** to open a Virtual Keyboard in the default language of your computer. You can use the virtual keyboard throughout the authentication.

To close the virtual keyboard, click it again from the **Options** menu.

Changing the Language

You can set the Preboot 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 Preboot screen:

1. From the Preboot screen, select **Options > Language**.

   The Language window opens.
2. Select a language and click **OK**.

   The computer restarts automatically. When it starts again, the Preboot screen is in the selected language.

Chapter 4

Anti-malware

The integrated Anti-malware features protect your computer against viruses, spyware, and riskware in a single powerful operation. Multiple scanning options automatically detect viruses, spyware, and riskware and make them harmless before they can damage your computer.

In This Chapter

Anti-malware Components

Anti-malware includes:

- **Anti-virus** - The Anti-virus feature keeps known and unknown viruses from affecting your computer by scanning files and comparing them to a database of known viruses and against a set of characteristics that tend to reflect virus behavior. If a virus is detected, it is rendered harmless, either by repairing or denying access to the infected file.
- **Anti-spyware -** The Anti-spyware feature detects spyware components on your computer and either removes them automatically, or places them in quarantine so that you can remove them manually after assessing their risk.
- **Riskware** - Riskware is computer software that was not intended to use maliciously, however it can potentially be dangerous. Anti-malware warns users if riskware is present.

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. Endpoint Security client can automatically uninstall some Anti-virus applications for you. If you are using a program that cannot be uninstalled automatically, use **Add/Remove Program**s from the Windows Control Panel.

Viewing Virus and Spyware Protection Status

To view the status of your Anti-malware protection, go to the Anti-malware Details page. From this area you can:

- Verify that Anti-malware is turned on.
- See the dates and times of your last scans and update.
- Run a scan.
- See files and paths that are excluded from scans.
- See items that are quarantined.

Updating Anti-malware

Every virus or spyware application contains a definition file, with information to identify and locate viruses and spyware on the computer. As new viruses or spyware applications are discovered, the client updates its databases with the definition files it needs to detect these new threats.

The Endpoint Security client regularly gets updates. In the History section of the **Anti-malware Detail** pane, you can see when the last update took place and when the next update is scheduled.

You can run a new update at any time by clicking **Update Now** from the **Tools** menu of the Endpoint Security Main Page.

Scanning

There are several ways you can initiate a scan of your computer or a specific file.

- In the **Anti-malware Details** page, click **Scan Now.**
- In the Endpoint Security Main Page, click **Scan Now** from the **Tools** menu.
- Right-click a file on your computer and choose **Scan with Check Point Anti-virus**.
- Open a file (if On-Access scanning is not excluded for the file type or folder).

You may run up to five scans simultaneously. Scans are performed in the order in which they are initiated.

System scans provide another level of protection by allowing you to scan the entire contents of your computer at one time. System scans detect viruses that may be dormant on your computer's hard drive, and if run frequently, can ensure that your Anti-virus signature files are up to date.

Because of the thorough nature of full-system scans, they can take some time to perform. As a result, your system's performance may be slowed down while a full-system scan is in progress. To avoid any impact on your workflow, your administrator can schedule system scans to run at a time when you are least likely to be using your computer.

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 **Pause** again to resume the current scan.

During the scan, the **Advanced** button is disabled.

Understanding Scan Results

After the scan is completed, details of malware detected shows in the scan window. It contains these fields:

- File - The name of the file.
- Type - The type of threat it is.
- Action - Action- what actions Endpoint Security took.
- Result - The result of the action. Results include: Quarantined, Deleted, Failed to Quarantine, and Failed to Delete.
- Path - Where the infection was found on the computer.

Submitting Viruses and Spyware to Check Point

Reporting suspected malware to Check Point helps to improve the security and protection of all Internet users. The Check Point Security Team monitors all incoming submissions for new files. The Check Point Security Team will act on your submission as appropriate and may contact you for more information or to provide details about the files you submit.

Due to the volume of malware released each day, our researchers cannot respond to each file you submit. However, we appreciate the assistance of our users and thank you for taking the time to help secure the Internet. Please address any questions or concerns to: security@checkpoint.com

To submit malware to Check Point for review:

1. Place the malware file in a password-protected .zip archive with the password set to *infected*.
   For help with creating a password protected archive, refer to the Help for WinZip.
2. Send the .zip file to malware@checkpoint.com
   Use this e-mail address only for sending malware to the Check Point Security Team.

Important - Do not send malware files if you feel you cannot do so safely or if it would increase the risk of infection or damage to your system. Do not e-mail suspected malware files to others as they could be malicious.

Viewing Quarantined Items

In some cases, items detected during a Anti-malware scan cannot be treated or removed automatically. These items are usually placed into quarantine so that they are rendered harmless but preserved so that they may be treated in the future after an update to your virus and spyware signature files.

To view and treat Anti-malware in quarantine:

1. Open the **Anti-malware Detail** pane**.**
2. Click **Quarantine**.
3. The details of the quarantined files open:
   - Infection - Name of the malware
   - Type - Either, virus, spyware, or a specific type of malware
   - Risk - The risk level of the infection
   - Path - The original location of the virus on your computer.
   - Days in Quarantine - Number of days the file has been in quarantine.
4. Select a file and click:
   - **Delete** - Send the item to the Recycle Bin.
   - **Restore** - Takes the file out of quarantine because you decide it is safe. Make sure that the file is really safe before you do this.

Chapter 5

Firewall & Application Control

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

In This Chapter

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

Application Control restricts network access of applications that act as either clients or servers.

When a program requests access for the first time, a New Program alert asks you if you want to grant the program access permission. If the program is trying to act as a server, a Server Program alert is displayed. A Server Program alert asks you if you want to grant server permission to a program.

To avoid seeing numerous alerts for the same program, select the **Remember this answer** checkbox before clicking **Yes** or **No**.

Afterwards, the client will silently block or allow the program. If the same program requests access again, a Repeat Program alert asks you if you want to grant (or deny) access permission to a program that has requested it before.

Because Trojan horses and other types of malware often need server rights, you should be particularly careful to give server permission only to programs that you know and trust, and that need server permission to operate properly.

Chapter 6

Media Encryption and Port Protection

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

- The policy says whether the Operating System can access devices connecting on a physical port, like a USB stick
- Based on your permissions, it gives you the option to encrypt external devices that you connect to your machine so that others will not be able to access the information

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

In This Chapter

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 relevant for you.

- Media Encryption lets you encrypt and control access to data on removable media connected to endpoint computers. The greatest threat when granting access to removable media storage devices is the loss of sensitive or proprietary information. Media Encryption ensures that data can be accessed only by authorized persons on authorized systems.

  You can also access encrypted devices on computers that do not have Media Encryption installed, as long as the media was encrypted allowing this and you have the password to the device.
- Port Protection controls access to removable media and devices such as: floppy disks, PDAs, flash memory, digital cameras, external hard disks (FAT formatted), etc. It controls device access on all available ports including USB and Firewire. Rules define access rights for each type of removable media and the ports that they connect to, including prerequisites such as virus scanning and data authorization.

  These rules specify whether you have Read Only, Read/Write, and/or Execute permissions to removable media connected to a port on your computer, such as: CD/DVD drives, PDAs, Blackberries, Bluetooth devices and external hard disks. The policy might also prevent you from connecting unauthorized devices to your computer ports at all.

Using Media Encryption and Port Protection

This section describes the process of encrypting, decrypting and managing removable media.

Media Encryption and Port Protection secures removable media by encrypting some or all of the storage area of the media, and then putting your files in this encrypted area.

Important - Media Encryption has no way of detecting hardware faults on external drives. For this reason, the encrypted area 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 media devices that are attached to your computer.

Encrypting Media

The policy in your organization can be configured to allow access only to encrypted media. You might also have sensitive data on removable devices that you want to encrypt to protect the information. For example, you need to transport sensitive files from one office to another on a USB stick. In both cases you are guided through the encryption process by on-screen instructions. The process creates an encrypted storage area on the device.

You can define, in percentage, how much of the device you want to encrypt. If, for example, you set this to 50%, Media Encryption creates an encrypted container that is half the size of the total disk space. When you import and encrypt files, the files are always placed in this container.

Note - If you define an area that is smaller than the data you want to put there, the encryption will fail.

Important - It is not advisable to encrypt removable media that may be used in external non-computer devices such as: digital cameras, iPods, MP3 players, etc. In such cases, a message appears and the media is granted read-only access. If the encryption process has started, let it finish and then decrypt the media by clicking **Export Media from EPM Control**.

To encrypt media:

1. From the **Media Encryption and Port Protection Details** window select a removable media device or CD/DVD from the list of devices and click **Create Encrypted Storage**.

   The **Password Protection** window opens.
2. In the Password Protection window, enter a **full access password** and confirm it. You will have to enter this password to access the device in the future. Optionally, enter a **read only password** that someone can use to access the device with read only permission.
3. Click **Continue**.
4. In the **Media Properties** section of the open window, select a percentage of the media to encrypt.

   Note - For CDs or DVDs, it is not possible to encrypt only a part of the disk, so this setting is grayed out.
5. Optionally, select **Secure Format** to erase everything on the device and reformat it before encryption. You might want to do this if there was confidential information on the device that you want to make sure is completely erased. Select the number of format passes. The more you select, the more secure the device is. The encryption process takes extra time for each format pass.
6. In the **Media Owner Information** section, define the owner of the media device. 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 media 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.

Note -When encrypting CDs/DVDs, only the **Assign media to a user** option is available.

7. Click **Encrypt**.
8. If you are encrypting a CD/DVD, a window displays where you can add and remove files which will be imported to the encrypted area on the disk.
   a) Go up one step in the folder structure.
   b) Add files or add an entire folder to be burnt on the disk.
   c) Select and delete any file or folder that you do not want to include on the disk. Click **Next**. The files will be imported, and the disk will be burnt.
   d) A message displays when the burning process is finished.
9. A window displays the encryption progress. Depending on the type of media 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 media.

10. When the Finish window opens, click **Finish** to complete the process. The **Media Encryption and Port Protection** window returns.

The encrypted media status now appears as **Encrypted.**

Encrypting CDs and DVDs

If permitted by your policy, Media Encryption 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.
- Encryption can be done only on RW and blank R/RW disks.
- Nothing can be added to or removed from a once-burnt CD/DVD. Such disks can only be erased completely.

The process of importing and exporting files to CD/DVDs is similar to that of other removable media described in Encrypting Media (on page 49). Two differences between CDs/DVDs and other removable media 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.

Accessing Encrypted Media from a Media Encryption Computer

When it protects information, Media Encryption creates an encrypted area on your removable device and puts the data there. To access the data in the protected area, you can choose between removing the files from the protected container or removing the encryption from the device. Normally, your Media Encryption and Port Protection policy permits only the owner or another authorized user to perform the decryption.

To remove the files from the encrypted container:

1. Insert your encrypted media to your computer.
2. If you do not have automatic access to the media, you may need to enter a password. In the **Password** window, enter the appropriate password. Click **Unlock**
3. The files are now accessible. They are not encrypted so you can move the files from the media to your hard disk by drag and drop or copy and paste.

To remove encryption from the encrypted device:

1. Insert your encrypted media to your computer.
2. If you do not have automatic access to the media, you may need to enter a password. In the **Password** window, enter the appropriate password. Click **OK**.
3. From the **Media Encryption and Port Protection Details** page, click **Remove Encryption**.

4. Click **Finish** to complete the process. The **decryption** may take some time depending on the size and type of the device. When the decryption process is finished, the encrypted area has been decrypted and removed. The data on the media is now unencrypted and unprotected.

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

Accessing Encrypted Media from non-Media Encryption Computers

If your profile allows access to encrypted information from computers that do not have Media Encryption and Port Protection installed, an unlock.exe file is copied automatically to the root folder of the removable media during the encryption process.

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 decrypt removable media from a computer without Media Encryption and Port Protection:

1. Insert the encrypted device into a machine not running Media Encryption and Port Protection. The following files are displayed:
   - **dvrem.epm**, - The encrypted storage
   - **autorun.exe** - Runs the unlock file
   - **unlock.exe** – The file that decrypts the encrypted storage.
2. To access encrypted data on the device, double-click the `unlock.exe` file (it will auto-run on most systems). Enter the access password.
3. The Endpoint Security Media Encryption Explorer window opens, which displays the contents of the encrypted device.
4. There are two methods of accessing the data on the encrypted device: extracting files to the local hard disk or to a secure location on the device itself. See the descriptions of these two methods below.

   If you used a Full access password, you can now drag-and-drop or copy-and-paste files to and from the encrypted device. If you used a Read Only password, you can only read the information on the device but not move files to or from the device.

Extracting Files to Local Hard Disk

You can extract files and folders from the encrypted area and save them on a local hard disk or network drive.

To extract files to your hard disk or network drive:

1. Select the files or folders that you want to decrypt and save to a local hard disk by using the **Ctrl** and **Shift** keys, then right-click and select **Extract**.
2. Select the location where you want the files to be saved.

   The files are now decrypted and saved in clear text at the location you chose.
3. When you close the Endpoint Security Media Encryption Explorer, you are asked if you wish to securely delete all of the extracted files. If you click **Yes,** all of the newly extracted files will be securely deleted, thus leaving no traces of sensitive information.

Extracting Files to Temporary Secure Location

To extract files to a temporary secure location:

- Double-click the file within the drive explorer.

  The Endpoint Security Media Encryption Explorer transparently decrypts the file to a temporary location and then automatically opens the file with the associated application.

To view a file in secure mode:

- Double-click the required file.

  If you make any changes to the decrypted file, a prompt is displayed asking you whether the encrypted file within the device should be updated. Click **Yes** if you want to save the file.

Media Encryption and Port Protection Scanning

To start a Media Encryption and Port Protection scan:

- In Media Encryption and Port Protection **Detail** pane, select a device and click **Scan Device**.
- Open a file and it is scanned automatically.

You can run up to five scans simultaneously. Scans are performed in the order in which they are initiated.

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 media 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 administrator-defined criteria that can be accessed by clicking **Policy Note**.

5. Click **OK**.

Chapter 7

WebCheck

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

In This Chapter

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.

- **Corporate Mode**: Your browser opens in Corporate mode automatically when you go to your corporate Web site or Internet Web sites your administrator deems trustworthy. WebCheck's 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 Corporate 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 reach your real computer hard disks.
- **Anti-phishing (signature)**: WebCheck tracks the most recently discovered phishing and spy sites. If you go to one of these sites, WebCheck interrupts your browsing with a warning so you can leave the site immediately.
- **Anti-phishing (heuristics)**: WebCheck also uses heuristics, which look for certain known characteristics of fraudulent sites, to detect phishing sites that were created even seconds before you encountered them.

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 7-1 ***Yellow Caution Banner***

Risk level of Web site	MEDIUM for entering data or downloading files from this site.
Recommendation	With WebCheck active, viewing the site should be safe, but do not enter any sensitive data or download files at this site.
Why is the site questionable?	Click the **Read more** link in the warning dialog box to get security related information about the site.

"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 7-2 ***Blue "May Be Unsafe" Warning***

Risk level of Web site	MEDIUM to HIGH for entering data or downloading files from this site.
Recommendations	The site may not be a phishing site, but we recommend you click **Avoid this Site** if any of the following are true: • Did you get to this site by clicking a link in an e-mail? • 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**.) • Is there a misspelling in the site address, such as "yahooo" instead of "yahoo"? • Was the site created very recently? • Is the site hosted in a country you weren't expecting?
Why is the site questionable?	Heuristic detection has found some characteristics common to phishing, but the site is not officially reported as a phishing site at his time.

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 7-3 ***Dangerous Site Warning***

Risk level of Web site	VERY HIGH
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 8

Troubleshooting

In This Chapter

Technical Difficulties

Most of 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.

What You Want to Do	Required Action
See details of a log entry	Double-click the log entry
Export logs to a file	Select **File > Export to file**
See logs of a specific type	Select **View > Event Filter**
See logs from a specific date	Select **View > Event Filter**
Sort logs According to a specific column	Click the column heading
Update the displayed logs one time	Select **File > Refresh** or click the **Refresh** icon
Update the displayed logs every 5 seconds	Select **File > Auto Refresh** or click the **Auto Refresh** icon

What You Want to Do	Required Action
Copy log entries to the clipboard	Select the entries and click Control +C

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